112TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 112–645
Part 1

FISA AMENDMENTS ACT REAUTHORIZATION ACT OF 2012

AUGUST 2, 2012.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SMITH of Texas, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

DISSENTING VIEWS AND ADDITIONAL VIEWS

[To accompany H.R. 5949]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 5949) to extend the FISA Amendments Act of 2008 for five years, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The Amendment

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "FISA Amendments Act Reauthorization Act of 2012".

SEC. 2. FIVE-YEAR EXTENSION OF FISA AMENDMENTS ACT OF 2008.

(a) EXTENSION.—Section 403(b) of the FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2474) is amended—

(1) in paragraph (1), by striking "December 31, 2012" and inserting "December 31, 2017"; and

(2) in paragraph (2) in the material preceding subparagraph (A), by striking "December 31, 2012" and inserting "December 31, 2017".

(b) CONFORMING AMENDMENT.—The heading of section 404(b)(1) of the FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2476) is amended by striking "DECEMBER 31, 2012" and inserting "DECEMBER 31, 2017".

Purpose and Summary

The purpose of this bill is to extend for 5 years the FISA Amendments Act of 2008.

Background and Need for the Legislation

In 2006 and 2007, then-Director of National Intelligence Admiral Mike McConnell explained to Congress that due to recent FISA court decisions, the government was forced to devote substantial resources to obtaining court approvals—based on a showing of probable cause—to conduct surveillance against terrorists located overseas in some circumstances. This is contrary to what Congress intended when it enacted the Foreign Intelligence Surveillance Act (FISA) in 1978 and had come about due to changes in telecommunication technology. Admiral McConnell stated that the Intelligence Community was not collecting approximately two-thirds of the foreign intelligence information that it collected prior to legal interpretations that required the government to obtain individualized FISA court orders for overseas surveillance.

On July 10, 2008, President Bush signed into law the FISA Amendments Act of 2008, which passed with a bipartisan majority of Congress and broad support from the intelligence community. The Act allows intelligence professionals to more quickly and effectively monitor terrorist communications, while protecting the civil liberties of Americans. Among other things, the law accomplishes the following:

- Ensures that the intelligence community has the tools it needs to determine who terrorists are communicating with, what they are saying and what they may be planning.
- Provides critical authorities that allow the intelligence community to acquire foreign intelligence information by targeting foreign persons reasonably believed to be outside the United States.
- Preserves and provides new civil liberties protections for Americans.

- Requires court orders to target Americans for foreign intelligence surveillance, no matter where they are, and requires court review of the procedures used to protect information about Americans.

Specifically, the new law authorizes the targeting of non-U.S. persons overseas to acquire foreign intelligence information, subject to specific targeting and minimization procedures that are reviewed by the FISA Court.

The Act permits the Attorney General and Director of National Intelligence to obtain an annual certification from the Foreign Intelligence Surveillance Court (FISC) to target foreign persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information. Under exigent circumstances, the Attorney General and Director of National Intelligence may immediately authorize such targeting based upon a determination that without immediate implementation of an authorization, intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order.

The Act strengthens protections for U.S. citizens by requiring the government to obtain an order from the FISC to target them *outside* the United States to acquire foreign intelligence information. Prior to 2008, targeting of U.S. persons outside the U.S. was governed by Executive Order 12333, which allowed the Attorney General to certify the targeting of U.S. persons overseas.

The Act expands congressional oversight with a semi-annual report to Congress from the Administration on certifications or orders obtained under the Act, compliance reviews, and incidents of noncompliance. The Act amends an existing reporting requirement that requires the Attorney General to submit to Congress a copy of any FISC order, opinion, or decision, and the accompanying pleadings, briefs, and other memoranda of law when the court's decision includes "significant construction or interpretation of any provision" of FISA. This expands the amount of background and supporting material that the Committee will receive in connection with a significant decision by the FISC. Prior to enactment of the FISA Amendments Act in 2008, only "decisions and opinions" containing significant construction or interpretation of FISA were required to be submitted to Congress.

At a hearing of the Subcommittee on Crime, Terrorism, and Homeland Security, Mr. Kenneth Wainstein, former head of the National Security Division of the Justice Department, testified that:

> In crafting this law, however, Congress recognized that it had to balance the need for a judicial review process for domestic surveillance against the government's need to freely conduct surveillance overseas. It accomplished that objective by clearly distinguishing between surveillances directed against persons located within the United States—where constitutional protections apply—and those directed against persons outside the United States, where the fourth amendment does not apply. It then imposed the court approval requirement on surveillances directed against persons within the United States and left the In-

telligence Community free to surveil overseas targets without the undue burden of court process.

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, both 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."

In support of the Administration's call for reauthorization, Mr. Wainstein asked Congress to focus on the three considerations: (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 4 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.

America and its allies face continuous national security threats from foreign nations and terrorist organizations. Foreign agents from rival nations continue to spy on the United States. And al Qaeda and other terrorist networks continue to plot attacks against America. America's security cannot be guaranteed at the border. Congress must ensure that our national security agencies are able to gather foreign intelligence information from foreign terrorists and nation-states so that we can stop threats before they reach our shores. The FISA Amendments Act has proven successful in achieving this goal and must be extended for an additional 5 years.

Hearings

The Committee's Subcommittee on Crime, Terrorism and Homeland Security held 1 day of hearings on H.R. 5949, on May 31, 2012. Testimony was received from (1) Mr. Keneith L. Wainstein, Partner, Cadwalader, Wickersham & Taft LLP, and former Assistant Attorney General for the National Security Division of the Department of Justice, and the former Homeland Security Advisor to the President; (2) Mr. Marc Rotenberg, President, Electronic Privacy Information Center (EPIC); (3) Jameel Jaffer, Director, Center for Democracy, American Civil Liberties Union (ACLU).

Committee Consideration

On June 19, 2012, the Committee on the Judiciary met in open session and ordered the bill H.R. 5949 favorably reported, without amendment, by recorded vote, a quorum being present.

Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall votes occurred during the Committee's consideration of H.R. 5949.

1. An amendment by Mr. Conyers to reauthorize the FISA Amendment Act to 2015. Defeated 12–12.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa			
Mr. Pence		X	
Mr. Forbes		X	
Mr. King			
Mr. Franks		X	
Mr. Gohmert	X		
Mr. Jordan			
Mr. Poe	X		
Mr. Chaffetz			
Mr. Griffin			
Mr. Marino		X	
Mr. Gowdy			
Mr. Ross			
Ms. Adams			
Mr. Quayle			
Mr. Amodei			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters			
Mr. Cohen			
Mr. Johnson, Jr.	X		
Mr. Pierluisi		X	
Mr. Quigley	X		
Ms. Chu	X		
Mr. Deutch	X		
Ms. Sánchez			
Mr. Polis			
Total	12	12	

2. An amendment by Mr. Nadler to require the Attorney General to make publicly available a declassified summary of every decision, order, or opinion of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes a significant construction or interpretation of Section 702 of the Foreign Intelligence Surveillance Act of 1978. Defeated, 14–17.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.	X		
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa		X	
Mr. Pence		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan		X	
Mr. Poe	X		
Mr. Chaffetz			
Mr. Griffin			
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams		X	
Mr. Quayle			
Mr. Amodei			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Cohen	X		
Mr. Johnson, Jr.	X		
Mr. Pierluisi		X	
Mr. Quigley	X		
Ms. Chu	X		
Mr. Deutch			
Ms. Sánchez			
Mr. Polis	X		
Total	14	17	

3. An Amendment by Mr. Scott to amend Section 702(l) of the Foreign Intelligence Surveillance Act of 2008 to require that each assessment or review under paragraph 1, 2 or 3 shall be published in unclassified form but may have a classified annex. Defeated, 10–19.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa		X	
Mr. Pence		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan		X	
Mr. Poe		X	
Mr. Chaffetz			
Mr. Griffin			
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams		X	
Mr. Quayle			
Mr. Amodei			
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee	X		
Ms. Waters			
Mr. Cohen	X		
Mr. Johnson, Jr.	X		
Mr. Pierluisi		X	
Mr. Quigley	X		
Ms. Chu	X		
Mr. Deutch			
Ms. Sánchez			
Mr. Polis			
Total	10	19	

4. An amendment by Ms. Jackson Lee to require a report by the Inspector General of the Department of Justice and the Inspector

General of that Intelligence Community on the implementation of the amendments made by the FISA Amendments Act of 2008. Defeated, 11–20.

ROLLCALL NO. 4

	Ayes	Nays	Present
Mr. Smith, Chairman		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Chabot		X	
Mr. Issa		X	
Mr. Pence		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan		X	
Mr. Poe		X	
Mr. Chaffetz			
Mr. Griffin			
Mr. Marino		X	
Mr. Gowdy		X	
Mr. Ross		X	
Ms. Adams		X	
Mr. Quayle			
Mr. Amodei		X	
Mr. Conyers, Jr., Ranking Member	X		
Mr. Berman			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee	X		
Ms. Waters			
Mr. Cohen	X		
Mr. Johnson, Jr.	X		
Mr. Pierluisi		X	
Mr. Quigley	X		
Ms. Chu	X		
Mr. Deutch	X		
Ms. Sánchez			
Mr. Polis			
Total	11	20	

5. On Reporting the bill favorably to the House. Passed 23–11.

ROLLCALL NO. 5

	Ayes	Nays	Present
Mr. Smith, Chairman	X		
Mr. Sensenbrenner, Jr.	X		
Mr. Coble	X		
Mr. Gallegly	X		
Mr. Goodlatte	X		
Mr. Lungren	X		
Mr. Chabot	X		
Mr. Issa	X		
Mr. Pence	X		
Mr. Forbes	X		
Mr. King	X		
Mr. Franks	X		
Mr. Gohmert	X		
Mr. Jordan	X		
Mr. Poe	X		
Mr. Chaffetz			
Mr. Griffin			
Mr. Marino	X		
Mr. Gowdy	X		
Mr. Ross	X		
Ms. Adams	X		
Mr. Quayle			
Mr. Amodei	X		
Mr. Conyers, Jr., Ranking Member		X	
Mr. Berman	X		
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee		X	
Ms. Waters		X	
Mr. Cohen		X	
Mr. Johnson, Jr.		X	
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu		X	
Mr. Deutch		X	
Ms. Sánchez			
Mr. Polis			
Total	23	11	

Committee Oversight Findings

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

New Budget Authority and Tax Expenditures

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

Congressional Budget Office Cost Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 5949, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 2, 2012.

Hon. LAMAR SMITH, CHAIRMAN,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5949, the "FISA Amendments Act Reauthorization Act of 2012."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226-2860.

Sincerely,

DOUGLAS W. ELMENDORF,
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 5949—FISA Amendments Act Reauthorization Act of 2012.

As ordered reported by the House Committee on the Judiciary on June 19, 2012.

H.R. 5949 would extend the authority of the Federal Government to conduct surveillance pursuant to the FISA Amendments Act of 2008 (Public Law 110-261). Because CBO does not provide cost estimates for classified programs, this estimate addresses only the budgetary effects on unclassified programs affected by the bill. On that basis, CBO estimates that implementing H.R. 5949 would have no significant cost to the Federal Government. Enacting the bill could affect direct spending and revenues; therefore, pay-as-you-go procedures apply. However, CBO estimates that any effects would be insignificant for each year.

The FISA Amendments Act of 2008 clarified the authority of the Federal Government to surveil and intercept communications of certain persons located outside the United States. H.R. 5949 would extend the provisions of that act by five years (otherwise they expire after December 31, 2012). As a result, the government might be able to pursue cases that it otherwise would not be able to pros-

ecute. CBO expects that H.R. 5949 would apply to a relatively small number of additional offenders, however, so any increase in costs for law enforcement, court proceedings, or prison operations would not be significant. Any such costs would be subject to the availability of appropriated funds.

Because those prosecuted and convicted under H.R. 5949 could be subject to criminal fines, the Federal Government might collect additional fines if the legislation is enacted. Criminal fines are deposited as revenues in the Crime Victims Fund and later spent. CBO expects that any additional revenues and direct spending would not be significant because of the relatively small number of cases likely to be affected.

The bill would impose both private-sector and intergovernmental mandates by extending an existing mandate that would limit civil actions and require providers of communication services to provide information. There is little information about the prevalence of electronic surveillance in those cases or the scope or size of potential awards from such cases. Consequently, CBO cannot determine whether the costs of those mandates would exceed the annual threshold established by the Unfunded Mandates Reform Act (UMRA) for private-sector mandates ($146 million in 2012, adjusted annually for inflation).

However, few public entities receive requests for such information, and the costs on them would be small. The bill also would extend an existing preemption on State and local governments regarding legal rights of action. CBO estimates that the costs to public entities of all the intergovernmental mandates in the bill would be small and well below the annual threshold established in UMRA ($73 million in 2012, adjusted annually for inflation).

On May 18, 2011, CBO transmitted a cost estimate for H.R. 1800, the FISA Sunsets Reauthorization Act of 2011, as ordered reported by the House Committee on the Judiciary on May 12, 2011. That bill would extend certain powers of the Federal Government to investigate terrorist acts. CBO estimated that implementing H.R. 1800 would have no significant cost to the Federal Government.

The CBO staff contacts for this estimate are Mark Grabowicz and Jason Wheelock (for Federal costs), J'nell L. Blanco (for the impact on State and local governments), and Elizabeth Bass (for the impact on the private sector). The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 5949, makes improvements to the criminal code that will help law enforcement officials pursue those who steal and traffic pre-retail medical cargo.

Advisory on Earmarks

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 5949 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

Section-by-Section Analysis

The following discussion describes the bill as reported by the Committee.

Section 1. Short Title

This section cites the short title of the bill as the "The FISA Amendment Act Reauthorization Act of 2012."

Section 2. Extends the Authorization for Five Years.

This section changes the expiration date of the FISA Amendments Act of 2008 to from December 31, 2012 to December 31, 2017.

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

FISA AMENDMENTS ACT OF 2008

* * * * * * *

TITLE IV—OTHER PROVISIONS

* * * * * * *

SEC. 403. REPEALS.

(a) * * *

(b) FISA AMENDMENTS ACT OF 2008.—

(1) IN GENERAL.—Except as provided in section 404, effective [December 31, 2012] *December 31, 2017*, title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Effective [December 31, 2012] *December 31, 2017*—

(A) * * *

* * * * * * *

SEC. 404. TRANSITION PROCEDURES.

(a) * * *

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON [DECEMBER 31, 2012] *DECEMBER 31, 2017*.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by

section 101(a), shall continue in effect until the date of the expiration of such order, authorization, or directive.

* * * * * * *

Dissenting Views

INTRODUCTION

H.R. 5949, the "FISA Amendments Act Reauthorization Act of 2012," extends the expiration date of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA or Act),[1] which authorizes the Federal Government to conduct electronic surveillance of persons reasonably believed to be outside the United States, from December 31, 2012 to June 1, 2017.

We strongly oppose this bill because it effectuates an unwarranted long-term extension of a controversial law that may have been used to violate the privacy interests of American citizens. To shed light on the scope of these alleged violations, we offered at the Committee's markup of H.R. 5949 a series of amendments that would have required certain information to be disclosed to the public and allowed Congress to exercise more effective oversight of the FAA. These carefully crafted amendments would not have compromised our national security or the integrity of the Act's underlying programs. Unfortunately, none of these amendments were adopted, and the Committee thereby missed an opportunity to improve a highly controversial law.

H.R. 5949 is opposed by the American-Arab Anti-Discrimination Committee, the American Association of Law Libraries, the American Civil Liberties Union, the American Library Association, the Association of Research Libraries, the Brennan Center for Justice, the Center for Democracy & Technology, the Council on American-Islamic Relations, the Cyber Privacy Project, the Defending Dissent Foundation, Demand Progress, the Electronic Frontier Foundation, the Government Accountability Project, the Liberty Coalition, the National Association of Criminal Defense Lawyers, and OpenTheGovernment.org.[2]

For these reasons, and those described below, we must respectfully dissent.

DESCRIPTION AND BACKGROUND

DESCRIPTION

H.R. 5949 extends the expiration date of the FAA from December 31, 2012 to June 1, 2017.

---

[1] Pub. L. No. 110–261, 122 Stat. 2435 (2008).

[2] Letter to Representatives F. James Sensenbrenner, Jr. (R–WI), Chairman, & Robert C. "Bobby" Scott (D–VA), Ranking Member, H. Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, from representatives of the American-Arab Anti-Discrimination Committee, the American Association of Law Libraries, the American Civil Liberties Union, the American Library Association, the Association of Research Libraries, the Brennan Center for Justice, the Center for Democracy & Technology, the Council on American-Islamic Relations, the Cyber Privacy Project, the Defending Dissent Foundation, Demand Progress, the Electronic Frontier Foundation, the Government Accountability Project, the Liberty Coalition, the National Association of Criminal Defense Lawyers, and OpenTheGovernment.org, (June 11, 2012) (on file with H. Comm. on the Judiciary Democratic Staff).

BACKGROUND

I. The Foreign Intelligence Surveillance Act

In 1978, the Foreign Intelligence Surveillance Act ("FISA") was enacted to establish a statutory framework for gathering "foreign intelligence information" from U.S. persons.[3] FISA authorizes special court orders for four purposes: electronic surveillance, physical searches, the installation and use of pen registers and trap and trace devices, and demands for the production of physical items. Although FISA is designed for intelligence gathering and not for the collection of criminal evidence, the law applies to activities to which a Fourth Amendment warrant requirement would apply if they were conducted as part of a criminal investigation.[4]

Most commonly, authorization for a wiretap or physical search under FISA is obtained by application to the Foreign Intelligence Surveillance Court ("FISC" or the "FISA court"). The FISC is composed of eleven Federal district court judges designated by the Chief Justice of the United States.[5] In most circumstances, the FISC will approve an application to conduct electronic surveillance of a U.S. person if there is probable cause to believe that the target is the agent of a foreign power. In exigent circumstances, FISA also allows the government to collect foreign intelligence information without FISC supervision for a limited period of time.[6]

II. Events Leading to the Enactment of the FAA

Preceding the enactment of the FAA in 2008 were two programs aimed at intercepting overseas communications: the warrantless wiretapping program, which was conducted without congressional authorization from 2001 to 2007, and the now-repealed Protect America Act.

A. Warrantless Wiretapping (2001–2007)

In 2005, *The New York Times* reported that the Federal Government had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[7] Subsequently, President George W. Bush acknowledged that he had authorized the National Security Agency (NSA) to "intercept international communications into and out of the United States" by "persons linked to al Qaeda or related terrorist organizations," based solely on "his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy."[8]

The House and Senate intelligence committees were not informed of the full scope of this program until early 2006. As the Senate Select Committee on Intelligence concluded:

---

[3] 50 U.S.C. §§ 1801 *et seq.*

[4] *See* 50 U.S.C. § 1801(f)(1) (limiting the definition of "electronic surveillance" to instances "in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes").

[5] 50 U.S.C. § 1803(a)(1).

[6] *Id.* § 1824(a).

[7] James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers without Courts, N.Y. TIMES, Dec. 16, 2005, at 1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?_r=1.

[8] U.S. Dept. of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President, at 5, 17, Jan. 19, 2006, *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

> The enormous secrecy surrounding the President's Program had little to do with the operational sensitivity of the collection methods. It was widely known that the NSA was surveilling terrorists. What was "sensitive" was that the surveillance was not lawful: it violated a statute passed by Congress and signed into law by the President.[9]

On January 17, 2007, Attorney General Alberto Gonzales stated to Congress that "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."[10] Several groups filed suit alleging statutory and constitutional violations by the telecommunications companies that participated in the program, and the question of retroactive immunity for these companies became central to debate about what statutory authority, if any, would replace the NSA program.

B. The Protect America Act (2007–2008)

On July 18, 2007, the Bush Administration announced that it had submitted a bill to Congress to amend FISA. President Bush explained that FISA was "badly out of date," despite several recent revisions, and that the Act did not apply to new technologies like disposable cell phones or internet-based communications.[11] Pressure from the Bush Administration interrupted negotiations on bipartisan legislation, and the Protect America Act ("PAA") was signed into law on August 5, 2007.[12]

The PAA modified FISA's definition of "electronic surveillance" to exclude from court oversight any surveillance "directed at a person reasonably believed to be outside of the United States."[13] This change was put forward as means to explicitly exclude from FISA purely foreign communications routed through United States telecommunications networks. In practice, however, the mechanism stripped away many protections for U.S. persons as well.[14]

The PAA also set up a new procedure under which the Attorney General or the Director of National Intelligence, without court oversight, could obtain foreign intelligence information "concerning" persons outside the United States. The Administration simply certified to itself that the acquisition did not fit the new definition of "electronic surveillance," and that a "significant purpose" of the acquisition was to obtain foreign intelligence.[15] These certifications were not subject to judicial review. The word "concerning" was read to allow warrantless surveillance of American citizens, including members of the U.S. armed forces, both at home and abroad.

In effect, the PAA compelled telecommunications companies to allow the government immediate access to their facilities for data collection. Any entity that refused ran the risk of a contempt cita-

---

[9] S. Rep. No. 110–209, at 13 (2007).
[10] Letter from Attorney General Alberto Gonzales to the Senate Judiciary Committee (Jan. 17, 2007).
[11] The White House, "President's Radio Address" (broadcast July 28, 2007).
[12] Protect America Act of 2007, Pub. L. No. 110–55 (2007) (expired).
[13] 50 U.S.C. § 1805A (expired).
[14] For example, FISA restricts the dissemination of information about U.S. persons acquired from "electronic surveillance." By excluding surveillance activities from the definition of "electronic surveillance," the PAA also rolled back these protections.
[15] 50 U.S.C. § 1805B(a) (expired).

tion from the FISC.[16] The PAA provided prospective immunity for entities that cooperated with the government, but did not address the question of retroactive immunity.[17] Because of its controversial nature, Congress included a 180-day sunset of the PAA.[18] The statute expired on February 17, 2008, and was explicitly repealed by the FISA Amendments Act.

III. Overview of the FAA

Signed into law on July 10, 2008, the FAA added title VII to FISA. This new title sets forth procedures for the acquisition of foreign intelligence information from overseas targets. Title VII applies to three types of intelligence collection: (1) targeting non-U.S. persons who are reasonably believed to be outside the United States;[19] (2) gathering electronic communications or other data in the United States with respect to U.S. persons who are outside the United States;[20] and (3) "other acquisitions" targeting U.S. persons who are outside the United States.[21]

All three of these authorities are scheduled to sunset on December 31, 2012.[22] The Obama Administration has asked that Congress reauthorize these authorities through June 1, 2017.[23] In closed session, on May 22, 2012, the Senate Select Committee on Intelligence approved S. 3276, the "FAA Sunsets Extension Act of 2012," to extend title VII for 5 years. H.R. 5949 is substantively identical to S. 3276.

Of the three authorities described in title VII, section 702 is the most controversial. This provision authorizes the Attorney General and the Director of National Intelligence—for up to 1 year—"to acquire foreign intelligence information" from "persons reasonably believed to be located outside the United States."[24] The FAA explicitly limits this power in several key aspects:

- The government may not intentionally target any person known at the time of acquisition to be in the United States;
- The government may not engage in "reverse targeting," i.e., targeting a non-U.S. person outside the United States for the purpose of intercepting the communications of a U.S. person without a warrant;
- The government may not intentionally target a U.S. person;
- The government may not intentionally acquire a communication that is sent and received entirely by persons known to be within the United States, and
- Any surveillance under this authority must be conducted in a manner consistent with the Fourth Amendment.[25]

---

[16] *Id.* §§ 1805B(e) and (g) (expired).
[17] *Id.* § 1805B(l) (expired).
[18] Pub. L. No. 110–55 § 6(c) (2007).
[19] 50 U.S.C. § 1881a.
[20] *Id.* § 1881b.
[21] *Id.* § 1881c. This provision is used when section 1881b is unavailable—i.e., because acquisition takes place outside the United States, or because the action involves something other than electronic surveillance, like a physical search.
[22] Pub. L. 110–261 § 403(b) (2008).
[23] Letter to Speaker John Boehner, Speaker, U.S. House of Representatives *et al.* from James R. Clapper, Director of National Intelligence (Mar. 26, 2012).
[24] 50 U.S.C. § 1881a.
[25] *Id.* § 1881a(b).

In addition, the government is obligated to use "targeting procedures" to narrow the scope of collection and "minimization procedures" to limit the retention and dissemination of information about U.S. persons.[26] Targeting procedures are the steps that the government takes prior to collection to ensure that it only targets non-U.S. persons overseas. Minimization procedures go into effect after collection, and describe how the government will handle information that falls outside the legal limits of the FAA.

The government is not required to obtain a warrant to conduct surveillance under this authority. Instead, the government must certify that appropriate targeting and minimization procedures are in place before surveillance begins.[27] If the certification is complete and targeting and minimization procedures are adequate, then the FISC enters an order approving the collection. Otherwise, the government has 30 days to correct any deficiencies in the application or cease its surveillance activities.[28] In exigent circumstances, the government may conduct surveillance for up to 7 days before submitting the related certification to the FISC.[29]

The FAA also bars the initiation or continuation of civil suits, in state and Federal court, against any entity "for providing assistance to an element of the intelligence community."[30] This provision includes retroactive immunity for telecommunications companies that participated in the warrantless wiretapping program "authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007."[31] The courts have upheld the constitutionality of this retroactive immunity against claims based in the First Amendment, the Due Process Clause of the Fifth Amendment, and the separation of powers.[32] This provision of the FAA is not scheduled to expire.

CONCERNS WITH H.R. 5949

The FAA raises significant civil liberties concerns. Without question, it enables the government to collect significant and valuable foreign intelligence. It also authorizes the interception of private communications with U.S. citizens and other individuals lawfully on U.S. soil, thereby presenting serious incursions against the privacy protections afforded by the Fourth Amendment and the rights of free speech and association under the First Amendment. Congress should not reauthorize these authorities unless the executive branch can assure all Americans publicly—to the greatest extent possible—that these concerns have been adequately addressed.

At the Committee's markup, we offered amendments that would have left the underlying authorities of the FAA intact, but have required the government to make basic, non-sensitive information available to the public. The FAA is an important tool for intelligence gathering, but classified reports and secret court opinions are no substitute for public oversight.

---

[26] *Id.* §§ 1881a(d) and (e).
[27] *Id.* § 1881a(g).
[28] *Id.* § 1881a(i)(3).
[29] 50 U.S.C. § 1881a(g)(B).
[30] *Id.* § 1885a.
[31] *Id.* § 1885a(a)(4).
[32] *In re* National Security Agency Telecommunications Records Litigation, 633 F. Supp. 2d 949 (N.D. Cal. 2009). The court also rejected a challenge under the Administrative Procedure Act. *Id.* at 974–76.

I. The Public Has a Right to Know How the Government Uses Warrantless Wiretapping Authorities

Under section 702 of FISA, as added by the FAA, the government can and does intercept the communications of U.S. citizens, even in the absence of any particularized warrant or showing of probable cause. This approach to electronic surveillance raises concerns under the Fourth Amendment, which prohibits unreasonable searches, warrantless eavesdropping, and the use of "general warrants."[33] In light of the fact that many United States entities, e.g., reporters, lawyers, religious groups, and human rights organizations, frequently communicate with overseas persons who are likely targets of section 702, this authority also raises First Amendment questions about the chilling effect of electronic surveillance on free speech and free association.

Section 702 imposes three different reporting requirements on the executive branch. Every 6 months, the Attorney General and the Director of National Intelligence must evaluate the effectiveness of targeting and minimization procedures.[34] Each component of the intelligence community must review its own use of section 702 authority.[35] Finally, each agency that uses section 702 must conduct an annual review of its activities and their impact on U.S. persons.[36]

Notwithstanding these requirements, the government has released very little information about its use of the FAA. The public has a right to know, at least in general terms, how often section 702 is invoked, what kind of information the government collects using this authority, and how the government limits the impact of these programs on American citizens.

During the Committee's markup of H.R. 5949, Representative Bobby Scott (D–VA) offered an amendment that would have made these basic items of information available to the public by requiring the government to submit these reports to Congress in unclassified form. This amendment would have give Americans a sense of how the government uses the FAA, what kind of information it collects under section 702, and what steps it takes to protect U.S. citizens from unwarranted government intrusion. The amendment would not have put sensitive information at risk because it would permitted the government to include a classified annex, if necessary, in each report. We are disappointed that this simple change, necessary for meaningful public participation in this debate, was defeated ten to 19.

II. The Public Has a Right to Know How the Government Interprets these Authorities

The FISA court plays a critical role in overseeing the government's use of section 702. Since 2008, each time that the intelligence community has sought to use this authority, the govern-

---

[33] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons to be seized.

U.S. Const. amend. IV.

[34] 50 U.S.C. § 1881a(l)(1).

[35] *Id.* § 1881a(l)(2).

[36] *Id.* § 1881a(l)(3).

ment has applied to the court for approval of its targeting and minimization procedures. These classified opinions are available to Members of the Committee, but the decisions and orders of the FISA court, which have shaped the government's interpretation of the FAA over time, are not available to the general public.

In markup, Representative Jerrold Nadler (D–NY) offered an amendment that would have, for the first time, required the government to publish unclassified summaries of this secret body of law. Specifically, this amendment would have required the Attorney General to provide an unclassified summary of each decision, order, and opinion, issued by the FISA court that includes a significant interpretation or construction of section 702 of FISA.

The disclosures mandated by this amendment have had bipartisan support. For example, the Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on reauthorization of the FAA on May 31, 2012. At the conclusion of that hearing, in response to a question about making more information about electronic surveillance available to the public, Chairman Sensenbrenner stated:

> 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. . . . I have always been one that has favored disclosure.[37]

Chairman Sensenbrenner was correct. An appropriately redacted summary of key FISA court opinions would go a long way towards a public understanding of section 702, and would underscore how seriously the FISC takes its oversight responsibilities.

Given the fact that the Nadler amendment would have only required summaries of these opinions—and not the opinions themselves—the government would still be able to protect sensitive intelligence sources and methods. This amendment aimed only to make the legal reasoning of the FISA court available to the public. It also sought to ensure that the United States should not have a secret body of law.

Notwithstanding support from both Democrats and Republicans, Representative Nadler's amendment failed by a vote of 14 to 17.

III. The Public Has a Right to Know If Its Privacy Has Been Violated

On its face, the FAA prohibits the intentional targeting of U.S. persons and persons located in the United States. Targeting and minimization procedures are required to limit the unintentional collection and use of information that the government could not normally access without a warrant. Unfortunately, the government has not always adhered to the legal limits of section 702 authority.

The FAA had been in place for only a few months when *The New York Times* reported that the NSA had "overcollected" domestic communications, a practice described as significant and systematic,

[37] The FISA Amendments Act: Hearing before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. (2012) (statement of Chairman Sensenbrenner).

even if unintentional.[38] Although the government assures the committees of jurisdiction that this issue has been corrected, nearly all of the oversight of these programs is conducted in secret. As a result, the public has no way of knowing that its right to privacy is secure.

The most troubling aspect of section 702 is its impact on the private communications of U.S. persons. The Office of the Director of National Intelligence has stated 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 FAA."[39] The Inspector General of the Intelligence Community has deferred to the NSA to reach a similar conclusion.[40]

We are prepared to accept that it might be difficult to determine the exact number of U.S. persons whose communications have been intercepted by the government under section 702, but the intelligence community surely has the ability to arrive at a rough estimate. If the government has never even estimated how many Americans have had their communications collected under the FAA, then the impact of this law on U.S. citizens may be more pronounced than Congress ever intended.

To address this concern, Representative Sheila Jackson Lee (D–TX) offered an amendment that would have directed the Inspectors General of the Intelligence Community and the Department of Justice to produce an estimate of how many Americans have had their communications collected under section 702. The amendment would have also directed the Inspectors General to review compliance incidents, with a particular focus on recurring problems affecting the privacy of persons inside the United States. The resulting report would have been made public, with whatever redactions might be necessary to protect properly classified information.

Although this amendment failed by a vote of 11 to 20, we will continue to press the government to provide this information.

IV. A 5-year Extension of this Law Ignores Our Oversight Responsibilities

The Obama Administration has asked Congress to extend these expiring authorities through December 31, 2017. If H.R. 5949 passes without amendment, no matter what the outcome of the election this fall, the next presidential administration will come and go before Congress next debates reauthorization of the FAA.

The legislative branch, however, must do better. We must require title VII of FISA to sunset earlier because this ensures that the delicate balance between the need to collect foreign intelligence information and the duty to protect the civil rights of American citizens is maintained. Congress should periodically revisit these authorities to examine the government's record, and, if necessary, to scale back the power we have given to the executive branch. Five years is simply too long to ignore these responsibilities.

---

[38] Eric Lichtblau & James Risen, Officials Say U.S. Wiretaps Exceeded Law, N.Y. TIMES, Apr. 15, 2009, at A1, *available at* http://www.nytimes.com/2009/04/16/us/16nsa.html?pagewanted=all.

[39] Letter to Senators Ron Wyden (D–OR) & Mark Udall (D–CO), S. Select Comm. on Intelligence, from Kathleen Turner, Director of Legislative Affairs, Office of the Director of National Intelligence (July 26, 2011).

[40] Letter to Senators Ron Wyden (D–OR) & Mark Udall (D–CO), S. Select Comm. on Intelligence, from I. Charles McCollough III, Inspector General of the Intelligence Community (June 15, 2012).

To address this shortcoming in the legislation, Ranking Member John Conyers, Jr. (D–MI) offered an amendment that would have moved the bill's sunset date to June 1, 2015. By requiring a 3-year extension instead of the bill's 5-year extension, this amendment was a very reasonable compromise between our national security interests and our obligation to conduct meaningful oversight. Ranking Member Conyers' amendment would have also had the effect of synching these authorities with the three sunsetting provisions of FISA enacted by the USA PATRIOT Act: the roving wiretap provision, which permits the government to follow an individual suspect, rather than a specific telephone or device;[41] the "section 215" business records provision, which allows the government to demand virtually any information or record from a person or business by showing that the seizure is "relevant" to a national security investigation;[42] and the never-used "lone wolf" provision, which enables the government to conduct surveillance on individuals suspected of terrorist activity but unaffiliated with any terrorist organization.[43] This amendment would have enabled us to consider all of these controversial FISA amendments at the same time, instead of piecemeal over the course of the next 5 years.

There is little harm, and much to gain, from revisiting the FAA sooner rather than later. Although the Conyers amendment failed 12 to 12, we believe that we can still persuade our colleagues to defend our oversight role and adopt a shorter sunset.

CONCLUSION

Unless it is amended, H.R. 5949 will represent a failure to conduct meaningful oversight of a controversial government authority. Americans are entitled to know how this law affects their constitutionally-protected rights to privacy, free association, and free speech; and Congress has a responsibility to withhold reauthorization of the FAA until a basic measure of transparency is ensured.

For these reasons, we must respectfully dissent.

JOHN CONYERS, JR.
JERROLD NADLER.
ROBERT C. "BOBBY" SCOTT.
MELVIN L. WATT.
ZOE LOFGREN.
SHEILA JACKSON LEE.
MAXINE WATERS.
STEVE COHEN.
HENRY C. "HANK" JOHNSON, JR.
JUDY CHU.
JARED POLIS.

Additional Views

I concur in the dissent of my colleagues to H.R. 5949, the "FISA Amendments Act Reauthorization Act of 2012." In addition to the dissenting views detailed by my colleagues, I offer these additional dissenting views. I believe there is inadequate due process for U.S.

[41] 50 U.S.C. § 1805 note.
[42] *Id.* §§ 1861 note and 1862 note.
[43] *Id.* § 1801 note.

persons in H.R. 5949. I was prepared to introduce an amendment to the Committee markup of H.R. 5949 that addressed this concern, but ultimately did not file the amendment—a copy of that unfiled amendment is included in this statement.

The FISA Amendments Act of 2008 (FAA) requires that an order from the FISA Court be based on probable cause in order to intentionally target any U.S. person for electronic surveillance. [Sec. 703(c)(1)(B)] In addition, the FAA prohibits so-called "reverse targeting"—in which the government targets a non-U.S. person for the purpose of acquiring information on a particular, known U.S. person. [Sec. 702(b)(2)]

However, the FAA does not make it clear that the government must obtain a warrant prior to searching for information acquired *incidentally* on a U.S. person in compliance with Sec. 702. Instead, the information of U.S. persons in such a situation is subject to guidelines and "minimization procedures" that are adopted by the Attorney General and that must be approved by the FISA Court—but which do not explicitly include a warrant requirement under the FAA. [Secs. 702(f)(1) and 702(c)(1)]

Congress should prohibit the Federal Government from intentionally searching for information on a U.S. person in a data pool amassed lawfully under Sec. 702 of FISA should such a data pool ever be amassed—*unless* the searching official has a warrant, consent of the data subject, an emergency authorization, or a reasonable belief that the life or safety of the data subject is threatened and the information is needed to assist that person.

The prohibition on "reverse targeting"—where the government deliberately targets a non-U.S. person *for the purpose* of acquiring information about a U.S. person at the other end of the line—is not a substitute for a warrant requirement to search a database for a U.S. person should such a database ever be amassed pursuant to Sec. 702. Congress should require a warrant for the government to search for any U.S. person in that data if such data exists. "Minimization procedures" are also not a substitute for a warrant in such a case.

The government must comply with the Fourth Amendment at all times, and the FAA should reflect that explicitly.

For the above reasons and those described in the dissenting views, I concur and join in the dissent of my colleagues to H.R. 5949.

ZOE LOFGREN.

ATTACHMENT

AMENDMENT TO H.R. 5949 **[UNFILED]**

BY MS. ZOE LOFGREN OF CALIFORNIA

At the end of the bill, add the following new section:

SEC. __. PROHIBITION ON SEARCHING OF DATA ACQUIRED UNDER SECTION 702 FOR INFORMATION ON UNITED STATES PERSONS.

(a) PROHIBITION.—Section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a) is amended—

(1) by redesignating subsection (l) as subsection (m); and

(2) inserting after subsection (k) the following new subsection:

"(l) PROHIBITION ON SEARCHING OF DATA FOR INFORMATION ON UNITED STATES PERSONS.—

"(1) IN GENERAL.—Except as provided in paragraph (2), no person may search information acquired under this section in an effort to find the communications of a particular United States person.

"(2) EXCEPTION.—Paragraph (1) shall not apply to a search of communications of a particular United States person—

"(A) if such United States person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105, 304, 703, or 704, or title 18, United States Code, during the effective period of that order;

"(B) if such search is authorized by a court order;

"(C) if the person carrying out the search has a reasonable belief that the life or safety of such United States person is threatened and the information is sought for the purpose of assisting such United States person; or

"(D) if such United States person consents to the search.

"(3) CLARIFICATION OF APPLICABILITY OF TARGETING AND MINIMIZATION PROCEDURES.—Nothing in this subsection shall be construed to affect the requirement of an acquisition under this section to comply with the targeting procedures and minimization procedures adopted under this section.".

(b) CONFORMING AMENDMENTS.—Section 404(b)(4) of the FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2477) is amended—

(1) in subparagraph (A), by striking "702(l)" and inserting "702(m)"; and

(2) in subparagraph (B)(iv), by striking "702(l)" each place it appears and inserting "702(m)".

END

○