FISA AMENDMENTS ACT OF 2008

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MAY 31, 2012

Serial No. 112–129

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
74–415 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JARED POLIS, Colorado

RICHARD HERTLING, *Staff Director and Chief Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
MARK AMODEI, Nevada

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois
JARED POLIS, Colorado

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MAY 31, 2012

FISA AMENDMENTS ACT OF 2008

THURSDAY, MAY 31, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10 a.m., in room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Goodlatte, Lungren, Marino, Gowdy, Scott, Conyers, Cohen, Johnson, Chu, Jackson Lee, and Polis.

Staff Present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Sam Ramer, Counsel; Arthur Radford Baker, Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; and Aaron Hiller, Counsel.

Mr. SENSENBRENNER. The Subcommittee will be in order.

Today's hearing examines the FISA Amendments Act of 2008, which is set to expire at the end of the year. The Foreign Intelligence Surveillance Act, or FISA, was enacted in 1978 to provide procedures for the domestic collection of foreign intelligence.

In the 40 years since FISA's enactment, communication technologies have changed dramatically and revolutionalized the transmission of international communication. The shift from wireless satellite communications to fiber-optic wire communications alter the manner in which foreign communications are transmitted. The use of wire technology inside the United States to transit a phone call that takes place overseas have the unintended consequence of requiring the government to obtain an individualized FISA Court order to monitor foreign communications by non-U.S. persons.

In 2008, Congress passed and the President signed the bipartisan FISA amendments to update our foreign intelligence laws. The Act permits the Attorney General and the Director of National Intelligence to target foreign persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information. The Act requires prior Court approval of all government surveillance using these authorities, including Court approval of the government's targeting and minimization procedures.

The FISA Amendments Act strengthens civil liberty protections for U.S. citizens by requiring the government to obtain an individualized Court order from the FISA Court to target them anywhere in the world to acquire foreign intelligence information.

Foreign surveillance under the FISA Amendments Act is subject to extensive oversight by the Administration and Congress. Every 60 days, the Justice Department and the Director of National Intelligence conduct on-site reviews of surveillance conducted pursuant to the FISA Amendments Act. In addition, the Attorney General and the DNI conduct detailed assessments of compliance with Court-approved targeting and minimization procedures and provide these assessments to Congress twice a year.

The Administration is also now required to submit to the Judiciary and Intelligence Committees a copy of any FISA Court order, opinion, or decision and the accompanying pleadings, briefs, and other memoranda of law relating to a significant construction or interpretation of any provision of FISA.

The Obama administration supports reauthorization of the FISA Amendments Act for 5 years. DNI James Clapper and Attorney General Eric Holder have identified reauthorization of the Act as the top legislative priority of the intelligence community and are urging Congress to reauthorize the Act without amendment.

Without objection, a February 8 letter from Director Clapper and General Holder and a March 26 letter from Director Clapper will be made part of the record.

Hearing no objection, so ordered.

[The information referred to follows:]

FEB 08 2012

The Honorable John Boehner
Speaker
United States House of Representatives
Washington, D.C. 20515

The Honorable Harry Reid
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Nancy Pelosi
Democratic Leader
United States House of Representatives
Washington, D.C. 20515

The Honorable Mitch McConnell
Republican Leader
United States Senate
Washington, D.C. 20510

Dear Speaker Boehner and Leaders Reid, Pelosi, and McConnell:

We are writing to urge that the Congress reauthorize Title VII of the Foreign Intelligence Surveillance Act (FISA) enacted by the FISA Amendments Act of 2008 (FAA), which is set to expire at the end of this year. Title VII of FISA allows the Intelligence Community to collect vital information about international terrorists and other important targets overseas. Reauthorizing this authority is the top legislative priority of the Intelligence Community.

One provision, section 702, authorizes surveillance directed at non-U.S. persons located overseas who are of foreign intelligence importance. At the same time, it provides a comprehensive regime of oversight by all three branches of Government to protect the privacy and civil liberties of U.S. persons. Under section 702, the Attorney General and the Director of National Intelligence may authorize annually, with the approval of the Foreign Intelligence Surveillance Court (FISC), intelligence collection targeting categories of non-U.S. persons abroad, without the need for a court order for each individual target. Within this framework, *no* acquisition may intentionally target a U.S. person, here or abroad, or any other person known to be in the United States. The law requires special procedures designed to ensure that all such acquisitions target only non-U.S. persons outside the United States, and to protect the privacy of U.S. persons

whose nonpublic information may be incidentally acquired. The Department of Justice and the Office of the Director of National Intelligence conduct extensive oversight reviews of section 702 activities at least once every sixty days, and Title VII requires us to report to the Congress on implementation and compliance twice a year.

A separate provision of Title VII requires that surveillance directed at U.S. persons overseas be approved by the FISC in each individual case, based on a finding that there is probable cause to believe that the target is a foreign power or an agent, officer, or employee of a foreign power. Before the enactment of the FAA, the Attorney General could authorize such collection without court approval. This provision thus increases the protection given to U.S. persons.

The attached background paper provides additional unclassified information on the structure, operation and oversight of Title VII of FISA.

Intelligence collection under Title VII has produced and continues to produce significant intelligence that is vital to protect the nation against international terrorism and other threats. We welcome the opportunity to provide additional information to members concerning these authorities in a classified setting. We are always considering whether there are changes that could be made to improve the law in a manner consistent with the privacy and civil liberties interests of Americans. Our first priority, however, is reauthorization of these authorities in their current form. We look forward to working with you to ensure the speedy enactment of legislation reauthorizing Title VII, without amendment, to avoid any interruption in our use of these authorities to protect the American people.

Sincerely,

James R. Clapper
Director of National Intelligence

Eric H. Holder, Jr.
Attorney General

Enclosure

Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of Director of National Intelligence (ODNI)

This paper describes the provisions of Title VII of the Foreign Intelligence Surveillance Act (FISA) that were added by the FISA Amendments Act of 2008 (FAA).[1] Title VII has proven to be an extremely valuable authority in protecting our nation from terrorism and other national security threats. Title VII is set to expire at the end of this year, and its reauthorization is the top legislative priority of the Intelligence Community.

The FAA added a new section 702 to FISA, permitting the Foreign Intelligence Surveillance Court (FISC) to approve surveillance of terrorist suspects and other foreign intelligence targets who are *non-U.S. persons outside the United States*, without the need for individualized court orders. Section 702 includes a series of protections and oversight measures to safeguard the privacy and civil liberties interests of U.S. persons. FISA continues to include its original electronic surveillance provisions, meaning that, in most cases,[2] an individualized court order, based on probable cause that the target is a foreign power or an agent of a foreign power, is still required to conduct electronic surveillance of targets inside the United States. Indeed, other provisions of Title VII extend these protections to U.S. persons overseas. The extensive oversight measures used to implement these authorities demonstrate that the Government has used this capability in the manner contemplated by Congress, taking great care to protect privacy and civil liberties interests.

This paper begins by describing how section 702 works, its importance to the Intelligence Community, and its extensive oversight provisions. Next, it turns briefly to the other changes made to FISA by the FAA, including section 704, which requires an order from the FISC before the Government may engage in surveillance targeted at U.S. persons overseas. Third, this paper describes the reporting to Congress that the Executive Branch has done under Title VII of FISA. Finally, this paper explains why the Administration believes it is essential that Congress reauthorize Title VII.

1. Section 702 Provides Valuable Foreign Intelligence Information About Terrorists and Other Targets Overseas, While Protecting the Privacy and Civil Liberties of Americans

Section 702 permits the FISC to approve surveillance of terrorist suspects and other targets who are non-U.S. persons outside the United States, without the need for individualized court orders. The FISC may approve surveillance of these kinds of targets

---

[1] Title VII of FISA is codified at 50 U.S.C. §§ 1881-1881g.

[2] In very limited circumstances, FISA expressly permits surveillance without a court order. *See, e.g.*, 50 U.S.C. § 1805(e) (Attorney General may approve emergency surveillance if the standards of the statute are met and he submits an application to the FISC within seven days).

when the Government needs the assistance of an electronic communications service provider.

Before the enactment of the FAA and its predecessor legislation, in order to conduct the kind of surveillance authorized by section 702, FISA was interpreted to require that the Government show on an individualized basis, with respect to all non-U.S. person targets located overseas, that there was probable cause to believe that the target was a foreign power or an agent of a foreign power, and to obtain an order from the FISC approving the surveillance on this basis. In effect, the Intelligence Community treated non-U.S. persons located overseas like persons in the United States, even though foreigners outside the United States generally are not entitled to the protections of the Fourth Amendment. Although FISA's original procedures are proper for electronic surveillance of persons inside this country, such a process for surveillance of terrorist suspects overseas can slow, or even prevent, the Government's acquisition of vital information, without enhancing the privacy interests of Americans. Since its enactment in 2008, section 702 has significantly increased the Government's ability to act quickly.

Under section 702, instead of issuing individual court orders, the FISC approves annual certifications submitted by the Attorney General and the DNI that identify categories of foreign intelligence targets. The provision contains a number of important protections for U.S. persons and others in the United States. First, the Attorney General and the DNI must certify that a significant purpose of the acquisition is to obtain foreign intelligence information. Second, an acquisition may not intentionally target a U.S. person. Third, it may not intentionally target any person known at the time of acquisition to be in the United States. Fourth, it may not target someone outside the United States for the purpose of targeting a particular, known person in this country. Fifth, section 702 prohibits the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of the acquisition" to be in the United States. Finally, it requires that any acquisition be consistent with the Fourth Amendment.

To implement these provisions, section 702 requires targeting procedures, minimization procedures, and acquisition guidelines. The targeting procedures are designed to ensure that an acquisition only targets persons outside the United States, and that it complies with the restriction on acquiring wholly domestic communications. The minimization procedures protect the identities of U.S. persons, and any nonpublic information concerning them that may be incidentally acquired. The acquisition guidelines seek to ensure compliance with all of the limitations of section 702 described above, and to ensure that the Government files an application with the FISC when required by FISA.

The FISC reviews the targeting and minimization procedures for compliance with the requirements of both the statute and the Fourth Amendment. Although the FISC does not approve the acquisition guidelines, it receives them, as do the appropriate congressional committees. By approving the certifications submitted by the Attorney General and the DNI as well as by approving the targeting and minimization procedures,

the FISC plays a major role in ensuring that acquisitions under section 702 are conducted in a lawful and appropriate manner.

Section 702 is vital in keeping the nation safe. It provides information about the plans and identities of terrorists, allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States. Failure to reauthorize section 702 would result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities. Although this unclassified paper cannot discuss more specifically the nature of the information acquired under section 702 or its significance, the Intelligence Community is prepared to provide Members of Congress with detailed classified briefings as appropriate.

The Executive Branch is committed to ensuring that its use of section 702 is consistent with the law, the FISC's orders, and the privacy and civil liberties interests of U.S. persons. The Intelligence Community, the Department of Justice, and the FISC all oversee the use of section 702. In addition, congressional committees conduct essential oversight, which is discussed in section 3 below.

Oversight of activities conducted under section 702 begins with components in the intelligence agencies themselves, including their Inspectors General. The targeting procedures, described above, seek to ensure that an acquisition targets only persons outside the United States and that it complies with section 702's restriction on acquiring wholly domestic communications. For example, the targeting procedures for the National Security Agency (NSA) require training of agency analysts, and audits of the databases they use. NSA's Signals Intelligence Directorate also conducts other oversight activities, including spot checks of targeting decisions. With the strong support of Congress, NSA has established a compliance office, which is responsible for developing, implementing, and monitoring a comprehensive mission compliance program.

Agencies using section 702 authority must report promptly to the Department of Justice and ODNI incidents of noncompliance with the targeting or minimization procedures or the acquisition guidelines. Attorneys in the National Security Division (NSD) of the Department routinely review the agencies' targeting decisions. At least once every 60 days, NSD and ODNI conduct oversight of the agencies' activities under section 702. These reviews are normally conducted on-site by a joint team from NSD and ODNI. The team evaluates and, where appropriate, investigates each potential incident of noncompliance, and conducts a detailed review of agencies' targeting and minimization decisions.

Using the reviews by Department of Justice and ODNI personnel, the Attorney General and the DNI conduct a semi-annual assessment, as required by section 702, of compliance with the targeting and minimization procedures and the acquisition guidelines. The assessments have found that agencies have "continued to implement the

procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702." The reviews have not found "any intentional attempt to circumvent or violate" legal requirements. Rather, agency personnel "are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States."[3]

Section 702 thus enables the Government to collect information effectively and efficiently about foreign targets overseas and in a manner that protects the privacy and civil liberties of Americans. Through rigorous oversight, the Government is able to evaluate whether changes are needed to the procedures or guidelines, and what other steps may be appropriate to safeguard the privacy of personal information. In addition, the Department of Justice provides the joint assessments and other reports to the FISC. The FISC has been actively involved in the review of section 702 collection. Together, all of these mechanisms ensure thorough and continuous oversight of section 702 activities.

2. Other Important Provisions of Title VII of FISA Also Should Be Reauthorized

In contrast to section 702, which focuses on foreign targets, section 704 provides heightened protection for collection activities conducted overseas and directed against U.S. persons located outside the United States. Section 704 requires an order from the FISC in circumstances in which the target has "a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." It also requires a showing of probable cause that the targeted U.S. person is "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power." Previously, these activities were outside the scope of FISA and governed exclusively by section 2.5 of Executive Order 12333.[4] By requiring the approval of the FISC, section 704 enhanced the civil liberties of U.S. persons.

The FAA also added several other provisions to FISA. Section 703 complements section 704 and permits the FISC to authorize an application targeting a U.S. person outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or data, and is conducted in the United States. Because the target is a U.S. person, section 703 requires an individualized court order and a showing of probable cause that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. Other sections of Title VII allow the Government to obtain various

---

[3] *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, Reporting Period: December 1, 2010 – May 31, 2011* at 2-3, 5 (December 2011).

[4] Since before the enactment of the FAA, section 2.5 of Executive Order 12333 has required the Attorney General to approve the use by the Intelligence Community against U.S. persons abroad of "any technique for which a warrant would be required if undertaken for law enforcement purposes." The Attorney General must find that there is probable cause to believe that the U.S. person is a foreign power or an agent of a foreign power. The provisions of section 2.5 continue to apply to these activities, in addition to the requirements of section 704.

authorities simultaneously, govern the use of information in litigation, and provide for congressional oversight. Section 708 clarifies that nothing in Title VII is intended to limit the Government's ability to obtain authorizations under other parts of FISA.

3. Congress Has Been Kept Fully Informed, and Conducts Vigorous Oversight, of Title VII's Implementation

FISA imposes substantial reporting requirements on the Government to ensure effective congressional oversight of these authorities. Twice a year, the Attorney General must "fully inform, in a manner consistent with national security," the Intelligence and Judiciary Committees about the implementation of Title VII. With respect to section 702, this semi-annual report must include copies of certifications and significant FISC pleadings and orders. It also must describe any compliance incidents, any use of emergency authorities, and the FISC's review of the Government's pleadings. With respect to sections 703 and 704, the report must include the number of applications made, and the number granted, modified, or denied by the FISC.

Section 702 requires the Government to provide to the Intelligence and Judiciary Committees its assessment of compliance with the targeting and minimization procedures and the acquisition guidelines. In addition, Title VI of FISA requires a summary of significant legal interpretations of FISA in matters before the FISC or the Foreign Intelligence Surveillance Court of Review. The requirement extends to interpretations presented in applications or pleadings filed with either court by the Department of Justice. In addition to the summary, the Department must provide copies of judicial decisions that include significant interpretations of FISA within 45 days.

The Government has complied with the substantial reporting requirements imposed by FISA to ensure effective congressional oversight of these authorities. The Government has informed the Intelligence and Judiciary Committees of acquisitions authorized under section 702; reported, in detail, on the results of the reviews and on compliance incidents and remedial efforts; made all written reports on these reviews available to the Committees; and provided summaries of significant interpretations of FISA, as well as copies of relevant judicial opinions and pleadings.

4. It Is Essential That Title VII of FISA Be Reauthorized Well in Advance of Its Expiration

The Administration strongly supports the reauthorization of Title VII of FISA. It was enacted after many months of bipartisan effort and extensive debate. Since its enactment, Executive Branch officials have provided extensive information to Congress on the Government's use of Title VII, including reports, testimony, and numerous briefings for Members and their staffs. This extensive record demonstrates the proven value of these authorities, and the commitment of the Government to their lawful and responsible use.

Reauthorization will ensure continued certainty with the rules used by Government employees and our private partners. The Intelligence Community has invested significant human and financial resources to enable its personnel and technological systems to acquire and review vital data quickly and lawfully. Our adversaries, of course, seek to hide the most important information from us. It is at best inefficient and at worst unworkable for agencies to develop new technologies and procedures and train employees, only to have a statutory framework subject to wholesale revision. This is particularly true at a time of limited resources. It is essential that these authorities remain in place without interruption—and without the threat of interruption—so that those who have been entrusted with their use can continue to protect our nation from its enemies.

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

The Honorable John Boehner
Speaker
United States House of Representatives
Washington, D.C. 20515

MAR 2 6 2012

The Honorable Harry Reid
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Nancy Pelosi
Democratic Leader
United States House of Representatives
Washington, D.C. 20515

The Honorable Mitch McConnell
Republican Leader
United States Senate
Washington, D.C. 20510

Dear Speaker Boehner and Leaders Reid, Pelosi, and McConnell:

On behalf of the Administration, I am pleased to provide you with the Administration's proposed legislation to reauthorize Title VII of the Foreign Intelligence Surveillance Act (FISA) enacted by the FISA Amendments Act of 2008 (FAA), for consideration by the Congress. On February 8, Attorney General Holder and I wrote you to urge that the Congress reauthorize Title VII of FISA, which is set to expire at the end of this year. Title VII of FISA allows the Intelligence Community to collect vital information about international terrorists and other important targets overseas while providing robust protection for the civil liberties and privacy of Americans. Reauthorizing this authority is the top legislative priority of the Intelligence Community.

We look forward to working with you to ensure the speedy enactment of legislation reauthorizing these authorities until June 1, 2017. The Office of Management and Budget advises that there is no objection, from the standpoint of the Administration's program, to the presentation of this legislative proposal package for your consideration and the consideration of the Congress at this time.

Sincerely,

James R. Clapper

Enclosure:
FISA Amendments Act of 2008 Extension Act of 2012

cc: The Honorable Mike Rogers
The Honorable C.A. Dutch Ruppersberger
The Honorable Lamar Smith
The Honorable John Conyers Jr.
The Honorable Dianne Feinstein
The Honorable Saxby Chambliss
The Honorable Patrick J. Leahy
The Honorable Charles E. Grassley

FISA AMENDMENTS ACT OF 2008 EXTENSION ACT OF 2012

(a) Extension- Section 403(b)(1) of the FISA Amendments Act of 2008 (Public Law 110-261; 50 U.S.C. 1881 note) is amended by striking `December 31, 2012' and inserting `June 1, 2017'.

(b) Technical and Conforming Amendments- Section 403(b)(2) of such Act (Public Law 110-261; 122 Stat. 2474) is amended by striking `December 31, 2012' and inserting `June 1, 2017'.

(c) Orders in Effect- Section 404(b)(1) of such Act (Public Law 110-261; 50 U.S.C. 1801 note) is amended in the heading by striking `December 31, 2012' and inserting `June 1, 2017'.

Sectional Analysis:

This section extends the sunset for Title VII of FISA, as added by the FISA Amendments Act of 2008 (Public Law 110–261), now scheduled to occur on December 31, 2012, to June 1, 2017. Title VII of FISA allows the Intelligence Community to collect vital information about international terrorist and other important targets overseas. Reauthorizing this authority is the top legislative priority of the Intelligence Community.

Mr. SENSENBRENNER. Foreign terrorists remain committed to the destruction of our country, and their methods of communication are constantly evolving. It is essential that our intelligence community has the necessary tools to detect and disrupt such attacks. We have a duty to ensure that the intelligence community can gather the in-

formation they need to protect our country and its citizens. I look forward to hearing more about this issue and thank all of our witnesses for participating in today's hearing.

It is now my pleasure to recognize for his opening statement the Ranking Member of the Subcommittee, the gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. I want to thank you for holding this hearing on the FISA Amendments Act of 2008. That is the FAA of 2008.

The Act established some parameters for the secret and, in my view, unconstitutional collection of intelligence information that had been ordered following the 9/11 attacks. However, some gaping holes were left in what is required to adequately protect the privacy of United States citizens. Americans have the right to feel as well as be free and secure in their persons belonging and activities from unwarranted government intrusion, and I am concerned that the FAA does not fully meet that standard.

The Foreign Intelligence Surveillance Act, or FISA, was passed in 1978 to curb abuses that had been occurring in the collection and use of intelligence information, foreign and domestic. It was not passed for the purpose of excluding all foreign intelligence collection from the United States but to regulate and separate foreign and domestic intelligence collection.

Collection of foreign intelligence requires merely that there is—collection of foreign intelligence requires merely that there is probable cause to believe that an actor is an agent of the foreign government and that foreign intelligence is a significant purpose of the collection. Now, foreign intelligence collection is only a significant purpose of the collection. We are left to wonder what is the primary purpose of information gathering. And with the USA Patriot Act we have added members of terrorist organizations and lone wolf terrorists to this low threshold for collecting intelligence.

FISA has also recognized that foreign intelligence collection falls under the requirements of the Fourth Amendment when rights of U.S. persons are implicated.

Such a low threshold for collecting intelligence—with such a low threshold for collecting intelligence, diligent oversight and reporting is required to ensure that the collection is not for a broader purpose than is necessary to achieve the goals. We should not be surveilling Americans by this low standard without some significant oversight. That is why we need clear standards that are rigorously enforced.

The Foreign Intelligence Surveillance Court was created under FISA to oversee the operations of foreign intelligence gathering, and I suspect that the Court is doing a good job and may be doing a good job within its authority, but it operates in secrecy. I believe that the public has a right to know from laws and policies and reports on their implementation that the government is being held accountable for the Constitution and the laws. I do not believe that the FAA provides sufficient assurances to the public in either of these areas.

We often hear the need for the government to expand its powers to meet the needs of technology but seldom do we hear the likewise need to protect privacy when technology advances. In 1978, there

was little American communication to and from foreign countries compared to today's constant barrage of emails, phone calls, and other electronic communications. What was rare in 1978 is now commonplace and just as deserving of privacy from government spying and intrusion.

The FAA processes result in massive amounts of information being collected with an untold amount of it affecting Americans in America. Now when we talk about government collection of data it is not just computers, it is government officials who may be your neighbors; and when you spread it around to other agencies you may be talking about other neighbors who are getting access to your private information.

The primary requirements of the Fourth Amendment are probable cause warrants and particularity in conduct and place. It is not clear that these standards are being met when required under the FAA's current structure.

Now we hear complaints that it is too burdensome for the government to go through the procedures required and that we have to give up some of our privacy for greater safety. I am reminded of Ben Franklin's comment that those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.

Neither the government's press for access to information to accomplish its authorized purposes or the ease by which it can get the information should lessen our constitutional protections. Emergency procedures are provided under the Constitution and under the FAA, but the exception should not become the rule.

I look forward to the testimony of our witnesses on where the FAA properly draws the lines between the insurance the public is entitled to under the Constitution and the legitimate needs of the government to do its job.

Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The Chair now recognizes the Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Sensenbrenner.

This is a sensitive discussion, as we all know, but the Fourth Amendment is critical. And I do not think that the Supreme Court—the courts have not finally ruled on what is going on. I come to this hearing disturbed by how little we know and how much more we need to know. I am glad that we are going to have closed door hearings in the near future, and I hope that they will be productive in terms of settling some of the lack of information that we have about this subject.

So I guess it is going to be legitimate for us to ask how much do we need to know, how much can we talk about publicly, and how do we make sure that, quite frankly, FISA is not out of control? At this point, we do not have any way of knowing that, and one of the problems is the so-called minimization strategy. So I think we need to strengthen minimization and to make sure that this is a very understandable FISA operation that is satisfactorily constitutional, and right now we are not able to do that.

So I am hoping that, in addition—and I hope the Chair will support or even lead in this—we need to talk to FISA officials. This

whole idea of us holding a hearing about FISA and nobody from FISA is here is part of the problem. We want to talk to the director, publicly or privately, and I have not had that opportunity yet, and I hope that the Members of the Committee share in my desire to do that.

And so I will put the rest of my statement into the record.

Mr. SENSENBRENNER. Without objection.

[The prepared statement of Mr. Conyers follows:]

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary

I want to begin by thanking both Chairman Smith and Chairman Sensenbrenner for scheduling this hearing in such a timely manner.

Mr. Scott, Mr. Nadler, and I wrote to Chairman Smith on May 9, requesting public hearings on the expiring provisions of the Foreign Intelligence Surveillance Act. Here we are, just a few days later, beginning an important discussion about civil liberties and the scope of secret government surveillance. I look forward to additional hearings on this topic, and I thank you both.

Four years ago, when we passed the FISA Amendments Act of 2008, we authorized the electronic surveillance of suspected terrorists and foreign agents located outside the United States.

Although the Foreign Intelligence Surveillance Court has some measure of oversight over these programs, the sweeping and general nature of this authority has given many cause for concern.

For example, the government may describe its operations to the court in exceptionally general terms—as broad as "all phone calls, emails, and text messages originating in Pakistan"—and conduct wide-ranging, dragnet surveillance from there. Although the law requires the government to use "minimization procedures" that limit the impact of these programs on American citizens, there is no question that the government can and does intercept and listen in on the communications of U.S. persons.

The scope of this law has also raised questions about the practice of "reverse targeting," where the government officially targets a foreign person in order to listen in on the conversations of U.S. persons on the other end of the line. This practice is explicitly prohibited by law—but with so much about these programs conducted in secret, including basic information about the impact of these programs on Americans, we have no way of knowing for sure whether the government conducts itself lawfully.

These concerns are more than theoretical. In 2009, the *New York Times* reported that the NSA had engaged in the "overcollection" of American communications in situations not permitted by law. The government assures us that this problem, although widespread, was an accident and has been corrected. Whether or not the practice was deliberate, it was illegal—and it does not inspire confidence in the program.

More recently, in a letter to Senators Ron Wyden (D-OR) and Mark Udall (D-CO), the Office of the Director of National Intelligence stated that it is "not reasonably possible" to determine how many people in the United States have had their communications intercepted and reviewed under this law. That answer is not satisfactory, and the public deserves better.

Four years ago, supporters of the bill assured us that it would adequately protect the privacy of American citizens and other U.S. persons. They continue to make those assurances. But the reason the FISA Amendment Act included a four-year sunset is so that Congress can conduct meaningful oversight—and not merely rubber stamp an executive branch prerogative.

The government can and must do a better job of responding to our questions about privacy and other civil liberties. It can do so without compromising national security or specific operations. I have no doubt that these programs are important to the executive branch, but Congress must have these answers before we can act responsibly.

I look forward to the testimony of each of the witnesses today.

Mr. CONYERS. But I would hope that my dear friend, Bobby Scott, will not support Ben Franklin's motto, take it too seriously, because we will end up in a worse situation than we are now.

I yield back the balance of my time.

Mr. SENSENBRENNER. I thank the gentleman.

Let me say for those who have missed it, this is a rare chance to see bipartisanship in action. You have the Republicans supporting the Obama administration and the Democrats criticizing the Obama administration, and I hope that everybody in the room duly notes that.

I would point out that since the FAA amendments of 2008 there has been no Federal court to my knowledge that has declared any part of the FAA amendments unconstitutional on Fourth Amendment grounds. There is a case where the Supreme Court has granted certiorari called Clapper vs. Amnesty International, but that is on the question of standing rather than on the question of alleged Fourth Amendment violations.

That being said, it is now my pleasure to introduce today's witnesses:

Kenneth Wainstein is a partner in the law firm of Cadwalader, Wickersham & Taft, where his practice focuses on corporate internal investigations. He is also an adjunct professor at Georgetown Law School. Mr. Wainstein served as an Assistant U.S. Attorney in both the Southern District of New York and the District of Columbia. Later, he served as U.S. Attorney in D.C. And then was Assistant Attorney General for National Security. He has served as FBI Director Robert Mueller's Chief of Staff and then as President Bush's Homeland Security Advisor. Mr. Wainstein received his undergraduate degree from the University of Virginia and his law degree from the University of California at Berkeley.

Marc Rotenberg is Executive Director of the Electronic Privacy Information Center, known as EPIC, in Washington, D.C., and is also an adjunct professor of law at Georgetown University Law Center. He has served on several national and international advisory panels and chairs the American Bar Association's Committee on Privacy and Information Protection. He is a founding board member and former chair of Public Interest Registry which manages the .org domain. He is a graduate of Harvard College and Stanford Law School.

Mr. Jameel Jaffer is Deputy Legal Director at the ACLU and Director of the ACLU Center for Democracy. He joined the staff of the ACLU in 2002. Before joining the staff of the ACLU, he served as a law clerk to Judge Amalya L. Kersey on the Court of Appeals for the Second Circuit and then to Judge Beverley McLachlin, the Chief Justice of the Supreme Court of Canada. He is a graduate of Williams College, Cambridge University, and Harvard Law School.

Without objection, the witnesses' statements will be entered into the record in their entirety, but I ask that you summarize your testimony in 5 minutes or less. And to help you stay within the time limit there are the green, yellow, and red lights before you, and I think you all know what they mean.

I now recognize Mr. Wainstein.

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

Mr. WAINSTEIN. Chairman Sensenbrenner, Ranking Member Scott, Ranking Member Conyers, Members of the Subcommittee, I want to thank you for the invitation to appear before you today.

Before getting into the intricacies of the FISA Amendments Act, it is important to remind ourselves about the national security threats and particularly the threat from international terrorism that this legislation was designed to address.

Since the attacks of 9/11, we have been at war with al Qaeda and its terrorist affiliates around the globe, and we are making great progress against them. There are many reasons for that progress. But one development that has contributed significantly to that progress has been Congress' decision to modernize our national security surveillance efforts with the passage of the FISA Amendments Act in 2008.

In considering the FAA's reauthorization, we also need to remember why it was that it was necessary to modernize the Foreign Intelligence Surveillance Act in the first place. As you know, FISA was passed in 1978 establishing the Foreign Intelligence Surveillance Court, or FISA Court, and requiring that any electronic surveillance of foreign powers or their agents must first be approved by that 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.

In identifying those targets that would fall within the statute and could therefore be surveilled only after the government puts together a voluminous application and obtains a court order from the FISA Court, the FISA statute laid out a number of factors the FISA Court and the government should look at, including the type of communications technology that the target was using, whether he was communicating by wire—a cable—or by satellite transmission. The result was a carveout from the court approval process for surveillances that targeted communications that were being made from overseas locations.

With the change in technology over the intervening years since 1978, however, that carveout has started to break down and the government found itself expending significant manpower generating FISA Court applications for surveillance against persons outside the United States. As a result, the government was unnecessarily expending significant resources and was increasingly forced to make tough choices regarding surveillance of worthy counterterrorism targets.

To its enduring credit, Congress recognized that this situation was untenable in a post-9/11 world; and after more than a year of careful consideration it passed the FAA, which did three critical things.

First, it authorized the FISA Court to approve surveillance of categories of non-U.S. person intelligence targets overseas without requiring the government to provide an individualized application as to each particular target, which brought the operation of FISA back in line with its original intent.

Second, it established a multi-level system of oversight by the FISA Court, by Congress, and by various actors within the executive branch to ensure this authority would be exercised in full compliance with the law and the Constitution.

And, third, it significantly added to the protections for U.S. persons by imposing 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 U.S. person is outside the United States.

In sum, the FISA Amendments Act was a particularly well calibrated piece of legislation.

With the FAA set to expire at the end of this year the Administration has strongly urged Congress to reauthorize the legislation. In supporting the Administration's call for reauthorization, I ask Congress to focus on the three considerations that have been the focus of my remarks here today: One, the vital importance of the FAA surveillance authority to our counterterrorism efforts; two, the extreme care with which Members of Congress considered, crafted, and limited that authority when they passed the FAA 4 years ago; and, three, the representations by the executive branch that that authority has been implemented to great effect and with full compliance with the law and the Constitution.

In addition, we must also focus on one other important consideration, which is the severity of the terrorist threat we still face today. While we have certainly weakened them in many ways, our terrorist adversaries are still intent on inflicting damage and death on the United States and its people. Given that reality, now is not the time to rest on our accomplishments, to weaken our defenses, or to scale back on a critical intelligence authority. To the contrary, now is the time to redouble our efforts, to press the advantage that we have gained, and to reauthorize the statute that has done so much to protect our people and their liberties over the past 4 years.

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

[The prepared statement of Mr. Wainstein follows:]

STATEMENT OF

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

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

THE REAUTHORIZATION OF
THE FISA AMENDMENTS ACT

PRESENTED ON

MAY 31, 2012

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

CONCERNING

THE REAUTHORIZATION OF
THE FISA AMENDMENTS ACT

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

MAY 31, 2012

Chairman Sensenbrenner, Ranking Member Scott and Members of the Subcommittee, 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, and it is a particular honor to be back here supporting the Act's reauthorization and discussing 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 have been at war with Al Qaeda and its terrorist affiliates around the globe, and we're making great progress against them. We have significantly degraded their operational effectiveness with our strike against their leadership, and we have succeeded in preventing a number of recent attack attempts – the best example being the Yemeni bomb plot that was foiled just recently.

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 Al Qaeda 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 an 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 communications streams of our terrorist adversaries. The government has taken a number of steps to enhance our electronic surveillance capacity over the past decade – refining our collection technologies and devoting more resources and manpower to the effort. But, the one development that has contributed most to that effort was Congress' decision to modernize our national security surveillance efforts with the passage of the FISA Amendments Act of 2008.

II. Background of the FISA Amendments Act

In 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.[1] 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 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

[1] 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 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 Surveillance Intelligence Act.

directed against persons within the United States and left the Intelligence Community free to surveil overseas targets without the undue burden of court process.[2]

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 location of target, location of interception and nationality of 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 by "radio." Given that "radio" (or 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 the 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.

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

---

[2] The report of the House Permanent Select Committee on Intelligence 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).

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. The statute amends FISA in the following three ways:

1. Approval Process for Surveillances of Foreign Persons Located Overseas

The most significant amendment 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. The government then 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 this 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 Surveil 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 that 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 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. Reauthorization of the FISA Amendments Act

With the FAA set to expire at the end of this year, the Administration has strongly urged Congress to reauthorize the legislation. In a recent letter to Congress the Attorney General and the DNI explain that the FAA "has proven to be an extremely valuable authority in protecting our nation from terrorism and other national security threats." They represent that the oversight of its implementation has been comprehensive, citing the findings of their semi-annual assessments that agencies have "continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the [FAA] requirements" and that agency personnel "are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States." And importantly, they conclude that the reauthorization of the FAA "is the top legislative priority of the Intelligence Community."

V. Conclusion

In supporting the Administration's call for 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 that authority when they passed the FAA four years ago; and (3) the representations of the Executive Branch that that authority has been implemented to great effect and with full compliance with the law and the Constitution.

In addition to these considerations, we must also focus on one other important consideration – which is the severity of the terrorist threat 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. Whether it is the continued attack planning by Al Qaeda and its associates or the recent threats emanating from within Iran, we are constantly reminded that our terrorist adversaries are still intent on inflicting damage and death on the United States and its people.

Given that reality, now is not the time to rest on our accomplishments, to weaken our defenses or to scale back on a critical intelligence authority. To the contrary, now is the time to redouble our efforts, to press the advantage that we've gained, and to reauthorize a statute that has done so much to protect our people and their liberties over the past four 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.

Mr. SENSENBRENNER. Thank you, Mr. Wainstein.
Mr. Rotenberg.

TESTIMONY OF MARC ROTENBERG, PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Mr. ROTENBERG. Mr. Chairman, Members of the Committee, thank you very much for the opportunity to testify today.

My name is Marc Rotenberg. I am Director of the Electronic Privacy Information Center. We are a nonpartisan research organization very much concerned about the government's use of electronic surveillance authority.

I am also the former chair of an ABA committee that looked at reform of the Foreign Intelligence Surveillance Act shortly after 9/11. The committee was fully aware of the threats to national security to our country and considered certainly the essential purpose of the FISA to enable the collection of important foreign intelligence information.

The committee made three recommendations to also ensure the protection of important privacy interests and constitutional interests of U.S. persons: Suggesting first that Congress had a critical oversight role to play—and in that spirit we are grateful for the hearing today; secondly, that data collection be focused so as to protect constitutional interests; and, third, I think of particular interest to the Committee this morning is a recommendation that the public reporting requirements for the use of the Foreign Intelligence Surveillance Act be expanded so that information would be available to the public on the use of FISA similar to the information that is available for the use of Title III criminal wiretap warrants. And my testimony this morning really focuses on the need to promote this type of transparency and accountability in the use of FISA authority.

Now, you may be aware that the administrative office of the U.S. courts publishes an annual report. It runs almost 200 pages. It details the use of wiretap authority in the United States for criminal investigations. It provides a great deal of information about the cost, about the effectiveness, about the jurisdictions that are using wiretap authority, as well as the number of incriminating and non-incriminating communications that are gathered.

Most critically, this report, which has been produced every year for over 30 years, provides only statistical data. It does not implicate any particular investigation. It does not reveal any details about ongoing investigations. It does, however, provide a basis for the public and for the Congress to evaluate the effectiveness and the use of electronic surveillance in criminal investigations.

The ABA recommended in 2033, and EPIC very much supports the view, that in your consideration of the FISA Amendments Act there should be greater public accountability for the use of these wiretap authorities. There is simply too little known today by the American public about the circumstances under which FISA authorities are used. And the problem has become somewhat worse because one of the key changes that was made in the FISA Amendments Act of 2008 was to authorize the use of warrants for categories of targets rather than particular individuals, raising significant constitutional questions but also calling into question the very

minimal reporting that currently takes place under the Foreign Intelligence Surveillance Act.

In our testimony, we suggest that a number of the internal procedures that have been established which provide from the Attorney General and from the Director of National Intelligence reports to you about the use of section 7 of the Act could be presented in such a way that they could be made available to the public with simply the statistical data about the use of the 702, 703, and 704 authorities. We think if this information were made available then the public would have more confidence about the use of FISA authority.

Now, Mr. Jaffer is going to speak in a moment, I know, about the case Clapper vs. Amnesty, which the Chairman mentioned a moment ago. The question that arises in that case is whether the American public has a well-founded fear that the FISA authorities might be misused, that they might be subject, in fact, to unlawful surveillance.

I think we have to say at this point without better public reporting we simply do not know. We simply do not know the circumstances under which FISA authorities are used. So we would recommend enhanced public reporting. We have additional suggestions as well that we think would improve oversight and transparency for the FISA Court of Review. There are checks there in the reporting to Congress, but the reporting to the public at this point is simply inadequate, and we would urge you to consider those changes before reauthorization.

Thank you.

[The prepared statement of Mr. Rotenberg follows:]

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on
"The FISA Amendments Act of 2008"

Before the

House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

May 31, 2012
2141 Rayburn House Office Building
Washington, DC

Introduction

Mister Chairman and Members of the Subcommittee, thank you for the opportunity to testify today regarding the reauthorization of Title VII of the FISA Amendments Act of 2008 ("FAA"). My name is Marc Rotenberg, and I am President of the Electronic Privacy Information Center ("EPIC"). I also teach Information Privacy Law at Georgetown University Law Center, and I am a former chair of the ABA Committee on Privacy and Information Security.

EPIC is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We work with a distinguished panel of advisors in the fields of law, technology, and public policy, and we have a strong interest in protecting the privacy of electronic communications. We have closely followed the developments of the Foreign Intelligence Surveillance Act ("FISA") and the Government's domestic and international surveillance activities. EPIC routinely reviews the annual reports concerning both Title III wiretap authority and FISA, and we have made recommendations to the Foreign Intelligence Surveillance Act Court of Review regarding that court's procedures.

We appreciate the Subcommittee's interest in the Foreign Intelligence Surveillance Act and its impact on important privacy interests.

Background

In my testimony today, I will review the key provisions of the FISA Amendment Act of 2008 ("FAA"),[1] discuss an important report from the American Bar Association ("ABA") on FISA reform, and make several recommendations to improve public accountability and oversight. In brief, I believe that requiring public dissemination of an annual FISA report, similar to reports for other forms of electronic surveillance, would improve Congressional and public oversight of the Government's information gathering activities. In addition, Congress should implement publication procedures for important decisions of the Foreign Intelligence Surveillance Court ("FISC"). At present, the FISA grants broad surveillance authority with little to no public oversight. To reauthorize the expansive provisions of Title VII of the FAA in their current form without improved transparency and oversight would be a mistake.

Passage of the FISA Amendments Act of 2008

The FISA Amendments Act of 2008, as adopted, clarified the legal basis for the use of electronic surveillance techniques by the Executive, but it also authorized surveillance of foreign communications, including communication of U.S. persons, on a mass scale without adequate public oversight. Among the achievements of the FAA was the recognition that federal statutes, such as FISA and ECPA, provide the exclusive authority for the Government's electronic surveillance activities. These statutory

[1] FISA Amendments Act of 2008, Title VII, 50 U.S.C. §§ 1881.

safeguards not only protect privacy, they also ensure the effective and efficient application of government resources to foreign intelligence gathering.

Section 702 of the FAA created new oversight mechanisms that require prior review the government surveillance and minimization procedures by the Foreign Intelligence Surveillance Court ("FISC").[2] The FAA prohibited surveillance of foreign targets as a pretext to conduct surveillance of persons within the United States, and added a new requirement of probable cause for surveillance of Americans abroad.[3]

However, section 702 of the FAA also gave the Government unprecedented authority to conduct electronic surveillance without first establishing probable cause to believe that a particular target was a foreign power or an agent of a foreign power. Instead, the FISC approves "certifications," submitted annually by the Attorney General and the Director of National Intelligence ("DNI"), which identify categories of foreign intelligence targets and describe minimization procedures and acquisition guidelines. The court's role in this process is merely to review the proposed procedures and guidelines, not to review the Government's actual surveillance practices. This procedure, which has the effect of a "rubber stamp," diminishes the independent role of the judiciary and leaves the executive with broad and minimally accountable collection authority.

Title VIII of the FAA also granted broad immunity to electronic service providers facilitating the Government's surveillance activities. This immunity was granted even though several alternative proposals would have provided adequate service provider protections for good faith compliance. While the companies were no doubt pleased to receive this broad immunity, the practical consequence was to further reduce the role of the courts and to diminish the opportunity for public oversight of FISA authorities.[4]

The 2003 ABA Resolution on FISA

Shortly after the attacks of September 11th, a special committee of the American Bar Association undertook an evaluation of the expanded use of the FISA, to ensure that Government conduct complied with constitutional principles while effectively and efficiently safeguarding national interests. The ABA report stressed the importance of both the Government's legitimate intelligence gathering activity and the protection of individuals from unlawful government intrusion. The ABA recommended that the Congress conduct regular and timely oversight, that FISA orders be sought only when the government has a "significant" foreign intelligence purpose, and that the Government

[2] 50 U.S.C. § 1881a.
[3] 50 U.S.C. § 1881b.
[4] This can be seen in the stark contrast between *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (denying phone company's motion to dismiss customer action for constitutional and statutory violations related to warrantless surveillance programs), *Hepting v. AT&T*, 539 F.3d 1157 (9th Cir. 2008) (remanding to the district court in light of the FISA Amendments Act of 2008), and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 671 F.3d 881 (9th Cir. 2011) (upholding challenge to FAA telecommunications providers immunity under the Due Process clause).

make available an "annual statistical report on FISA investigations, comparable to the reports prepared by the Administrative Office of the United States Courts pursuant to 18 U.S.C. § 2519."[5]

This ABA report is particularly useful as the Congress now considers whether to renew the FISA Amendments Act, and the specific recommendation to provide an annual public report on FISA should be adopted.

The Need for Improved Reporting on FISA

Mr. Chairman, for almost twenty years, I have reviewed the annual reports produced by the Administrative Office of the US Courts on the use of federal wiretap authority as well as the letter provided each year by the Attorney General to the Congress regarding the use of the FISA authority.[6] EPIC routinely posts these reports when they are made available and notes any significant changes or developments.[7]

The report of the Administrative Office is remarkable document. I believe it is the most comprehensive report on wiretap authority produced by any government agency in the world. Pursuant to section 2519 of Title 18, the administrative office works closely with prosecutors and federal courts to provide a detailed overview of the cost, duration, and effectiveness of wiretap surveillance.[8] The report also breaks requests down into

---

[5] American Bar Association, *FISA Resolution*, February 10, 2003, *available at* http://epic.org/privacy/terrorism/fisa/aba_res_021003.html.

[6] *See, e.g.*, Administrative Office of the US Courts, *Wiretap Report 2010,* http://www.uscourts.gov/statistics/WiretapReports/WiretapReport2010.aspx; Letter from Assistant Attorney General Ronald Weich to Joseph Biden, President, United States Senate, Apr. 30, 2012 ("2011 FISA Annual Report to Congress"), http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[7] *See* EPIC, *Title III Wiretap Orders: 1968-2010*, http://epic.org/privacy/wiretap/stats/wiretap_stats.html; EPIC, *Foreign Intelligence Surveillance Act*, http://epic.org/privacy/terrorism/fisa/; EPIC, *Foreign Intelligence Surveillance Court (FISC)*, https://epic.org/privacy/terrorism/fisa/fisc.html.

[8] Section 2519 of Title 18 provides in full:

§ 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) In January of each year, any judge who has issued an order (or an extension thereof) under section 2518 [18 USCS § 2518] that expired during the preceding year, or who has denied approval of an interception during that year, shall report to the Administrative Office of the United States Courts

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title [18 USCS §§ 2518(1)(b)(ii) and 2518(3)(d)] did not apply by reason of section 2518(11) of this title [18 USCS § 2518(11)]);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized hy the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

useful statistical categories, including the type of crimes involved.[9] Such information is critical to evaluating both the effectiveness and the need for various types of Government surveillance activities.

We might disagree over whether the federal government engages in too much or too little electronic surveillance, but the annual report of the Administrative Basis provides a basis to evaluate the effectiveness of wiretap authority, to measure its cost, to even determine the percentage of communications captured that are relevant to an investigation. These reporting requirements ensure that law enforcement resources are appropriately and efficiently used while safeguarding important constitutional privacy interests.

By way of contrast, the Attorney General's annual FISA report provides virtually no meaningful information about the use of FISA authority other than the applications

---

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In March of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts--

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In June of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter [18 USCS §§ 2510 et seq.] and the number of orders and extensions granted or denied pursuant to this chapter [18 USCS §§ 2510 et seq.] during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

[9] 18 U.S.C. § 2519(1)(c).

made by the government to the Foreign Intelligence Surveillance Court.[10] There is no information about cost, purposes, effectiveness, or even the number of non-incriminating communications of US persons that are collected by the government. Moreover, under the new procedures that authorize programmatic surveillance without a specific target, it is almost impossible to assess and compare the aggregate numbers since passage of the FAA. And while we acknowledge a 2006 amendment to the FISA reporting that now includes the numbers of National Security Letter requests made by the FBI concerning US persons, without more information it is very difficult to assess the significance of this number. Again by way of contrast, the reports prepared by the Department of Justice Inspect General concerning the misuse of NSL authority provide a great deal of information, but these reports are not prepared annually. So, while FISA authority remains in place and NSL authority remains in place, there is little information available to Congress or the public beyond the absolute numbers involved in the use of these authorities.

We recognize that section 702 contains internal auditing and reporting requirements. The Attorney General and DNI assess compliance with targeting and minimization procedures every six months, and provide reports to the FISC, congressional intelligence committees, and the Committees on the Judiciary.[11] The inspector general of each agency authorized to acquire foreign intelligence information pursuant to FISA must submit similar semiannual assessments. The head of each authorized agency must also conduct an annual review of FISA-authorized "acquisitions" and account for their impacts on domestic targets and American citizens.[12] Yet none of this information is made available to Congress or the public broadly, and no public oversight has occurred. There is simply no meaningful public record created for the use of these expansive electronic surveillance authorities.

Similar internal auditing procedures have failed in the past, and Congress would be wise to take the opportunity of the review of the FAA to establish more robust public reporting requirements and oversight procedures.[13]

The use of aggregate statistical reports has provided much needed public accountability of federal wiretap practices. These reports allow Congress and interested groups to evaluate the effectiveness of Government programs and to ensure that

---

[10] It is clear from the Attorney General's annual reports that FISC applications are routinely approved with very rare exceptions. *See Amnesty Int'l USA v. Clapper*, 638 F.3d 118, 140 (2d Cir. 2011) ("Empirical evidence supports this expectation: in 2008, the government sought 2,082 surveillance orders, and the FISC approved 2,081 of them."). Of the Government's 1,676 requests to the FISC for surveillance authority in 2011, none were denied in whole or in part. *See* 2011 FISA Annual Report to Congress, *supra*, note 6.

[11] 50 U.S.C. § 1881a(j)(1).

[12] 50 U.S.C. § 1881a(j)(3).

[13] The warrantless wiretapping program continued for several years because the government failed to routinely inform the Foreign Intelligence Surveillance Court of its activities. And the public was also kept in the dark. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec., 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html.

important civil rights are protected. Such reports do not reveal sensitive information about particular investigations, but rather provide aggregate data about the Government's surveillance activities. That is the approach that should be followed now for FISA.

Transparency is Necessary for Adequate Oversight: *Clapper v. Amnesty Int'l USA*

It is against this background that the Supreme Court recently decided to review *Clapper v. Amnesty Int'l USA*, an important case challenging the FAA. The question presented in *Clapper* is whether individuals who live in the United States and frequently communicate internationally have Article III standing to challenge the Government's surveillance activities pursuant to FISA based on a reasonable fear that their private communications are being intercepted.[14]

While some scholars have expressed sympathy for the government's position in *Clapper*, suggesting that it is too speculative to allow parties to sue when they have failed to establish that the surveillance occurred,[15] others have noted that the plaintiffs can likely establish the necessary "fear of future injury and costs incurred to avoid that injury" necessary under Article III.[16] Additionally, a lack of transparency or knowledge of the extent of government surveillance can have a severe chilling effect on protected speech and public activity. Individuals who are not reasonably certain that their communications will be private and confidential could be forced to censor themselves to protect sources and clients. This broad chilling effect is an injury in and of itself, regardless of the specific unlawful interception of private communications.

Given the lack of transparency and FISA reporting, it seems eminently reasonable for these individuals to fear unlawful interception of their private communications. In the absence of public reporting, similar to the annual reports provided for Title III Wiretaps, Americans are understandably concerned about the scope of surveillance pursued under the FISA.

The most obvious reason for this is that electronic surveillance is difficult to detect. Unlike physical entry into a home or the seizure of private property, electronic surveillance routinely occurs without any noticeable disturbance to the target or to innocent bystanders whose personal communications are intercepted. Federal Wiretap law traditionally addressed this problem by establishing Government notification requirements, once an investigation is closed, to those who had been the subject of surveillance.[17] These notification procedures helped ensure accountability. However,

---

[14] *See Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011), *reh'g denied*, 667 F.3d 163, *cert. granted*, 132 S. Ct. ____, 2012 WL 526046 (2012).

[15] Orin Kerr, *Amnesty International USA v. Clapper and Standing to Challenge Secret Surveillance Regimes*, Volokh Conspiracy (Mar. 24, 2011, 2:46 AM).

[16] Steve Vladeck, *Why Clapper Matters: The Future of Programmatic Surveillance*, Lawfare (May 22, 2012, 10:13 AM), http://www.lawfareblog.com/2012/05/clapper-and-the-future-of-surveillance/.

[17] *See* 18 U.S.C. § 2518(8)(d) (Wiretap Act notification provision); 50 U.S.C. § 1806(c) (FISA notification provision).

there has clearly been a move by the government, post 9/11, to move away from subject notification. In this respect, the FAA has done much to undermine the means of accountability that existed previously which helped ensure accountability

Congress should not reauthorize Title VII of the FAA without adequate transparency and oversight procedures in place.

The Need for Increased FISC Oversight Authority and Transparency

In addition to the Government's FISA activities, Congress should be concerned with the transparency of the FISC itself, and its authority to oversee Government surveillance procedures. Often referred to as a secret court, the FISC rarely publishes any substantive information regarding the cases and controversies that are heard by its judges; only a handful of written opinions have been released since the Court's inception, and little else, despite the potential for these types of Court documents to provide valuable guidance on the Court's purpose and function.

The public remains concerned by the secrecy that surrounds the FISC and its proceedings. The sensitive nature of the proceedings that come in front of the FISC must protect national security and provide notice to the individual targeted by the proceeding, at an appropriate time.[18] Currently, the FISC is only required to report on the number of orders it issues and denies: no other information accompanies the annual report and the public receives no other information about what cases come before the court each year. The only information currently available about the FISC on the U.S. Courts website is its adopted rules of procedure from November 2010.[19]

Any renewal of the FAA must take account of this lack of transparency and provide some assurance that the FISC can conduct sufficient oversight of Government surveillance activities. This could include public reporting procedures for FISC opinions, published statistics for FISC orders, and a provision for an increased web presence, or other source of data that can be easily accessed. It is important to provide the public with information about the Court, without compromising the government's security and intelligence gathering interests. Such information could include an overview of the Courts docket and the identity of the judge who is assigned to each case. The best way to increase public understanding of the FISC would be to publish past orders and opinions. Publishing such opinions while redacting sensitive materials would provide increased accountability for an important executive branch function.

---

[18] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806.

[19] *See* U.S. Foreign Intelligence Surveillance Court, *Rules of Procedure*, Nov. 1, 2010, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/FISC2010.pdf. *See also* EPIC, *Comments to Proposed Amended FISC Rules* (Oct. 4, 2010), http://epic.org/privacy/terrorism/fisa/EPIC%20Comments_FISC%202010%20Proposed%20Rules.pdf.

Conclusion

In the lead up to the passage of the FISA Amendments Act of 2008, there was much discussion of the need to "balance" national security and privacy interests. But the better way to understand the challenge facing Congress may be to think in terms of the need to establish a counter-balance. Where the government is given new authorities to conduction electronic surveillance, there should be new means of oversight and accountability. The FISA Amendments Act failed this test. There is simply too little known about the operation of the FISA today to determine whether it is effective and whether the privacy interests of Americans are adequately protected. Before renewing the Act, we urge the committee to carefully assess these new procedures and to strengthen the oversight mechanisms by (1) improving public reporting requirements, and (2) strengthening the authority of the FISA Court to review the government's use of FISA authorities.

Thank you again for the opportunity to testify today. I would be pleased to answer your questions.

Mr. SENSENBRENNER. Thank you very much.
Mr. Jaffer.

TESTIMONY OF JAMEEL JAFFER, DIRECTOR, CENTER FOR DEMOCRACY, AMERICAN CIVIL LIBERTIES UNION (ACLU)

Mr. JAFFER. Chairman Sensenbrenner, Ranking Member Scott, thank you for inviting me to share the ACLU's concerns about the FISA Amendments Act.

We urge you not to reauthorize the Act in its current form and not to reauthorize the Act in any form until the government discloses more about how the Act has been used. In essence, this Act allows the dragnet surveillance of Americans' international communications. Although it bars the government from intentionally targeting people who are overseas—inside the United States, it places virtually no restrictions on targeting people overseas, even if those targets are communicating with U.S. citizens and residents.

The Act's effect is to give the government nearly unrestricted access to Americans' international phone calls and emails. It permits the government to acquire those communications without requiring it to specify the people or facilities to be monitored, without requiring it to comply with meaningful limitations on retention, use, and dissemination, and without requiring it to obtain individualized warrants or even to make prior administrative determinations that the targets of government surveillance or foreign agents are connected in any way to terrorism.

The technology is more advanced now, but the Act authorizes what the framers would have described as general warrants. A single surveillance order can be used to justify the monitoring of millions of communications. It can authorize the acquisition of all phone calls to or from a country of foreign policy interest, Russia or Iran or Mexico, for example, including phone calls to and from U.S. citizens inside the United States.

To engage in that kind of surveillance the government would need to target people outside the United States. But in targeting people outside the United States it would collect countless Americans' private communications.

The Act also has dramatic implications for the freedoms of speech and association. The experience of other countries shows that these freedoms whither in an environment in which government surveillance is unrestrained. Thirty-five years ago, the Church Committee warned that unrestrained government surveillance threatened to undermine our democratic society and fundamentally alter its nature.

It would be irresponsible to disregard that warning. You should not reauthorize the FISA Amendments Act without prohibiting the dragnet surveillance of Americans' communications and more narrowly restricting the circumstances in which those communications can be retained, used, and disseminated.

And you should not reauthorize the Act in any form without first requiring the government to make public more information about its interpretation and use of the Act. The government has not disclosed its legal memos interpreting the Act, nor has it disclosed even in part any relevant opinions issued by the FISA Court. It has not disclosed the number of times the DNI and the Attorney Gen-

eral have invoked the Act, the number of Americans who have been unlawfully targeted, or the number of Americans whose communications have been collected in the course of surveillance nominally directed at people overseas.

Now, some of that information has been made available to some Members of Congress and the FISA Court, but there is no reason why this same information, redacted to protect intelligence sources and methods if necessary, should not be made available to the public and to all Members of Congress. The public surely has a right to know how the government interprets its surveillance authorities, and it has a right to know at least in general terms how those authorities are being used.

Further, Congress cannot responsibly reauthorize a surveillance statute whose implications for Americans' privacy the executive refuses to explain. The little that we do know about the executive's use of the Act is troubling. Records obtained by the ACLU show that the Act has been violated repeatedly. The New York Times reported in 2009 that the NSA had intercepted private email messages and phone calls of Americans, quote, on a scale that went beyond the broad legal limits established by Congress.

We strongly urge Congress not to reauthorize the Act in any form without first requiring the government to disclose more information about how the Act has been interpreted and used.

Thank you again for giving me this opportunity, and I look forward to hearing your questions.

[The prepared statement of Mr. Jaffer follows:]

Testimony of Jameel Jaffer
Deputy Legal Director of the
American Civil Liberties Union Foundation

Before
The House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

Oversight Hearing on
The FISA Amendments Act of 2008

May 31, 2012

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting me to testify before the Subcommittee. As you know, the FISA Amendments Act of 2008 will expire in December unless Congress reauthorizes it. For the reasons explained below, Congress should not reauthorize the Act without prohibiting dragnet surveillance of Americans' communications and strengthening minimization requirements, and it should not reauthorize the Act in any form unless and until the executive branch discloses basic information about how the law has been interpreted and used.

The FISA Amendments Act is unconstitutional because it allows the mass acquisition of U.S. citizens' and residents' international communications. Although the Act prohibits the government from intentionally "targeting" people inside the United States, it places virtually no restrictions on the government's targeting of people outside the United States, even if those targets are communicating with U.S. citizens and residents. The Act's effect is to give the government nearly unfettered access to Americans' international communications. It permits the government to acquire these communications:

- Without requiring it to specify the people, facilities, places, premises, or property to be monitored;

- Without requiring it to obtain individualized warrants based on criminal or foreign intelligence probable cause, or even to make prior administrative

determinations that the targets of government surveillance are foreign agents or connected in any way, however tenuously, to terrorism; and

- Without requiring it to comply with meaningful limitations on the retention and dissemination of acquired information.

Congress should not reauthorize the Act without prohibiting the dragnet surveillance of U.S. persons' communications and more narrowly restricting the circumstances in which Americans' communications can be acquired, retained, used, and disseminated.

Further, Congress should not reauthorize the Act in *any* form without first requiring the executive branch to make public more information about its interpretation and use of the Act. The executive branch has not disclosed to the public the number of times the Director of National Intelligence (DNI) and the Attorney General have invoked the Act, the number of U.S. persons who have been unlawfully targeted, or the number of U.S. persons whose communications have been collected in the course of surveillance nominally directed at non-U.S. persons outside the country.[1] It has not disclosed any legal memoranda in which the executive branch has interpreted the authorities granted by the Act; nor has it disclosed, even in part, any relevant opinions issued by the Foreign Intelligence Surveillance Court ("FISA Court"). Given the Act's implications for Americans' privacy rights, it is unacceptable that even this basic information is being withheld from the public and most members of Congress.[2] The secrecy surrounding the Act extends far beyond the executive's legitimate interest in protecting sources and methods.

The little that we do know about the executive's implementation and use of the Act is deeply troubling. Records obtained by the ACLU show that agencies conducting surveillance under the Act have repeatedly violated targeting and minimization procedures, meaning that they have improperly collected, retained, or disseminated U.S. persons' communications. At one point the FISA Court, apparently frustrated with the executive's repeated violations of the Act's limitations, ordered the Justice Department to provide reports every 90 days describing "compliance issues." The *New York Times* reported in 2009 that the National Security Agency (NSA) had "intercepted private e-mail messages and phone calls of Americans . . . on a scale that went beyond the broad

[1] The Director of Legislative Affairs for the Office of the Director of National Intelligence wrote last year that "it is not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the Authority of the [FISA Amendments Act]." Letter from Kathleen Turner, Director of Legislative Affairs, Office of the DNI, to Senators Ron Wyden and Mark Udall (July 26, 2011), *available at* http://bit.ly/LYC77M.

[2] Some of this information has reportedly been made available to the intelligence committees. There is no good reason, however, why this same information should not be made available to Congress more generally and to the American public – with redactions, if necessary, to protect sources and methods.

legal limits established by Congress," and that the "'overcollection' of domestic communications" was "significant and systemic."[3] We urge Congress not to reauthorize the Act in any form without first requiring the executive to disclose more information about how the Act has been interpreted and used.

I. FISA, the Warrantless Wiretapping Program, and the 2007 FISA Orders

In 1978, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the FISA Court and empowered it to grant or deny government applications for surveillance orders in foreign intelligence investigations.[4] Congress enacted FISA after the Supreme Court held, in *United States v. U.S. District Court*, 407 U.S. 297 (1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. FISA was a response to that decision and to a congressional investigation that revealed that the executive branch had engaged in widespread warrantless surveillance of U.S. citizens—including journalists, activists, and members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security."[5]

Congress has amended FISA multiple times. In its current form, the statute regulates, among other things, "electronic surveillance," which is defined to include:

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.[6]

Before passage of the FAA, FISA generally foreclosed the government from engaging in "electronic surveillance" without first obtaining individualized and particularized orders from the FISA Court. To obtain an order, the government was required to submit an application that identified or described the target of the surveillance; explained the government's basis for believing that "the target of the electronic surveillance [was] a foreign power or an agent of a foreign power"; explained the government's basis for believing that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power"; described the procedures the government would use to "minimiz[e]" the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons; described the nature of the foreign intelligence information sought and the type of communications that would be subject to

---

[3] Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 16, 2009, *available at* http://nyti.ms/LBPPrn.

[4] 50 U.S.C. § 1803(a).

[5] S. Rep. No. 95-604(I), at 6 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3909 (internal quotation marks omitted).

[6] 50 U.S.C. § 1801(f)(2).

surveillance; and certified that a "significant purpose" of the surveillance was to obtain "foreign intelligence information."[7] The FISC could issue such an order only if it found, among other things, that there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power."[8]

In late 2001, President Bush secretly authorized the NSA to inaugurate a program of warrantless electronic surveillance inside the United States. President Bush publicly acknowledged the program after *The New York Times* reported its existence in December 2005. According to public statements made by senior government officials, the program involved the interception of emails and telephone calls that originated or terminated inside the United States. The interceptions were not predicated on judicial warrants or any other form of judicial authorization; nor were they predicated on any determination of criminal or foreign intelligence probable cause. Instead, according to then-Attorney General Alberto Gonzales and then-NSA Director Michael Hayden, NSA "shift supervisors" initiated surveillance when in their judgment there was a "reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[9]

On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISA Court had effectively ratified the warrantless wiretapping program and that, as a result, "any electronic surveillance that was occurring as part of the [program] will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."[10] The FISA Court orders issued in January 2007, however, were modified in the spring of that same year. The modifications reportedly narrowed the authority that the FISA Court had extended to the executive branch in January. After these modifications, the administration pressed Congress to amend FISA to permit the warrantless surveillance of Americans' international communications in certain circumstances.

---

[7] *Id.* § 1804(a) (2006). "Foreign intelligence information" was (and still is) defined broadly to include, among other things, information concerning terrorism, national security, and foreign affairs.

[8] 50 U.S.C. § 1805(a)(2)(B).

[9] Alberto Gonzales, Attorney General, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19. 2005), *available at* http://bit.ly/JSLH4Z.

[10] Letter from Alberto Gonzales, Attorney General, to Senators Patrick Leahy and Arlen Specter (Jan. 17, 2007), *available at* http://bit.ly/JSMPWu.

II. The FISA Amendments Act of 2008

President Bush signed the FAA into law on July 10, 2008.[11] While leaving FISA in place for purely domestic communications, the FAA revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications. Under the FAA, the Attorney General and Director of National Intelligence ("DNI") can "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[12] The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," but an acquisition authorized under the FAA may nonetheless sweep up the international communications of U.S. citizens and residents.[13]

Before authorizing surveillance under § 1881a—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a "mass acquisition order").[14] A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year. To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court "a written certification and any supporting affidavit" attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "targeting procedures" reasonably designed to ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[15] The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "minimization procedures" that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4). Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information."[16]

---

[11] The FISA Amendments Act replaced the Protect America Act, which President Bush signed into law on August 5, 2007.

[12] 50 U.S.C. § 1881a(a).

[13] *Id.* § 1881a(b)(1).

[14] *Id.* § 1881a(a), (c)(2).

[15] *Id.* § 1881a(g)(2)(A)(i).

[16] *Id.* § 1881a(g)(2)(A)(iii)–(vii).

Importantly, the Act does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed.[17]

Nor does the Act place meaningful limits on the government's retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt "minimization procedures,"[18] that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[19] The Act does not, however, prescribe specific minimization procedures or give the FISA Court any authority to oversee the implementation of those procedures. Moreover, the FAA specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is "foreign intelligence information."[20] The phrase "foreign intelligence information" is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs.[21]

As the FISA Court has itself acknowledged, its role in authorizing and supervising FAA surveillance is "narrowly circumscribed."[22] The judiciary's traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FAA is simply to issue advisory opinions blessing in advance the vaguest of parameters, under which the government is then free to conduct surveillance for up to one year. The FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not supervise the implementation of the government's targeting or minimization procedures. In short, the role that the FISA Court plays under the FAA bears no resemblance to the role that it has traditionally played under FISA.

The FISA Amendments Act is unconstitutional. The Act violates the Fourth Amendment by authorizing warrantless and unreasonable searches. It violates the First Amendment because it sweeps within its ambit constitutionally protected speech that the

---

[17] *Id.* § 1881a(g)(4).

[18] *Id.* § 1881a.

[19] *Id.* §§ 1801(h)(1), 1821(4)(A).

[20] *Id.* § 1881a(e) (referring to *id.* §§ 1801(h)(1), 1821(4)(A)).

[21] *Id.* § 1801(e).

[22] *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), *available at* http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf.

government has no legitimate interest in acquiring and because it fails to provide adequate procedural safeguards. It violates Article III and the principle of separation of powers because it requires the FISA Court to issue advisory opinions on matters that are not cases and controversies.[23]

On behalf of a broad coalition of advocacy, human rights, labor, and media groups, the ACLU has raised these claims in *Clapper v. Amnesty International USA*.[24] In August 2009, the district court dismissed the Complaint on the grounds that the plaintiffs could not establish with certainty that their communications would be monitored under the Act, but in March 2010 the United States Court of Appeals for the Second Circuit reinstated the suit. The Supreme Court recently granted the DNI's petition for *certiorari*.[25]

Our concerns about the Act include:

a. The Act allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored.

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was

---

[23] In litigation, the government has cited *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008), in support of its argument that the FISA Amendments Act is constitutional. That decision, however, concerned surveillance that was individualized—i.e. directed at specific foreign powers or agents of foreign powers "reasonably believed to be located outside the United States." *Id.* at 1008. Moreover, while the Court of Review concluded that the surveillance at issue was consistent with the Fourth Amendment, it reached this conclusion only after noting that the surveillance had been predicated on probable cause and a determination of necessity and had been limited in duration. *See* Letter from ACLU to Hon. John G. Koeltl (Feb. 4, 2009), *available at* http://www.aclu.org/files/pdfs/natsec/amnesty/02_04_2009_Plaintiffs_Letter_re_In_Re_Directives.pdf.

[24] The plaintiffs are Amnesty International USA, Global Fund for Women, Global Rights, Human Rights Watch, International Criminal Defence Attorneys Association, *The Nation* Magazine, PEN American Center, Service Employees International Union, Washington Office on Latin America, and attorneys Daniel N. Arshack, David Nevin, Scott McKay, and Sylvia Royce. The Complaint and other legal filings are available at http://www.aclu.org/national-security/amnesty-et-al-v-clapper-legal-documents.

[25] Robert Barnes, *Supreme Court Agrees to Hear Case on Electronic Surveillance*, Wash. Post, May 21, 2012, *available at* http://wapo.st/KZSUWy.

also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court who it intends to target or which facilities it intends to monitor, and without making any showing to the Court—or even making an internal administrative determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, the Act allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

b. The Act allows the government to conduct intrusive surveillance without meaningful judicial oversight.

The Act allows the government to conduct intrusive surveillance without meaningful judicial oversight. It gives the FISA Court an extremely limited role in overseeing the government's surveillance activities. The FISA Court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is inaugurating any particular surveillance program. The FISA Court's role is limited to reviewing the government's "targeting" and "minimization" procedures. And even with respect to the procedures, the FISA court's role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time. Even at the outset of a new surveillance program, the government can initiate the program without the court's approval so long as it submits a "certification" within seven days. In the highly unlikely event that the FISA Court finds the government's procedures to be deficient, the government is permitted to continue its surveillance activities while it appeals the FISA Court's order. In other words, the government can continue its surveillance activities even if the FISA Court finds those activities to be unconstitutional.

c. The Act places no meaningful limits on the government's retention and dissemination of information relating to U.S. citizens and residents.

As a result of the Act, thousands or even millions of U.S. citizens and residents will find their international telephone and e-mail communications swept up in surveillance that is "targeted" at people abroad. Yet the law fails to place any meaningful limitations on the government's retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt "minimization" procedures—procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning

unconsenting United States persons." However, these minimization procedures must accommodate the government's need "to obtain, produce, and disseminate foreign intelligence information." In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is "foreign intelligence information." Because "foreign intelligence information" is defined so broadly (as discussed below), this is an exception that swallows the rule.

d. The Act does not limit government surveillance to communications relating to terrorism.

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather "foreign intelligence information." There are multiple problems with this. First, under the new law the "foreign intelligence" requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase "foreign intelligence information" has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the "foreign affairs of the United States." Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and e-mail that relates to the foreign affairs of the U.S. (Consider, for example, a journalist who is researching drone strikes in Yemen, or an academic who is writing about the policies of the Chávez government in Venezuela, or an attorney who is negotiating the repatriation of a prisoner held at Guantánamo Bay.) The Bush and Obama administrations have argued that the new law is necessary to address the threat of terrorism, but the law in fact sweeps much more broadly and implicates all kinds of communications that have nothing to do with terrorism or criminal activity of any kind.

e. The law gives the government access to some communications that are purely domestic.

The Act prohibits the government from "intentionally acquiring any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." The government itself, however, has acknowledged that, particularly with email communications, it is not always possible to know where the parties to the communication are located. Under the Act, the government can acquire communications so long as there is uncertainty about the location of the sender or recipient.

f. The Act has a chilling effect on activity that is crucial to our democracy and protected by the First Amendment.

The government's surveillance activities have implications even for those whose communications may never be acquired. Thus, in the debate before passage of the FAA, Senator Cardin observed:

> [F]ormidable, though incalculable, is the chilling effect which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with Governmental activities which effectively inhibit exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy within lawful limits, without having to sacrifice the expectation of privacy they rightfully hold. Warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.[26]

III. Implementation and Use of the FISA Amendments Act

Publicly available information about the executive's implementation and use of the FISA Amendments Act is very limited. The executive branch has not disclosed any legal memoranda in which the executive branch has interpreted the authorities granted by the Act; nor has it disclosed, even in part, any relevant opinions issued by the FISA Court. It has not disclosed to the public the number of times the DNI and the Attorney General have invoked the Act, the number of Americans who have been unlawfully targeted, or the number of Americans whose communications have been collected in the course of surveillance nominally directed at non-Americans outside the country.[27]

Some of this information has reportedly been made available to the intelligence committees and FISA Court, but there is no reason why this same information—redacted to protect intelligence sources and methods, if necessary—should not be made available to the general public. The public surely has a right to know how the government interprets its surveillance authorities, and it surely has a right to know, at least in general terms, how these authorities are being used. Further, Congress cannot responsibly reauthorize a surveillance statute whose implications for Americans' privacy the executive branch refuses to explain. Oversight by the intelligence committees is crucial,

---

[26] Cong. Rec. S574 (Feb. 4, 2008). *Cf.* Intelligence Activities and the Rights of Americans, Book II, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, S. Rep. No. 94-755, at 96 (1976) ("Unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature.").

[27] The Director of Legislative Affairs for the Office of the DNI wrote last year that "it is not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the Authority of the [FISA Amendments Act]." Letter from Kathleen Turner, Director of Legislative Affairs, Office of the Director of Nat'l Intelligence, to Senators Ron Wyden and Mark Udall (July 26, 2011), *available at* http://bit.ly/LYC77M.

but the last decade has confirmed that such oversight is not a substitute for oversight by Congress more generally or by the American public.

It is particularly important that Congress require the executive to disclose more information about its implementation and use of the Act because it is still unclear why the Act was necessary at all. As noted above, the Bush administration pressed Congress to amend FISA after the FISA Court issued orders in the spring of 2007 withdrawing or modifying January 2007 orders that had allowed the warrantless wiretapping program to continue in some form. These orders, however, have never been released.[28] Nor has the executive released all of the Office of Legal Counsel memoranda that were the basis for the program. Using the FOIA, the ACLU has learned that the OLC produced at least ten such memoranda. Of these, only two have been released, and one of the two is very heavily redacted.[29]

The limited publicly available information about the executive's implementation and use of the FISA Amendments Act supplies additional reason for concern. Using the FOIA, the ACLU has learned that multiple "assessments" conducted by the DNI and Attorney General between August 2008 and March 2010 found violations of the FAA's targeting and minimization procedures, indicating that the executive had improperly collected, retained, or disseminated Americans' communications. Some of the violations apparently concerned failures by the executive to properly assess "U.S. person status"—in other words, failures to afford U.S. persons the privacy protections that the Act mandates. At one point the FISA Court, apparently frustrated with the executive's repeated violations of the Act's limitations, ordered the Justice Department to provide reports every 90 days describing "compliance issues." The FOIA documents are heavily redacted, and accordingly it is difficult to draw firm conclusions from them. They strongly suggest, however, that the executive repeatedly collected, retained, and

---

[28] In August 2007, the ACLU filed a motion with the FISA Court requesting the unsealing of the January 2007 orders; any subsequent orders extending, modifying, or vacating the January 2007 orders; and any legal briefs submitted by the government in connection with the January 2007 orders or in connection with subsequent orders that extended, modified, or vacated the January 2007 orders. The motion requested that the Court make the materials public "with only those redactions essential to protect information that the Court determine[d], after independent review, to be properly classified." The FISA Court denied the motion. *In re Motion for Release of Court Records*, 526 F.Supp.2d 484 (FISA Ct. 2007).

In 2010, the Justice Department and DNI established a process to declassify FISA Court opinions that contained "important rulings of law," but the process has not resulted in the release of any opinion. *See* Steven Aftergood, *Move to Declassify FISA Court Rulings Yields No Results*, Secrecy News, May 29, 2012, http://www.fas.org/blog/secrecy/2012/05/fisa_null.html.

[29] The two released memoranda are available here: http://www.aclu.org/national-security/justice-department-memos-heavily-redacted-conceal-full-scope-bush-administration-s.

disseminated communications that it was not entitled to collect, and that at least some instances of overcollection involved the communications of U.S. persons.[30] In light of the documents, it is not surprising that the *New York Times* reported in 2009 that the NSA had "intercepted private e-mail messages and phone calls of Americans . . . on a scale that went beyond the broad legal limits established by Congress," and that the "'overcollection' of domestic communications" was "significant and systemic."[31]

IV. Recommendations

The ACLU recommends:

1. Congress should not reauthorize the FISA Amendments Act without prohibiting the dragnet surveillance of Americans' communications. Congress could effectively prohibit such dragnet surveillance in a variety of different ways. The ACLU is ready to work with Congress to develop a provision that respects constitutional rights while preserving the executive's legitimate interest in monitoring communications of suspected terrorists and foreign agents.

2. Congress should not reauthorize the FISA Amendments Act without strengthening minimization requirements—i.e. more narrowly restricting the circumstances in which Americans' communications can be acquired, retained, used, and disseminated.

3. Congress should not reauthorize the FISA Amendments Act in any form without first requiring the executive branch to disclose basic information about its implementation and use of the Act. Such information would include:

    - Statistics indicating how many times the DNI and AG have invoked the Act, how many U.S. persons have been inappropriately or unlawfully targeted, and how many U.S. persons' communications have been collected in the course of surveillance nominally directed at non-Americans outside the country

    - Any legal memoranda in which the executive branch has interpreted the authorities granted by the Act, and any FISA Court opinions interpreting the authorities granted by the Act.

    - The January 2007 FISA Court orders that reportedly allowed the warrantless wiretapping program to continue in some form, and the spring 2007 FISA Court orders that reportedly extended, modified, or vacated the

---

[30] The FOIA documents are available at http://www.aclu.org/national-security/faa-foia-documents.

[31] Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 16, 2009, *available at* http://nyti.ms/LBPPrn.

January 2007 orders.

- The OLC memoranda that were the basis for the warrantless wiretapping program.

To the extent these records reference intelligence sources and methods, the records could be released with redactions. Congress should not, however, allow the government's legitimate interest in protecting intelligence sources and methods from disclosure to serve as a pretext for denying the public basic information about government policy that implicates Americans' constitutional rights.

Thank you for giving us the opportunity to provide our views.

Mr. SENSENBRENNER. I want to thank all of the witnesses for staying within the 5-minute time limit.

The Chair will withhold his questioning and will start by recognizing the Chairman from California, Mr. Lungren, for 5 minutes.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Mr. Jaffer, do you have a problem with the FISA Court's competence in reviewing on an annual basis the procedures that are used by the intelligence community to conduct these programs, that is, that the programs have an annual review?

Mr. JAFFER. I do not think the question is one of competence. I think the question is one of the Court's jurisdiction and the Court's mandate. And here the question is, has the Court given—has the Court been given the authority to actually ask the government why it is engaged in this kind of surveillance, who its targets are, what kinds of communication——

Mr. LUNGREN. So your question is you do not know whether that is the case or you believe that that is not the case?

Mr. JAFFER. I don't think there is enough public information to know anything about the way the Court has acted or——

Mr. LUNGREN. So your statement that there is a failure to have an auditing process of the procedures they use that then leads you to talk about this being a dragnet is based on lack of sufficient information in the public domain to make that judgment, is that correct?

Mr. JAFFER. Well, there are two things. There is the statute itself which authorizes this kind of dragnet surveillance, and the Obama administration has not disagreed with that.

Mr. LUNGREN. I do not think they call it "dragnet", but go ahead.

Mr. JAFFER. Well, they did not use that word, but they did say that this statute can be used for nonindividuals——

Mr. LUNGREN. What I was trying to understand is you said there is no auditing process. In fact, there is a requirement that the Court must review these programs—these specific programs on an annual basis in addition to the specific applications that are requested by the Court in particular cases.

Mr. Wainstein, could you reflect on that, based on your prior experience?

Mr. WAINSTEIN. The competence of the Court, sir?

Mr. LUNGREN. Yeah. And whether they do in fact ask these kinds of questions. I mean, I could tell you what I know from classified briefings and what we have seen, but your experience on that.

Mr. WAINSTEIN. Thank you for the question, sir.

I was the Assistant Attorney General for National Security and so I was sort of on point with my folks in dealing with the FISA Court for the time I was in that position, and I can tell you from personal experience they are very active. They are Federal judges. They are used to asking questions and getting answers to those questions. And they take their responsibility very seriously—their responsibility being their oversight responsibility.

So when you go in—I mean, there are routine orders that you apply for and get, and that is just sort of like any Federal judge who issues search warrants. They base their decision on the facts that you present to them. But they also have the broader purpose

of making sure that the program is being run responsibly, and they ask the tough questions.

And I cannot speak from personal experience about their oversight under the FAA, because that happened after I moved out of that position, but I can tell you, knowing those judges, that they are being very aggressive in asking the questions about making sure that the targeting procedures are well designed and they are being well applied to minimize the instances where there might be mistakes and people within the United States end up getting swept into that.

Mr. LUNGREN. And, Mr. Rotenberg, it is a fact that those of us in Congress who serve on the Judiciary Committees and the Intelligence Committee have the ability to look at the documents and the decisions made by the Court, both in terms of the general review of programs and any decision made by the Court that has a significant legal issue. Is your problem that that is limited to just those Members of Congress—although I believe if another Member of Congress asked the Chairman of either Intelligence or Judiciary it would be up to the Chairman of either of those Committees to make that decision. But is it your objection that that is too limited and that those of us on these Committees either do not have the competence or that it should be expanded, that other Members have it, or that the public should have that information as well?

Mr. ROTENBERG. Well, I think it is the latter, Mr. Lungren. I mean, clearly, it is an important oversight mechanism that you do have access to this information, and we fully support that. But we also do think that the public could be provided with statistical reports. It is something that has been done routinely over the years for Title III.

And going back, of course, to the history of the warrantless wiretapping program, part of the reason that the oversight mechanism broke down and the FISA Court itself was not informed about the activities the government was engaged in, because there were not enough routinized reports that were put in place.

So we are certainly not questioning the competence of the Court or the oversight committees. We are saying that this additional safeguard that would give the public the opportunity to have a general picture of this very important government function would be helpful.

Mr. LUNGREN. I appreciate that, and I understand the different positions here. I would just stress that this is an independent Court. It is made up of regularly sitting Federal judges. There is a review Court as well, and those of us in the Congress who serve on these Committees have access to any major decision made by the Court as well as these annual reviews done by the Court.

Mr. SENSENBRENNER. The time of the gentleman is expired.

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you. Thank you, Mr. Chairman.

Mr. Jaffer, you indicated that you could target emails if they are sent overseas. You can pick up emails anywhere. How do you know that an email has been sent overseas?

Mr. JAFFER. Thank you for the question.

So this is actually one of the questions that I think Congress should try to get to the bottom of. Because it really is a concern

that the Act forecloses the government from targeting people who are known to be in the United States. In a lot of instances, you do not know. You do not know where a person is. You do not know where the communication is coming from or going to. And under this statute the government has the authority to pick up those kinds of communications. That is one of our concerns about the Act.

Mr. SCOTT. You talked about nonindividualized as technology allows you to get a whole lot of information. Should there be a difference between getting information and then what you do with it after you get it, what sort, select and search kind of things?

Mr. JAFFER. Absolutely. I think that is exactly—you have to divide this into two questions. There is a front-end question of what the government should be permitted to pick up in the first instance, and then there is a back-end question about what the government can do with what it has picked up.

I think on the front end—and this goes to Mr. Lungren's questions, too—it is important to recognize that the Court's role here is very, very limited. This is not like a search warrant—a traditional search warrant process in which the Court is presented with evidence about a particular target, some justification for wiretapping that target.

This is a system in which the FISA Court reviews broad programs. The only question that the FISA Court asks is whether the program as a whole has as its significant purpose gathering foreign intelligence information and whether the targets are overseas. But, again, targets overseas very commonly speak to people inside the United States, and it is those communications that we are worried about here.

Mr. SCOTT. Well, you said "the" significant purpose. It is "a" significant purpose. In response to a question I asked the former attorney general, it is just a significant purpose and not the primary purpose, what could the primary purpose do. And we have some of these joint task forces where you may have an intelligence official sitting up there and others who are restrained by criminal warrant standards where they need real probable cause that a crime is being committed in evidence and the foreign intelligence standard which means that it is relevant to foreign intelligence which could be about anything.

In response to a question, what could the primary purpose be if it is not foreign intelligence, you said it could be a criminal investigation, which means you are doing a criminal investigation on a much different standard. Should we change a significant purpose back to the primary purpose, the way it was before the early 2000's?

Mr. JAFFER. I think that that would be a great thing to do.

I think that there are a few other things that you should consider doing as well. One is foreclosing dragnet surveillance of Americans' communications, and there are a variety of ways to do that, and a variety of proposals have already been made.

And then the other is—and you were alluding to this, Mr. Scott—strengthening the minimization requirement. So even if Congress decides that it is in the interest of the country to give the government unfettered access to Americans' international communications in the first instance, there is still the question what can the gov-

ernment do with those communications once acquired, and there are ways to strengthen minimization to ensure that Americans' privacy is protected.

Mr. SCOTT. Thank you.

Mr. Wainstein, you indicated the comparison between in FISA Courts the search warrants and how the Court has to go through a process. The difference between search warrants in a criminal case and the FISA warrant is that search warrants eventually become public so the public can see what is going on. What kind of information should be made available to the public so that we can have confidence that the program is being run appropriately?

Mr. WAINSTEIN. Ranking Member Scott, that is a very good question. And the concern about transparency and public knowledge of any national security program is a very serious concern. Because the more knowledge the public has the more confidence they have that an authority is being responsibly exercised. So that is an important concern.

I will say that when it comes to FISA Court operations they are the most sensitive of the sensitive operations in our national security apparatus. And, recognizing that, FISA, the statute itself, decided appropriately to give that insight into—for Congress. So Congress gets reports on a regular basis about all the orders that are issued by the FISA Court, can ask questions about the program, can bring members of the executive branch up and quiz them about, in closed session, about classified information. And that is the balance. That is the balancing that provides the representatives of the people with insight into a very classified world but also does not divulge important secrets.

Mr. SENSENBRENNER. Okay. Thank you very much.

The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, sir.

I think our discussion so far this morning brings us to this issue: Can and should we get more information in the process of reauthorizing FISA? And with the exception of the former attorney general of California on the Committee I think everybody that I have heard thinks that there is nothing wrong with getting a little bit more information so that we know what is happening. Would you say that is a fair opinion to hold at this point, Mr. Wainstein?

Mr. WAINSTEIN. I would say in theory, as a matter of principle, more information to the public is better, all things being equal. However, in this area where you are talking about intelligence officials coming into the FISA Court, laying out the most sensitive information about sources and methods——

Mr. CONYERS. Well, we did not say—I do not want to do that either. So I agree with you. We do not want to throw out sensitive information. That is why I said this is a somewhat tricky sensitive kind of a discussion we are having. Let us agree that we do not want to do that, and I would never rationalize doing it.

What do you think, Mr. Rotenberg?

Mr. ROTENBERG. I think it is a very good approach, Mr. Conyers. If nothing else, it will give us more information to evaluate the effectiveness of the program. Certainly in looking at the annual wiretap report we get very useful information. It shows us strengths

and weaknesses and where government authorities maybe need to be enhanced, and I think that would help here.

Mr. CONYERS. After all, we want to improve the laws. I know you are very generous in your compliments about the Congress acting on this originally. But for goodness sake, just to okay it again because we did it before—couldn't we improve it a little bit?

What about minimization, Mr. Jaffer? Doesn't that require a little more carefulness?

Mr. JAFFER. I think it does, Mr. Conyers.

The way that minimization works right now, the government is required to minimize only insofar as the information obtained is not foreign intelligence information. But foreign intelligence information is defined extremely broadly. And so anything—any communication about, for example, foreign affairs is one that the government under the statute can disseminate.

And Americans talk about foreign affairs all the time, over the phone, in emails. And I think it is unacceptable to say to Americans that when you are communicating about foreign affairs in an email that is something that the government can have access to, even if you have never done anything wrong and even if the person you are talking to is not believed to have done anything wrong.

But, Mr. Conyers, if I could just say one more thing about the transparency point that you raised. There is precedent for the release of FISA Court opinions with redactions. The FISA Court released an opinion in 2002 about the significant purpose amendment. The FISA Court of Review released an opinion in 2003 about that same amendment. In 2008, the FISA Court of Review released another opinion about the Protect America Act.

So there is precedent for the release of legal reasoning in these opinions with the redaction of legitimate sources and methods, and I think everybody is in agreement that some information in these opinions is likely to be sensitive and the government has a legitimate interest in keeping that information secret. But it is a different story when what the government is keeping secret is legal reasoning.

Mr. CONYERS. Professor Rotenberg, let me close with this observation. We have been told that we cannot even tell how many people are being subjected to this process located in the United States and that we do not know and they cannot tell us. And I think we could get a little bit closer. There could be some reasonableness there to give——

You know, it is this kind of vagueness that creates in those of us in the Congress suspicions that are negative rather than suspicions that are positive. We do not know and we cannot be told basic information like this.

Mr. SENSENBRENNER. The gentleman's time is expired.

Mr. CONYERS. Do you mind if he responds?

Mr. SENSENBRENNER. The witness will respond.

Mr. ROTENBERG. Well, I agree of course, Mr. Conyers.

As I said in my statement, I think when you create authorities for the government you need to create a counterbalance of oversight. And the problem with the FISA Amendments Act of 2008 that actually went quite far with new surveillance authorities, in

our view, these means of public oversight do not match the authorities.

Mr. SENSENBRENNER. The gentlewoman from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair.

Mr. Jaffer, in your testimony you mentioned the New York Times article which revealed that the National Security Agency had intercepted private emails and phone calls of Americans. You stated that the ACLU had obtained records showing that agencies conducting surveillance under FAA have improperly collected, retained, or disseminated U.S. persons' communications. Could you talk more specifically on the kinds of information that the ACLU obtained?

Mr. JAFFER. Sure. Thank you for the question.

The ACLU filed Freedom of Information Act litigation a few years ago to find out how the statute had been implemented. And all of the records are now—we have made them available on our Web site. But the records show, among other things, that the government has repeatedly violated minimization and targeting rules, and at least some of those violations resulted in the collection of Americans' communications. There have also been violations of the targeting restriction against directing surveillance in Americans. So, in some cases, Americans have been targeted inappropriately and unlawfully.

There was also at least one occasion in which the FISA Court apparently got so frustrated with the executive's repeated violations of the Act that the Court ordered the Justice Department to provide reports every 90 days to explain compliance issues.

On the one hand, I think that is a sign that the FISA Court sometimes does have the authority to do what we want it to do. On the other hand, it raises real concerns about whether we can trust the executive branch to police these limitations; and I think that we have at least enough information now to warrant Congress asking more questions and certainly to warrant pausing before reauthorizing the statute in its current form.

Ms. CHU. Do you believe that there is any legislative remedy to this—to address the fears that Americans have that they are being subjected to warrantless surveillance?

Mr. JAFFER. Absolutely. I think that when this Act was first proposed by the Bush administration the main problem that the Bush administration identified was that they believed that they could not wiretap foreign-to-foreign communication—so communications between non-U.S. persons—without getting a warrant, because some of those communications were running through the United States.

And nobody is making the argument that we should revert to a world in which the government has to get a warrant for those kinds of communications. What we are talking about is something relatively narrow here. What we are asking for is a fix that prevents the government from engaging in suspicionless dragnet surveillance of Americans' international communications, and there are a variety of ways in which Congress could make that fix.

Ms. CHU. Mr. Rotenberg, how rigorous is the certification process of the Attorney General and the Director of National Intelligence

regarding the authorization of a surveillance program under Title VII of FISA? Has the FISA Court ever rejected an application under Title VII?

Mr. ROTENBERG. Well, that is a very good question, Congresswoman, and I could not answer because the information is not made available to the public.

There are statutory provisions as to the contents of the report that are made available to your Committee. But here is the information that is made available to the public about the use of the Foreign Intelligence Surveillance Act. It is a two-page letter. It is sent at the end of April every year from the Attorney General to the Speaker and to the President of the Senate. And this is what we know about the use of FISA authority.

So in recommending that more information be made available to the public about the use of FISA we are suggesting in part it would make it possible to evaluate the adequacy of the oversight techniques.

They may be working, by the way. I am not suggesting that there is a competency or a systemic problem here. But you see it is a small number of people that have access to this information and it takes time to evaluate.

Ms. CHU. In exigent circumstances the FAA allows the government to conduct electronic surveillance for 7 days without even making an application to the FISA Court. What is the standard for exigent circumstances and who gets to decide when that standard applies?

Mr. ROTENBERG. Well, I mean, that is also set out in the statute, and that is actually consistent with other provisions in similar surveillance authorities.

So certainly there will be circumstances, for example, where the government needs to undertake a search. It believes that it does not have time to obtain the Court authority. It can go forward with the search. But it is quite important, actually, that the statute requires the government to come back later and make the application that is required; and if they cannot get approval for the application, then the surveillance activity is suspended. And, again, the requirements for that are set out in the statute.

Ms. CHU. Thank you. I yield back.

Mr. SENSENBRENNER. The gentleman from Colorado, Mr. Polis.

Mr. POLIS. Thank you, Mr. Chairman.

My question is for Mr. Jaffer. The first question, in your testimony you mention your concern that the Administration is conducting "bulk collection" of American communications. I was hoping you could explain that term and kind of the evidence that you have that this is occurring.

Mr. JAFFER. Well, when the Bush administration proposed the statute, they explained that one purpose of the statute was to allow for bulk collection, meaning nonindividualized collection. In that kind of situation, the government does not go to the Court and say we want to target this specific person. Instead, it goes to the Court and says we want to target people overseas generally. Maybe we want to target everybody in this particular city or we want to target everybody in this particular country.

Mr. POLIS. So, to be clear, they could be like every email from Karachi or something like that, hypothetically.

Mr. JAFFER. Or Mexico, right, absolutely.

Mr. POLIS. And do you have any evidence that this is occurring?

Mr. JAFFER. Well, this is something that came up in Clapper vs. Amnesty, the case that we are litigating right now, involving this Act. And the Administration was asked this question—the Obama administration was asked this question by the Southern District and then again by the appeals court. And the Administration had an opportunity to say that this is not how the Act is being used, and it declined to take that opportunity.

Mr. POLIS. Now, presumably, if used for bulk collection, there would be enormous amounts of resulting data. Do we—or is there any public knowledge about how that data might even be gone through or what safeguards might be in place to prevent inappropriate use of personal data unrelated to a threat from that data?

Mr. JAFFER. Well, we have the statute, and the statute does lay out in broad terms what safeguards have to be put in place. And our concern is that those safeguards are too weak.

One of the concerns is that the definition of foreign intelligence information is so broad that minimization applies only to a subcategory of the most sensitive information. And the result is that Americans' communications about things like foreign affairs can be disseminated, analyzed, retained forever without really any other safeguard.

And that is a concern not just from a privacy standpoint but from a First Amendment standpoint as well. Because, as I said in my introductory remarks, this kind of surveillance has a chilling effect on activity that is not just protected but is sort of necessary to our democracy.

Mr. POLIS. Now, many proponents also say that any issues that arise under it can be dealt with by Federal judges who actually approve the FAA applications, and I wanted to question you about how effective that has been. How effective has the role of Federal judges been in administering the FAA and are there any specific recommendations for improving the ability of judges to administer the FAA?

Mr. JAFFER. Thank you for that question. I think that is an important question.

So I guess there are two separate parts of this. One is the FISA Court itself. And I think, as Mr. Rotenberg has pointed out, part of the problem is we do not know precisely what is going on or even in the most general terms what is going on in the FISA Court. And we think it is important that some of the FISA Court opinions relating to the FAA be released, at least in redacted form.

But then—and this goes to something that Chairman Sensenbrenner said right at the beginning—it is true that no other Federal Court has weighed in on the constitutionality of the FAA and no Court has found any provision of the FAA to be unconstitutional. But that is because the Administration, first the Bush administration now the Obama administration, have insulated the FAA from judicial review. And they have done that by saying to plaintiffs that the only people who can challenge this kind of surveillance are people who can show that their own communications

have been monitored. And obviously nobody can show that their own communications have been monitored, because that is not information that the Administration has released.

So you are in this situation where this extremely far-reaching surveillance statute, definitely the most far-reaching surveillance statute ever enacted by Congress, is essentially beyond the reach of the courts, and that I think is a problem in itself.

Mr. POLIS. And I think from your description it sounds like one of the issues is there is insufficient standing to bring it to Federal Court. So one legislative improvement might be to define standing in such a way that you do not have to know something that by its very nature you do not know about yourself. So there might be others or some that therefore have standing to get it to Federal Court. Is that the issue you identified?

Mr. JAFFER. I think that would be an improvement to the law.

That said, we believe we have standing in the case that we are litigating before the Supreme Court, and the Second Circuit agreed with us.

Mr. POLIS. But you believe that there is still this issue with regard to standing; and, as you said, it is something by very nature people do not know about themselves would be the ones who would have to object.

Thank you, and I yield back.

Mr. SENSENBRENNER. The gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON. With respect to the Director of National Intelligence, what is the relationship between that office and the other—I believe it is—what—26 intelligence-gathering agencies within the U.S. Government? What is the relationship, Mr. Wainstein.

Mr. WAINSTEIN. Well, Congressman Johnson, the Office of the Director of National Intelligence was established sort of to be the "quarterback of the intelligence community" so the DNI, the Director of National Intelligence, sets the requirements for the Intelligence Community, the collection requirements, and provides oversight in a number of ways. And in this particular process the DNI plays a critical role, because, as you know, the Director of National Intelligence and the Attorney General have to jointly certify to these collections and certify that they are being done legally and constitutionally.

Mr. JOHNSON. Certainly. But DNI is pretty much the quarterback for all of the other intelligence agencies within the Federal Government. How many are there, about 26 of them?

Mr. WAINSTEIN. Sixteen, right? I am forgetting, but I want to say 16.

Mr. JOHNSON. Sixteen, okay. That might be good.

But now the process is—16?

Mr. WAINSTEIN. I am getting nods from the audience, 16.

Mr. JOHNSON. The process is that the intelligence community uses or the tools that are used to conduct surveillance are products from defense contractors and intelligence agency contractors; is that correct?

Mr. WAINSTEIN. A lot of the technology is worked on by contractors as well as people within the intelligence community, yes.

Mr. JOHNSON. And I suppose there are some firewalls between the various intelligence agencies, but perhaps not. What do you think about that?

Mr. WAINSTEIN. Firewalls for the passage or the conveying of information?

Mr. JOHNSON. Yes.

Mr. WAINSTEIN. Actually, one of the major efforts since 9/11 has been to take down the stovepipes and the walls between these different agencies. And there are—obviously, for sensitive information there are limitations on dissemination, et cetera. But the focus of the DNI has been to try to make sure that everybody gets the information they need to do their job.

Mr. JOHNSON. Certainly.

Well, tell me this now. Does the intelligence community have the technological capacity to identify Americans based upon the content of their electronic communications?

Mr. WAINSTEIN. That is actually a very good question; and, obviously, I can't get into classified techniques that they use to identify communicants——

Mr. JOHNSON. But they do have that capability, wouldn't you agree?

Mr. WAINSTEIN. My understanding is they have the capability to an extent.

But keep in mind when you try to identify a communication like a telephone call, just in our own experience, you look at—you know, if you try to figure out whether the person is American or not you might look at the phone number, you might try to ask the person on the phone. I mean, you might listen to the content to determine whether they are talking about being overseas or not. There is not sort of one set of indicia that definitively identifies every communication being overseas.

Mr. JOHNSON. I have a hard time getting a good answer for that question.

Tell me, what I would assume that we do have the ability to identify Americans based upon the content of their electronic communications. I would assume that we would be able to do that. But I can't get anyone to admit that we do have that capability, not that we do it but we have the capability, and that causes me a lot of suspicion.

And I tell you, with the Chamber leaks problem that came out a couple of years ago, where a couple of defense contractors were making a proposal to the U.S. Chamber of Commerce to use information gleaned from these processes that they have developed to spy on and disrupt and destroy opponents of the U.S. Chamber of Commerce, I am concerned about that.

I am concerned about the recent USA Today situation where reporters reporting on a defense contractor engaged in propaganda actions. We are targeted by persons in that company, in that defense company. Subcontractor.

Mr. Jaffer, how would you add to this.

Mr. JAFFER. Mr. Johnson, I think that you are absolutely right to be worried about the way that these powers will be used. If you look at the way that similar powers were used before FISA was enacted, there were all kinds of abuses. There were Members of Con-

gress who were wiretapped. There were journalists who were wiretapped. There were Supreme Court justices who were wiretapped. There was a Member of Congress whom the NSA sought to wiretap in 2006 or 2007. That is in the same New York Times story that we referred to earlier.

I think that history shows us that these kinds of broad surveillance powers can and will be abused, and that is part of the reason why you need to set out limits now to make sure that that doesn't happen.

Mr. SENSENBRENNER. The gentleman's time has expired.

The gentleman from Tennessee, Mr. Cohen.

Mr. COHEN. Thank you, sir.

I want to follow up with the article. I must have missed that one. You say it revealed that they had been listening in on conversations of judges.

Mr. JAFFER. That Church Committee report—yes, the Church Committee report goes into some detail about that. That was back in——

Mr. COHEN. The '70's.

Mr. JAFFER. That is right.

Mr. COHEN. We don't have any knowledge of any current?

Mr. JAFFER. No.

Mr. COHEN. Okay. I tuned in a little late, and 40 years is a long time.

Mr. JAFFER. No. The current evidence is of wiretapping a Member of Congress, and all I know about that is from the Eric Lichtblau story that several of us have already referred to.

Mr. COHEN. And who was the Member?

Mr. JAFFER. I don't know.

Mr. COHEN. What was revealed about the purpose of which they wiretapped the individual or what they learned or was anything revealed?

Mr. JAFFER. All I know is from that story. The story reports that a Member of Congress was traveling overseas somewhere in the Middle East and the NSA sought the authority to wiretap the conversations of that Member. I don't know if they actually got that authority. There are just three or four sentences in the New York Times story.

Mr. COHEN. How much is available for us to know about the dealings of the FISA Court as far as applications denied, basis for denial? Is any of that available?

Mr. JAFFER. Almost nothing is available. The only thing that is available is this raw number, number of applications filed with the FISA Court and number of applications granted or denied. And even that number doesn't break down between traditional FISA and the FISA Amendments Act.

So you don't know how many programs of surveillance have been authorized. You don't know how many have been approved by the Court. You don't know how broad those programs have been. You don't know how many Americans have been wiretapped as a result. And you don't know what has been done with the communications that have been acquired. So that all sorts of, in our view, crucial facts are still being withheld at least from the public.

And then, on top of that, there is this question of the legal authority.

So this is a complicated statute, and there are legitimate questions about how it ought to be interpreted. We don't know how the Obama administration is interpreting this statute, because it hasn't disclosed even in redacted form the Office of Legal Council memos. And we don't know how the FISA Court has interpreted the statute, because we don't have, even in redacted form, the FISA Court's opinions.

I should have said this earlier, but there was a process put in place a couple of years ago by the Obama administration to declassify other FISA Court opinions, and there was a recognition on the part of the Obama administration at that time that more of these opinions needed to be released, that the public had a right to know more about how that Court was interpreting the law.

Two or 3 years later, the result of that process is the release of no FISA Court opinions. We still don't have anything out of that process, and it is not clear to us why nothing has come out of that process. It might be something that the Committee could consider looking into.

Mr. COHEN. Thank you, sir.

I yield back the remainder of my time.

Mr. SENSENBRENNER. Before recognizing the gentleman from South Carolina, I notice that the gentlewoman from Texas, Ms. Jackson Lee, was in the room and stepped out, and I will recognize her following the conclusion of the gentleman from South Carolina's questioning. But I intend to be the last questioner, so I would ask the Democratic staff, if she wishes to ask questions, to have her brought back in the room.

The gentleman from South Carolina, Mr. Gowdy.

Mr. GOWDY. Thank you, Mr. Chairman.

Mr. Jaffer, you made reference to the Clapper case. I don't have my notes in front of me. What was the breakdown of the en banc?

Mr. JAFFER. It was six-six on the en banc. In total, eight judges agreed that our plaintiffs had standing, and six disagreed. But two of the judges——

Mr. GOWDY. I thought it was six to six. It just threw me off when you said the Second Circuit agreed with you. I thought it was six to six, which some people claim ties as victories and some people don't. I guess if you prevailed on the three-judge panel then you are entitled to claim victory of a six-six tie.

Mr. JAFFER. It was three-zero on the panel, and the full Court decided not to rehear the case. There were actually eight judges, though, who agreed with us of the full Court. Two of them didn't participate in the en banc.

Mr. GOWDY. Well, let me see if you and I can agree on something. Does the Fourth Amendment apply to foreign targets in foreign lands?

Mr. JAFFER. I don't think that is the question presented by——

Mr. GOWDY. No, no, no. That is my question. So I promise you it is the right question, because that is my question. Does it apply?

Mr. JAFFER. I don't think it does.

Mr. GOWDY. When you say you don't "think" it does——

Mr. JAFFER. Well, in the circumstances of this statute, I don't think it does. We certainly haven't made the argument that it does.

Mr. GOWDY. Does the Fourth Amendment—I am not talking about a statute. I am talking about does the Fourth Amendment apply to foreign nationals in foreign lands?

Mr. JAFFER. It does not.

Mr. GOWDY. Does the Second Amendment apply?

Mr. JAFFER. I don't know the law, but I think no.

Mr. GOWDY. The First? Eighth?

Mr. JAFFER. I think it would depend on the circumstances.

Mr. GOWDY. Women's suffrage? Does that apply?

Mr. JAFFER. No.

Mr. GOWDY. That is my point. They don't. So we are not talking about surveillance of foreign nationals in foreign lands, right? You don't think there is a constitutional——

Mr. JAFFER.—American communications——

Mr. GOWDY. That is my second point. If you will let me get to it. If you will let me get to it.

Professor Rotenberg was quoted—and it would not be the first time somebody's been quoted incorrectly, so I am going to give you a chance to say if you were quoted incorrectly—that there was a constitutional problem with monitoring foreign targets, and I am trying to understand what that constitutional problem might be of foreign targets in foreign land. Or the third alternative is that you were quoted incorrectly.

Mr. ROTENBERG. Well, Congressman, I am not quite sure of the context, but I am sure the concern I have was the constitutional problem was in the targeting of a foreign target in a foreign land. You would also acquire the communication of a U.S. Person.

Mr. GOWDY. Which leads to my next question. In a domestic setting, Title III, where there is an unintentional interceptee, does that unintentional interceptee have standing?

Mr. ROTENBERG. Probably not. I mean, there certainly wouldn't be a suppression motion if the person is not the target. However—and this goes actually to my recommendation before the Committee—you would have a great deal of information about the percentage of communications in the course of an investigation that were non-incriminating.

Mr. GOWDY. How do we handle the unintentional interception of conversations with non-targets in the Title III arena?

Mr. ROTENBERG. Well, you do it both through minimization and also through the reporting of non-incriminating communications.

Mr. GOWDY. But they don't have standing—if it is an American citizen who is intercepted unintentionally on a domestic wire, they don't have standing to challenge.

Mr. ROTENBERG. I take your question. It is an interesting point. But you see, of course, if people in the United States became concerned that their government was engaging in routine surveillance of their private communications, they may well take steps to try to protect themselves.

Mr. GOWDY. I am just asking you what the law is.

Mr. ROTENBERG. I think you are asking a standing question.

Mr. GOWDY. And the answer is, no, they don't have standing.

Mr. ROTENBERG. Well, I am not sure the answer is no.

Mr. GOWDY. Has any court held that they have standing?

Mr. ROTENBERG. Well, I don't think a court has answered the question.

I mean, the Second Circuit, to the extent that it found in the Clapper case that there was standing based on the possibility of injury and the steps that the plaintiffs had taken to try to protect their communications, I think in fact they did find they had standing.

Mr. GOWDY. I thought in the White case they found that unintentional interceptees of domestic wires do not have standing?

Mr. ROTENBERG. I think in that case the parties did not engage in any activity to try to prevent that type of interception.

That is the problem here. The problem is the government engaging in a surveillance activity with neither you nor me knowing if in fact we are a target.

Mr. GOWDY. Which leads—Mr. Wainstein, you have been there before. We can't make legislation by episode or anecdote. Is the government routinely targeting American citizens in foreign land and what protections are in place?

Mr. WAINSTEIN. The answer is no. The statute says that the government, if it is going to target a U.S. person in a foreign land, based on the provision in the FAA for the first time the government actually has to notify the FISA Court and get an individualized FISA order.

There is also a provision in the FAA that says you can't reverse target, which means you can't target somebody overseas with the real purpose of trying to get the communications from the person inside the United States that the person overseas is talking to.

Mr. SENSENBRENNER. The gentleman's time has expired.

The Chair, in the absence of the gentlewoman from Texas, Ms. Jackson Lee, will recognize himself as the last questioner.

Mr. Wainstein, I think that we have already established that the Fourth Amendment does not apply to foreign targets overseas. You agree with that.

Mr. WAINSTEIN. I agree with that.

Mr. SENSENBRENNER. What is the difference between probable cause as it applies to Title I for FISA and the requirements for foreign surveillance approval in Title VII of the FAA?

Mr. WAINSTEIN. Well, under FISA, regular FISA, traditional FISA, you have to establish probable cause that the target is a foreign power or an agent of a foreign power; and you have to lay evidence of that out in an application to the FISA Court. The FISA Court has to find probable cause of that showing, which is different from the probable cause you have to show in Title III criminal contacts.

Mr. SENSENBRENNER. That was my next question, and you said it is different.

Professor Rotenberg, I think as a goal we want to have more transparency in all of the laws that we have except when you are dealing with national security. If we have too much transparency, then people who wish to do our country and its citizens harm will end up being able to connect the dots and be able to get away with a terrorist strike. And this is something that this Committee has had to wrestle with really since FISA but more acutely since 9/11.

Now, how are we able to make any sense if the law is amended to require the government to release the numbers of people who were incidentally monitored without identifying the individuals that you don't want identified.

Mr. ROTENBERG. Well, Mr. Chairman, as I said, I think statistical reporting, based on the current statute in Section 707, in fact, you do get numbers as to how many orders were authorized under 702, 703. None of that information would jeopardize any investigation to yield any activity.

Mr. SENSENBRENNER. Okay.

Mr. ROTENBERG. I would also point out I think Mr. Jaffer's suggestion that the legal reasoning of the FISA Court to the extent that it can be released with appropriate sections redacted would also be very helpful to make an effort to——

Mr. SENSENBRENNER. Now, following up on my question, say we release the number of people who are incidentally monitored—and you can pick a number from one to whatever—then how would that number mean anything to the public if we don't release the number of targeted individuals to compare it to?

Mr. ROTENBERG. Well, you know, obviously, you would make the decisions about what you think is appropriate to release. But my own experience, having read these reports for many, many years, is that it is actually quite helpful to evaluate trends in the use of surveillance authority.

It was significant, for example, that in 2003 the number of FISA warrants for the first time exceeded the number of Title III warrants that were issued in the United States, and that was a reflection of the changing character of investigations within this country. I think that information would be helpful not only to the Committee but also to the public.

Mr. SENSENBRENNER. Okay. Next question is that say we release the actual number of people who were targeted. Does that give the other side an indication as to the extent of the operational strength of our national security agencies?

Mr. ROTENBERG. You know, I don't see how it would. I imagine someone could make the argument. But we are truly talking about aggregate numbers, and you could choose, for example, which numbers to disclose.

The main point, I think—and maybe there is agreement on this point—the current numbers that are provided are simply inadequate. You just don't know from the information that is made available from the Court how this legal authority is being used, and I don't think that is where you would want to leave this as you are considering renewal of the Act.

Mr. SENSENBRENNER. My guess is that, rather than playing the numbers game either with the actual targets or the people who were incidentally surveilled, perhaps decisions of the FISA Court, particularly the review of the FISA Court appropriately redacted, would be able to give us the answer to that question, rather than saying there were X number of people who were incidentally surveilled and Y number of people, you know, who were actual targets. I have always been one that has favored disclosure.

On the other hand, you know, I know that there is a danger involved in that, particularly looking at what was disclosed during

the trial of the Twin Towers bombers that Michael Mukasey as a Federal judge presided over. There was information that was disclosed during that trial that was used by al Qaeda to pull off 9/11, and I don't think we want to change the law so that that happens ever again.

Well, my time is up.

I would like to thank the witnesses for appearing. This has been a very useful hearing.

Let me say that Thursday of next week we will have a classified briefing where many of the Members of this Committee who have had questions can ask NDI Clapper and a yet-to-be determined representative of the Justice Department whatever they want. So that will be a classified briefing, and I would encourage the Members to come to it and to re-ask the questions that they don't think they got an adequate answer to today.

So, without objection, the hearing is adjourned.

[Whereupon, at 11:30 a.m., the Subcommittee was adjourned.]