

Today, the lifesaving procedure for one of the fetuses would be illegal under the new 20-week ban mode.

Then there is the ordeal that Vikki Stella faced.

Vikki is a diabetic who discovered months into her pregnancy that the fetus she was carrying suffered from several major anomalies and had no chance of survival.

As a result of her diabetic medical condition, Vikki's doctor determined that induced labor and Caesarian section were both riskier procedures for Vikki than an abortion.

The procedure not only protected Vikki from immediate medical risks, but also ensured that she would be able to have children in the future.

As you see from each woman's story, every pregnancy is different.

In fact, none of us here is in the position to decide what is best for a woman and her family in their unique circumstances.

H.R. 36 would deprive women the ability to make very difficult and extremely personal medical decisions.

A woman's health, not politics should drive important medical decisions and ignoring a woman's individual circumstances threatens her health and takes an extremely personal medical decision away from a woman and her health care provider.

The Administration urges Congress in its Statement of Administration Policy to oppose H.R. 36 because it would unacceptably restrict women's health and reproductive right to choose.

Women, regardless of their status in life should be able to make choices about their bodies and their healthcare, and we as elected officials should not inject ourselves into decisions best made between a woman and her doctor.

I yield back the balance of my time, and I move the previous question on the resolution.

The previous question was ordered.

The SPEAKER pro tempore. The question is on the resolution.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Ms. SLAUGHTER. Madam Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The vote was taken by electronic device, and there were—yeas 240, nays 186, not voting 6, as follows:

[Roll No. 221]

YEAS—240

Abraham	Bucshon	Denham
Aderholt	Burgess	Dent
Allen	Byrne	DeSantis
Amodei	Calvert	DesJarlais
Babin	Carter (GA)	Diaz-Balart
Barr	Carter (TX)	Dold
Barton	Chabot	Donovan
Benishkek	Chaffetz	Duffy
Bilirakis	Clawson (FL)	Duncan (SC)
Bishop (MI)	Coffman	Duncan (NC)
Bishop (UT)	Cole	Ellmers (MN)
Black	Collins (GA)	Emmer (MN)
Blackburn	Collins (NY)	Farenthold
Blum	Comstock	Fincher
Bost	Conaway	Fitzpatrick
Boustany	Cook	Fleischmann
Brady (TX)	Costello (PA)	Fleming
Brat	Cramer	Flores
Bridenstine	Crawford	Forbes
Brooks (AL)	Crenshaw	Fortenberry
Brooks (IN)	Culberson	Fox
Buchanan	Curbelo (FL)	Franks (AZ)
Buck	Davis, Rodney	Frelinghuysen

Garrett	Luetkemeyer	Ross
Gibbs	Lummis	Rothfus
Gibson	MacArthur	Rouzer
Gohmert	Marchant	Royce
Goodlatte	Marino	Russell
Gosar	McCarthy	Ryan (WI)
Gowdy	McCaul	Salmon
Granger	McClintock	Sanford
Graves (GA)	McHenry	Scalise
Graves (LA)	McKinley	Schweikert
Griffith	McMorris	Scott, Austin
Grothman	Rodgers	Sensenbrenner
Guinta	McSally	Sessions
Guthrie	Meadows	Shimkus
Hanna	Meehan	Shuster
Hardy	Messer	Simpson
Harper	Mica	Smith (MO)
Harris	Miller (FL)	Smith (NE)
Hartzler	Miller (MI)	Smith (NJ)
Heck (NV)	Moolenaar	Smith (TX)
Hensarling	Mooney (WV)	Smith (TX)
Herrera Beutler	Mullin	Stefanik
Hice, Jody B.	Mulvaney	Stewart
Hill	Murphy (PA)	Stivers
Holding	Neugebauer	Stutzman
Hudson	Newhouse	Thompson (PA)
Huelskamp	Noem	Thornberry
Huizenga (MI)	Nugent	Tiberi
Hultgren	Nunes	Tipton
Hunter	Olson	Trott
Hurd (TX)	Palazzo	Turner
Hurt (VA)	Palmer	Upton
Issa	Paulsen	Valadao
Jenkins (KS)	Pearce	Wagner
Jenkins (WV)	Perry	Walberg
Johnson (OH)	Pittenger	Walder
Johnson, Sam	Pitts	Walker
Jolly	Poe (TX)	Walorski
Jones	Poliquin	Walters, Mimi
Jordan	Pompeo	Weber (TX)
Joyce	Posey	Webster (FL)
Katko	Price, Tom	Wenstrup
Kelly (PA)	Ratcliffe	Westerman
King (IA)	Reed	Westmoreland
King (NY)	Reichert	Whitfield
Kinzinger (IL)	Renacci	Williams
Kline	Ribble	Wilson (SC)
Knight	Rice (SC)	Wittman
Labrador	Rigell	Womack
LaMalfa	Roby	Woodall
Lamborn	Roe (TN)	Yoder
Lance	Rogers (AL)	Yoho
Latta	Rogers (KY)	Young (AK)
LoBiondo	Rohrabacher	Young (IA)
Long	Rokita	Young (IN)
Loudermilk	Rooney (FL)	Zeldin
Love	Ros-Lehtinen	Zinke
Lucas	Roskam	

NAYS—186

Adams	Crowley	Higgins
Aguilar	Cuellar	Himes
Amash	Cummings	Honda
Ashford	Davis (CA)	Hoyer
Bass	Davis, Danny	Huffman
Beatty	DeFazio	Israel
Becerra	DeGette	Jackson Lee
Bera	Delaney	Jeffries
Beyer	DeLauro	Johnson (GA)
Bishop (GA)	DelBene	Johnson, E. B.
Blumenauer	DeSaulnier	Kaptur
Bonamici	Deutch	Keating
Boyle, Brendan	Dingell	Kelly (IL)
F.	Doggett	Kennedy
Brady (PA)	Doyle, Michael	Kildee
Brown (FL)	F.	Kilmer
Brownley (CA)	Duckworth	Kind
Bustos	Edwards	Kirkpatrick
Butterfield	Ellison	Kuster
Capuano	Engel	Langevin
Cárdenas	Eshoo	Larsen (WA)
Carney	Esty	Larson (CT)
Carson (IN)	Farr	Lawrence
Cartwright	Fattah	Lee
Castor (FL)	Foster	Levin
Castro (TX)	Frankel (FL)	Lewis
Chu, Judy	Fudge	Lieu, Ted
Cicilline	Gabbard	Lipinski
Clark (MA)	Gallo	Loeb
Clarke (NY)	Garamendi	Lofgren
Clay	Graham	Lowenthal
Cleaver	Grayson	Lowey
Clyburn	Green, Al	Lujan Grisham
Cohen	Green, Gene	(NM)
Connolly	Grijalva	Lujan, Ben Ray
Conyers	Gutiérrez	(NM)
Cooper	Hahn	Lynch
Costa	Hastings	Maloney,
Courtney	Heck (WA)	Carolyn

Maloney, Sean	Pocan	Speier
Massie	Polis	Swalwell (CA)
Matsui	Price (NC)	Takai
McCollum	Quigley	Takano
McDermott	Rangel	Thompson (CA)
McGovern	Rice (NY)	Thompson (MS)
McNerney	Richmond	Titus
Meeks	Roybal-Allard	Tonko
Meng	Ruppersberger	Torres
Moore	Rush	Tsongas
Moulton	Ryan (OH)	Van Hollen
Murphy (FL)	Sánchez, Linda	Vargas
Nadler	T.	Veasey
Napolitano	Sanchez, Loretta	Vela
Neal	Sarbanes	Velázquez
Nolan	Schakowsky	Visclosky
Norcross	Schiff	Walz
O'Rourke	Schrader	Wasserman
Pallone	Scott (VA)	Schultz
Pascarella	Scott, David	Waters, Maxine
Payne	Serrano	Watson Coleman
Pelosi	Sewell (AL)	Welch
Perlmutter	Sherman	Wilson (FL)
Peters	Sinema	Yarmuth
Peterson	Sires	
Pingree	Slaughter	

NOT VOTING—6

Barletta	Graves (MO)	Ruiz
Capps	Hinojosa	Smith (WA)

□ 1416

Mr. LUETKEMEYER changed his vote from "nay" to "yea."

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

PERMISSION TO POSTPONE PROCEEDINGS ON MOTION TO RECOMMIT

Mr. GOODLATTE. Mr. Speaker, I ask unanimous consent that the Chair may postpone further proceedings today on a motion to recommit as though under clause 8 of rule XX.

The SPEAKER pro tempore (Mr. SIMPSON). Is there objection to the request of the gentleman from Virginia? There was no objection.

UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015

Mr. GOODLATTE. Mr. Speaker, pursuant to House Resolution 255, I call up the bill (H.R. 2048) to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes, and ask for its immediate consideration.

The Clerk read the title of the bill.

The SPEAKER pro tempore. Pursuant to House Resolution 255, the amendment printed in part B of House Report 114-111 is adopted, and the bill, as amended, is considered read.

The text of the bill, as amended, is as follows:

H.R. 2048

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the “Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015” or the “USA FREEDOM Act of 2015”.

(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
 Sec. 2. Amendments to the Foreign Intelligence Surveillance Act of 1978.

TITLE I—FISA BUSINESS RECORDS REFORMS

- Sec. 101. Additional requirements for call detail records.
 Sec. 102. Emergency authority.
 Sec. 103. Prohibition on bulk collection of tangible things.
 Sec. 104. Judicial review.
 Sec. 105. Liability protection.
 Sec. 106. Compensation for assistance.
 Sec. 107. Definitions.
 Sec. 108. Inspector General reports on business records orders.
 Sec. 109. Effective date.
 Sec. 110. Rule of construction.

TITLE II—FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

- Sec. 201. Prohibition on bulk collection.
 Sec. 202. Privacy procedures.

TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

- Sec. 301. Limits on use of unlawfully obtained information.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

- Sec. 401. Appointment of amicus curiae.
 Sec. 402. Declassification of decisions, orders, and opinions.

TITLE V—NATIONAL SECURITY LETTER REFORM

- Sec. 501. Prohibition on bulk collection.
 Sec. 502. Limitations on disclosure of national security letters.
 Sec. 503. Judicial review.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

- Sec. 601. Additional reporting on orders requiring production of business records; business records compliance reports to Congress.
 Sec. 602. Annual reports by the Government.
 Sec. 603. Public reporting by persons subject to FISA orders.
 Sec. 604. Reporting requirements for decisions, orders, and opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

- Sec. 701. Emergencies involving non-United States persons.
 Sec. 702. Preservation of treatment of non-United States persons traveling outside the United States as agents of foreign powers.
 Sec. 703. Improvement to investigations of international proliferation of weapons of mass destruction.
 Sec. 704. Increase in penalties for material support of foreign terrorist organizations.
 Sec. 705. Sunsets.

TITLE VIII—SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A—Safety of Maritime Navigation

- Sec. 801. Amendment to section 2280 of title 18, United States Code.

Sec. 802. New section 2280a of title 18, United States Code.

Sec. 803. Amendments to section 2281 of title 18, United States Code.

Sec. 804. New section 2281a of title 18, United States Code.

Sec. 805. Ancillary measure.

Subtitle B—Prevention of Nuclear Terrorism

Sec. 811. New section 2332i of title 18, United States Code.

Sec. 812. Amendment to section 831 of title 18, United States Code.

SEC. 2. AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Except as otherwise expressly provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or a repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

TITLE I—FISA BUSINESS RECORDS REFORMS

SEC. 101. ADDITIONAL REQUIREMENTS FOR CALL DETAIL RECORDS.

(a) **APPLICATION.**—Section 501(b)(2) (50 U.S.C. 1861(b)(2)) is amended—

(1) in subparagraph (A)—
 (A) in the matter preceding clause (i), by striking “a statement” and inserting “in the case of an application other than an application described in subparagraph (C) (including an application for the production of call detail records other than in the manner described in subparagraph (C)), a statement”; and

(B) in clause (iii), by striking “; and” and inserting a semicolon;

(2) by redesignating subparagraphs (A) and (B) as subparagraphs (B) and (D), respectively; and

(3) by inserting after subparagraph (B) (as so redesignated) the following new subparagraph:

“(C) in the case of an application for the production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism, a statement of facts showing that—

“(i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and

“(ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor; and”.

(b) **ORDER.**—Section 501(c)(2) (50 U.S.C. 1861(c)(2)) is amended—

(1) in subparagraph (D), by striking “; and” and inserting a semicolon;

(2) in subparagraph (E), by striking the period and inserting “; and”; and

(3) by adding at the end the following new subparagraph:

“(F) in the case of an application described in subsection (b)(2)(C), shall—

“(i) authorize the production on a daily basis of call detail records for a period not to exceed 180 days;

“(ii) provide that an order for such production may be extended upon application under subsection (b) and the judicial finding under paragraph (1) of this subsection;

“(iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selec-

tion term that satisfies the standard required under subsection (b)(2)(C)(ii);

“(iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii);

“(v) provide that, when produced, such records be in a form that will be useful to the Government;

“(vi) direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production; and

“(vii) direct the Government to—

“(I) adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information; and

“(II) destroy all call detail records produced under the order as prescribed by such procedures.”.

SEC. 102. EMERGENCY AUTHORITY.

(a) **AUTHORITY.**—Section 501 (50 U.S.C. 1861) is amended by adding at the end the following new subsections:

“(i) **EMERGENCY AUTHORITY FOR PRODUCTION OF TANGIBLE THINGS.**—

“(1) Notwithstanding any other provision of this section, the Attorney General may require the emergency production of tangible things if the Attorney General—

“(A) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained;

“(B) reasonably determines that the factual basis for the issuance of an order under this section to approve such production of tangible things exists;

“(C) informs, either personally or through a designee, a judge having jurisdiction under this section at the time the Attorney General requires the emergency production of tangible things that the decision has been made to employ the authority under this subsection; and

“(D) makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.

“(2) If the Attorney General requires the emergency production of tangible things under paragraph (1), the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

“(3) In the absence of a judicial order approving the production of tangible things under this subsection, the production shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest.

“(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

“(5) If such application for approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived

from such production shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof, and no information concerning any United States person acquired from such production shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(6) The Attorney General shall assess compliance with the requirements of paragraph (5).”.

(b) CONFORMING AMENDMENT.—Section 501(d) (50 U.S.C. 1861(d)) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking “pursuant to an order” and inserting “pursuant to an order issued or an emergency production required”;

(B) in subparagraph (A), by striking “such order” and inserting “such order or such emergency production”;

(C) in subparagraph (B), by striking “the order” and inserting “the order or the emergency production”;

(2) in paragraph (2)—

(A) in subparagraph (A), by striking “an order” and inserting “an order or emergency production”;

(B) in subparagraph (B), by striking “an order” and inserting “an order or emergency production”.

SEC. 103. PROHIBITION ON BULK COLLECTION OF TANGIBLE THINGS.

(a) APPLICATION.—Section 501(b)(2) (50 U.S.C. 1861(b)(2)), as amended by section 101(a) of this Act, is further amended by inserting before subparagraph (B), as redesignated by such section 101(a) of this Act, the following new subparagraph:

“(A) a specific selection term to be used as the basis for the production of the tangible things sought;”.

(b) ORDER.—Section 501(c) (50 U.S.C. 1861(c)) is amended—

(1) in paragraph (2)(A), by striking the semicolon and inserting “, including each specific selection term to be used as the basis for the production;”;

(2) by adding at the end the following new paragraph:

“(3) No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements of subsection (b)(2).”.

SEC. 104. JUDICIAL REVIEW.

(a) MINIMIZATION PROCEDURES.—

(1) JUDICIAL REVIEW.—Section 501(c)(1) (50 U.S.C. 1861(c)(1)) is amended by inserting after “subsections (a) and (b)” the following: “and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g)”.

(2) RULE OF CONSTRUCTION.—Section 501(g) (50 U.S.C. 1861(g)) is amended by adding at the end the following new paragraph:

“(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall limit the authority of the court established under section 103(a) to impose additional, particularized minimization procedures with regard to the production, retention, or dissemination of nonpublicly available information concerning unconsenting United States persons, including additional, particularized procedures related to the destruction of information within a reasonable time period.”.

(3) TECHNICAL AND CONFORMING AMENDMENT.—Section 501(g)(1) (50 U.S.C. 1861(g)(1)) is amended—

(A) by striking “Not later than 180 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the” and inserting “The”; and

(B) by inserting after “adopt” the following: “, and update as appropriate.”.

(b) ORDERS.—Section 501(f)(2) (50 U.S.C. 1861(f)(2)) is amended—

(1) in subparagraph (A)(i)—

(A) by striking “that order” and inserting “the production order or any nondisclosure order imposed in connection with the production order”; and

(B) by striking the second sentence; and

(2) in subparagraph (C)—

(A) by striking clause (ii); and

(B) by redesignating clause (iii) as clause (ii).

SEC. 105. LIABILITY PROTECTION.

Section 501(e) (50 U.S.C. 1861(e)) is amended to read as follows:

“(e)(1) No cause of action shall lie in any court against a person who—

“(A) produces tangible things or provides information, facilities, or technical assistance in accordance with an order issued or an emergency production required under this section; or

“(B) otherwise provides technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

“(2) A production or provision of information, facilities, or technical assistance described in paragraph (1) shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.”.

SEC. 106. COMPENSATION FOR ASSISTANCE.

Section 501 (50 U.S.C. 1861), as amended by section 102 of this Act, is further amended by adding at the end the following new subsection:

“(j) COMPENSATION.—The Government shall compensate a person for reasonable expenses incurred for—

“(1) producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application described in subsection (b)(2)(C) or an emergency production under subsection (i) that, to comply with subsection (i)(1)(D), requires an application described in subsection (b)(2)(C); or

“(2) otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.”.

SEC. 107. DEFINITIONS.

Section 501 (50 U.S.C. 1861), as amended by section 106 of this Act, is further amended by adding at the end the following new subsection:

“(k) DEFINITIONS.—In this section:

“(1) IN GENERAL.—The terms ‘foreign power’, ‘agent of a foreign power’, ‘international terrorism’, ‘foreign intelligence information’, ‘Attorney General’, ‘United States person’, ‘United States’, ‘person’, and ‘State’ have the meanings provided those terms in section 101.

“(2) ADDRESS.—The term ‘address’ means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

“(3) CALL DETAIL RECORD.—The term ‘call detail record’—

“(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity

number), a telephone calling card number, or the time or duration of a call; and

“(B) does not include—

“(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

“(ii) the name, address, or financial information of a subscriber or customer; or

“(iii) cell site location or global positioning system information.

“(4) SPECIFIC SELECTION TERM.—

“(A) TANGIBLE THINGS.—

“(i) IN GENERAL.—Except as provided in subparagraph (B), a ‘specific selection term’—

“(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

“(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.

“(ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—

“(I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or

“(II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).

“(iii) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

“(B) CALL DETAIL RECORD APPLICATIONS.—For purposes of an application submitted under subsection (b)(2)(C), the term ‘specific selection term’ means a term that specifically identifies an individual, account, or personal device.”.

SEC. 108. INSPECTOR GENERAL REPORTS ON BUSINESS RECORDS ORDERS.

Section 106A of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109-177; 120 Stat. 200) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by inserting “and calendar years 2012 through 2014” after “2006”; and

(B) by striking paragraphs (2) and (3);

(C) by redesignating paragraphs (4) and (5) as paragraphs (2) and (3), respectively; and

(D) in paragraph (3) (as so redesignated)—

(i) by striking subparagraph (C) and inserting the following new subparagraph:

“(C) with respect to calendar years 2012 through 2014, an examination of the minimization procedures used in relation to orders under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) and whether the minimization procedures adequately protect the constitutional rights of United States persons;”;

(ii) in subparagraph (D), by striking “(as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)))”;

(2) in subsection (c), by adding at the end the following new paragraph:

“(3) CALENDAR YEARS 2012 THROUGH 2014.—Not later than 1 year after the date of enactment of the USA FREEDOM Act of 2015, the Inspector General of the Department of Justice shall submit to the Committee on the

Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under subsection (a) for calendar years 2012 through 2014.”;

(3) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively;

(4) by inserting after subsection (c) the following new subsection:

“(d) INTELLIGENCE ASSESSMENT.—

“(1) IN GENERAL.—For the period beginning on January 1, 2012, and ending on December 31, 2014, the Inspector General of the Intelligence Community shall assess—

“(A) the importance of the information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) to the activities of the intelligence community;

“(B) the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community;

“(C) the minimization procedures used by elements of the intelligence community under such title and whether the minimization procedures adequately protect the constitutional rights of United States persons; and

“(D) any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the court established under section 103(a) of such Act (50 U.S.C. 1803(a)).

“(2) SUBMISSION DATE FOR ASSESSMENT.—Not later than 180 days after the date on which the Inspector General of the Department of Justice submits the report required under subsection (c)(3), the Inspector General of the Intelligence Community shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2012 through 2014.”;

(5) in subsection (e), as redesignated by paragraph (3)—

(A) in paragraph (1)—

(i) by striking “a report under subsection (c)(1) or (c)(2)” and inserting “any report under subsection (c) or (d)”;

(ii) by striking “Inspector General of the Department of Justice” and inserting “Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, and any Inspector General of an element of the intelligence community that prepares a report to assist the Inspector General of the Department of Justice or the Inspector General of the Intelligence Community in complying with the requirements of this section”;

(B) in paragraph (2), by striking “the reports submitted under subsections (c)(1) and (c)(2)” and inserting “any report submitted under subsection (c) or (d)”;

(6) in subsection (f), as redesignated by paragraph (3)—

(A) by striking “The reports submitted under subsections (c)(1) and (c)(2)” and inserting “Each report submitted under subsection (c)”;

(B) by striking “subsection (d)(2)” and inserting “subsection (e)(2)”;

(7) by adding at the end the following new subsection:

“(g) DEFINITIONS.—In this section:

“(1) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

“(2) UNITED STATES PERSON.—The term ‘United States person’ has the meaning given that term in section 101 of the Foreign Intel-

ligence Surveillance Act of 1978 (50 U.S.C. 1801).”.

SEC. 109. EFFECTIVE DATE.

(a) IN GENERAL.—The amendments made by sections 101 through 103 shall take effect on the date that is 180 days after the date of the enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to alter or eliminate the authority of the Government to obtain an order under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) as in effect prior to the effective date described in subsection (a) during the period ending on such effective date.

SEC. 110. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed to authorize the production of the contents (as such term is defined in section 2510(8) of title 18, United States Code) of any electronic communication from an electronic communication service provider (as such term is defined in section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(b)(4))) under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.).

TITLE II—FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

SEC. 201. PROHIBITION ON BULK COLLECTION.

(a) PROHIBITION.—Section 402(c) (50 U.S.C. 1842(c)) is amended—

(1) in paragraph (1), by striking “; and” and inserting a semicolon;

(2) in paragraph (2), by striking the period at the end and inserting “; and”;

(3) by adding at the end the following new paragraph:

“(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device.”.

(b) DEFINITION.—Section 401 (50 U.S.C. 1841) is amended by adding at the end the following new paragraph:

“(4)(A) The term ‘specific selection term’—

“(i) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

“(ii) is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device.

“(B) A specific selection term under subparagraph (A) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device, such as an identifier that—

“(i) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or

“(ii) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).

“(C) For purposes of subparagraph (A), the term ‘address’ means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

“(D) Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).”.

SEC. 202. PRIVACY PROCEDURES.

(a) IN GENERAL.—Section 402 (50 U.S.C. 1842) is amended by adding at the end the following new subsection:

“(h) PRIVACY PROCEDURES.—

“(1) IN GENERAL.—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

“(2) RULE OF CONSTRUCTION.—Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.”.

(b) EMERGENCY AUTHORITY.—Section 403 (50 U.S.C. 1843) is amended by adding at the end the following new subsection:

“(d) PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h).”.

TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

SEC. 301. LIMITS ON USE OF UNLAWFULLY OBTAINED INFORMATION.

Section 702(i)(3) (50 U.S.C. 1881a(i)(3)) is amended by adding at the end the following new subparagraph:

“(D) LIMITATION ON USE OF INFORMATION.—

“(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.”.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

SEC. 401. APPOINTMENT OF AMICUS CURIAE.

Section 103 (50 U.S.C. 1803) is amended by adding at the end the following new subsections:

“(i) AMICUS CURIAE.—

“(1) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after the enactment of this subsection, jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall

serve pursuant to rules the presiding judges may establish. In designating such individuals, the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate.

“(2) AUTHORIZATION.—A court established under subsection (a) or (b), consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

“(A) shall appoint an individual who has been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate; and

“(B) may appoint an individual or organization to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit an individual or organization leave to file an amicus curiae brief.

“(3) QUALIFICATIONS OF AMICUS CURIAE.—

“(A) EXPERTISE.—Individuals designated under paragraph (1) shall be persons who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to a court established under subsection (a) or (b).

“(B) SECURITY CLEARANCE.—Individuals designated pursuant to paragraph (1) shall be persons who are determined to be eligible for access to classified information necessary to participate in matters before the courts. Amicus curiae appointed by the court pursuant to paragraph (2) shall be persons who are determined to be eligible for access to classified information, if such access is necessary to participate in the matters in which they may be appointed.

“(4) DUTIES.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2)(A), the amicus curiae shall provide to the court, as appropriate—

“(A) legal arguments that advance the protection of individual privacy and civil liberties;

“(B) information related to intelligence collection or communications technology; or

“(C) legal arguments or information regarding any other area relevant to the issue presented to the court.

“(5) ASSISTANCE.—An amicus curiae appointed under paragraph (2)(A) may request that the court designate or appoint additional amici curiae pursuant to paragraph (1) or paragraph (2), to be available to assist the amicus curiae.

“(6) ACCESS TO INFORMATION.—

“(A) IN GENERAL.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

“(i) shall have access to any legal precedent, application, certification, petition, motion, or such other materials that the court determines are relevant to the duties of the amicus curiae; and

“(ii) may, if the court determines that it is relevant to the duties of the amicus curiae, consult with any other individuals designated pursuant to paragraph (1) regarding information relevant to any assigned proceeding.

“(B) BRIEFINGS.—The Attorney General may periodically brief or provide relevant materials to individuals designated pursuant to paragraph (1) regarding constructions and interpretations of this Act and legal, technological, and other issues related to actions authorized by this Act.

“(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or proceedings only if that individual is eligible for access to classified information and to the extent consistent with the national security of the United States.

“(D) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Government to provide information to an amicus curiae appointed by the court that is privileged from disclosure.

“(7) NOTIFICATION.—A presiding judge of a court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (2).

“(8) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a nonreimbursable basis) the assistance of the executive branch in the implementation of this subsection.

“(9) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support for an individual designated to serve as amicus curiae under paragraph (1) or appointed to serve as amicus curiae under paragraph (2) in a manner that is not inconsistent with this subsection.

“(10) RECEIPT OF INFORMATION.—Nothing in this subsection shall limit the ability of a court established under subsection (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.

“(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

“(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

“(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

“(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(1), or any other person, to provide briefing or other assistance.”

SEC. 402. DECLASSIFICATION OF DECISIONS, ORDERS, AND OPINIONS.

(a) DECLASSIFICATION.—Title VI (50 U.S.C. 1871 et seq.) is amended—

(1) in the heading, by striking “REPORTING REQUIREMENT” and inserting “OVERSIGHT”; and

(2) by adding at the end the following new section:

“SEC. 602. DECLASSIFICATION OF SIGNIFICANT DECISIONS, ORDERS, AND OPINIONS.

“(a) DECLASSIFICATION REQUIRED.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveil-

lance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term ‘specific selection term’, and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

“(b) REDACTED FORM.—The Director of National Intelligence, in consultation with the Attorney General, may satisfy the requirement under subsection (a) to make a decision, order, or opinion described in such subsection publicly available to the greatest extent practicable by making such decision, order, or opinion publicly available in redacted form.

“(c) NATIONAL SECURITY WAIVER.—The Director of National Intelligence, in consultation with the Attorney General, may waive the requirement to declassify and make publicly available a particular decision, order, or opinion under subsection (a), if—

“(1) the Director of National Intelligence, in consultation with the Attorney General, determines that a waiver of such requirement is necessary to protect the national security of the United States or properly classified intelligence sources or methods; and

“(2) the Director of National Intelligence makes publicly available an unclassified statement prepared by the Attorney General, in consultation with the Director of National Intelligence—

“(A) summarizing the significant construction or interpretation of any provision of law, which shall include, to the extent consistent with national security, a description of the context in which the matter arises and any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision; and

“(B) that specifies that the statement has been prepared by the Attorney General and constitutes no part of the opinion of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review.”

(b) TABLE OF CONTENTS AMENDMENTS.—The table of contents in the first section is amended—

(1) by striking the item relating to title VI and inserting the following new item:

“TITLE VI—OVERSIGHT”;

and

(2) by inserting after the item relating to section 601 the following new item:

“Sec. 602. Declassification of significant decisions, orders, and opinions.”

TITLE V—NATIONAL SECURITY LETTER REFORM

SEC. 501. PROHIBITION ON BULK COLLECTION.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709(b) of title 18, United States Code, is amended in the matter preceding paragraph (1) by striking “may” and inserting “may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request”.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114(a)(2) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(2)) is amended by striking the period and inserting “and a term that specifically identifies a customer, entity, or account to be used as the basis for the production and disclosure of financial records.”

(c) DISCLOSURES TO FBI OF CERTAIN CONSUMER RECORDS FOR COUNTERINTELLIGENCE PURPOSES.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) in subsection (a), by striking “that information,” and inserting “that information that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information.”;

(2) in subsection (b), by striking “written request,” and inserting “written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information.”; and

(3) in subsection (c), by inserting “, which shall include a term that specifically identifies a consumer or account to be used as the basis for the production of the information,” after “issue an order ex parte”.

(d) DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES OF CONSUMER REPORTS.—Section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)) is amended by striking “analysis,” and inserting “analysis and that includes a term that specifically identifies a consumer or account to be used as the basis for the production of such information.”.

SEC. 502. LIMITATIONS ON DISCLOSURE OF NATIONAL SECURITY LETTERS.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended by striking subsection (c) and inserting the following new subsection:

“(c) PROHIBITION OF CERTAIN DISCLOSURE.—

“(1) PROHIBITION.—

“(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

“(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

“(i) a danger to the national security of the United States;

“(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(iii) interference with diplomatic relations; or

“(iv) danger to the life or physical safety of any person.

“(2) EXCEPTION.—

“(A) IN GENERAL.—A wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with the request;

“(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

“(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

“(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (b) in the same manner as the person to whom the request is issued.

“(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) in-

formation otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

“(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.”.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended—

(1) in subsection (a)(5), by striking subparagraph (D); and

(2) by inserting after subsection (b) the following new subsection:

“(c) PROHIBITION OF CERTAIN DISCLOSURE.—

“(1) PROHIBITION.—

“(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a).

“(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

“(i) a danger to the national security of the United States;

“(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(iii) interference with diplomatic relations; or

“(iv) danger to the life or physical safety of any person.

“(2) EXCEPTION.—

“(A) IN GENERAL.—A financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with the request;

“(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

“(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

“(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

“(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

“(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to

whom such disclosure was made prior to the request.”.

(c) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended by striking subsection (d) and inserting the following new subsection:

“(d) PROHIBITION OF CERTAIN DISCLOSURE.—

“(1) PROHIBITION.—

“(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (e) is provided, no consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a), (b), or (c).

“(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

“(i) a danger to the national security of the United States;

“(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(iii) interference with diplomatic relations; or

“(iv) danger to the life or physical safety of any person.

“(2) EXCEPTION.—

“(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with the request;

“(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

“(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

“(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) or (b) or an order under subsection (c) is issued in the same manner as the person to whom the request is issued.

“(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

“(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.”.

(d) CONSUMER REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended by striking subsection (c) and inserting the following new subsection:

“(c) PROHIBITION OF CERTAIN DISCLOSURE.—

“(1) PROHIBITION.—

“(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no consumer reporting agency that receives a request under subsection

(a), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that a government agency described in subsection (a) has sought or obtained access to information or records under subsection (a).

“(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of the government agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

“(i) a danger to the national security of the United States;

“(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(iii) interference with diplomatic relations; or

“(iv) danger to the life or physical safety of any person.

“(2) EXCEPTION.—

“(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with the request;

“(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

“(iii) other persons as permitted by the head of the government agency described in subsection (a) or a designee.

“(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) is issued in the same manner as the person to whom the request is issued.

“(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

“(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of the government agency described in subsection (a) or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.”

(e) INVESTIGATIONS OF PERSONS WITH ACCESS TO CLASSIFIED INFORMATION.—Section 802 of the National Security Act of 1947 (50 U.S.C. 3162) is amended by striking subsection (b) and inserting the following new subsection:

“(b) PROHIBITION OF CERTAIN DISCLOSURE.—

“(1) PROHIBITION.—

“(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a).

“(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

“(i) a danger to the national security of the United States;

“(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(iii) interference with diplomatic relations; or

“(iv) danger to the life or physical safety of any person.

“(2) EXCEPTION.—

“(A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with the request;

“(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

“(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee.

“(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

“(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

“(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of an authorized investigative agency described in subsection (a), or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head of the authorized investigative agency or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.”

(f) TERMINATION PROCEDURES.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall adopt procedures with respect to nondisclosure requirements issued pursuant to section 2709 of title 18, United States Code, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 3162), as amended by this Act, to require—

(A) the review at appropriate intervals of such a nondisclosure requirement to assess whether the facts supporting nondisclosure continue to exist;

(B) the termination of such a nondisclosure requirement if the facts no longer support nondisclosure; and

(C) appropriate notice to the recipient of the national security letter, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the applicable court as appropriate, that the nondisclosure requirement has been terminated.

(2) REPORTING.—Upon adopting the procedures required under paragraph (1), the Attorney General shall submit the procedures to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(g) JUDICIAL REVIEW.—Section 3511 of title 18, United States Code, is amended by striking subsection (b) and inserting the following new subsection:

“(b) NONDISCLOSURE.—

“(1) IN GENERAL.—

“(A) NOTICE.—If a recipient of a request or order for a report, records, or other information under section 2709 of this title, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414), or section 802 of the National

Security Act of 1947 (50 U.S.C. 3162), wishes to have a court review a nondisclosure requirement imposed in connection with the request or order, the recipient may notify the Government or file a petition for judicial review in any court described in subsection (a).

“(B) APPLICATION.—Not later than 30 days after the date of receipt of a notification under subparagraph (A), the Government shall apply for an order prohibiting the disclosure of the existence or contents of the relevant request or order. An application under this subparagraph may be filed in the district court of the United States for the judicial district in which the recipient of the order is doing business or in the district court of the United States for any judicial district within which the authorized investigation that is the basis for the request is being conducted. The applicable nondisclosure requirement shall remain in effect during the pendency of proceedings relating to the requirement.

“(C) CONSIDERATION.—A district court of the United States that receives a petition under subparagraph (A) or an application under subparagraph (B) should rule expeditiously, and shall, subject to paragraph (3), issue a nondisclosure order that includes conditions appropriate to the circumstances.

“(2) APPLICATION CONTENTS.—An application for a nondisclosure order or extension thereof or a response to a petition filed under paragraph (1) shall include a certification from the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or a designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of the department, agency, or instrumentality, containing a statement of specific facts indicating that the absence of a prohibition of disclosure under this subsection may result in—

“(A) a danger to the national security of the United States;

“(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(C) interference with diplomatic relations; or

“(D) danger to the life or physical safety of any person.

“(3) STANDARD.—A district court of the United States shall issue a nondisclosure order or extension thereof under this subsection if the court determines that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period may result in—

“(A) a danger to the national security of the United States;

“(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

“(C) interference with diplomatic relations; or

“(D) danger to the life or physical safety of any person.”

SEC. 503. JUDICIAL REVIEW.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

(2) by inserting after subsection (c) the following new subsection:

“(d) JUDICIAL REVIEW.—

“(1) IN GENERAL.—A request under subsection (b) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511.

“(2) NOTICE.—A request under subsection (b) shall include notice of the availability of judicial review described in paragraph (1).”.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection:

“(d) JUDICIAL REVIEW.—

“(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

“(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).”.

(c) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) by redesignating subsections (e) through (m) as subsections (f) through (n), respectively; and

(2) by inserting after subsection (d) the following new subsection:

“(e) JUDICIAL REVIEW.—

“(1) IN GENERAL.—A request under subsection (a) or (b) or an order under subsection (c) or a non-disclosure requirement imposed in connection with such request under subsection (d) shall be subject to judicial review under section 3511 of title 18, United States Code.

“(2) NOTICE.—A request under subsection (a) or (b) or an order under subsection (c) shall include notice of the availability of judicial review described in paragraph (1).”.

(d) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

(2) by inserting after subsection (c) the following new subsection:

“(d) JUDICIAL REVIEW.—

“(1) IN GENERAL.—A request under subsection (a) or a non-disclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

“(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).”.

(e) INVESTIGATIONS OF PERSONS WITH ACCESS TO CLASSIFIED INFORMATION.—Section 802 of the National Security Act of 1947 (50 U.S.C. 3162) is amended—

(1) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively; and

(2) by inserting after subsection (b) the following new subsection:

“(c) JUDICIAL REVIEW.—

“(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (b) shall be subject to judicial review under section 3511 of title 18, United States Code.

“(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).”.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

SEC. 601. ADDITIONAL REPORTING ON ORDERS REQUIRING PRODUCTION OF BUSINESS RECORDS; BUSINESS RECORDS COMPLIANCE REPORTS TO CONGRESS.

(a) REPORTS SUBMITTED TO COMMITTEES.—Section 502(b) (50 U.S.C. 1862(b)) is amended—

(1) by redesignating paragraphs (1), (2), and (3) as paragraphs (6), (7), and (8), respectively; and

(2) by inserting before paragraph (6) (as so redesignated) the following new paragraphs:

“(1) a summary of all compliance reviews conducted by the Government for the production of tangible things under section 501;

“(2) the total number of applications described in section 501(b)(2)(B) made for orders approving requests for the production of tangible things;

“(3) the total number of such orders either granted, modified, or denied;

“(4) the total number of applications described in section 501(b)(2)(C) made for orders approving requests for the production of call detail records;

“(5) the total number of such orders either granted, modified, or denied;”.

(b) REPORTING ON CERTAIN TYPES OF PRODUCTION.—Section 502(c)(1) (50 U.S.C. 1862(c)(1)) is amended—

(1) in subparagraph (A), by striking “and”;

(2) in subparagraph (B), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following new subparagraphs:

“(C) the total number of applications made for orders approving requests for the production of tangible things under section 501 in which the specific selection term does not specifically identify an individual, account, or personal device;

“(D) the total number of orders described in subparagraph (C) either granted, modified, or denied; and

“(E) with respect to orders described in subparagraph (D) that have been granted or modified, whether the court established under section 103 has directed additional, particularized minimization procedures beyond those adopted pursuant to section 501(g).”.

SEC. 602. ANNUAL REPORTS BY THE GOVERNMENT.

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by section 402 of this Act, is further amended by adding at the end the following new section:

“SEC. 603. ANNUAL REPORTS.

“(a) REPORT BY DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—

“(1) REPORT REQUIRED.—The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes—

“(A) the number of applications or certifications for orders submitted under each of sections 105, 304, 402, 501, 702, 703, and 704;

“(B) the number of such orders granted under each of those sections;

“(C) the number of orders modified under each of those sections;

“(D) the number of applications or certifications denied under each of those sections;

“(E) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each indi-

vidual appointed to serve as amicus curiae; and

“(F) the number of findings issued under section 103(i) that such appointment is not appropriate and the text of any such findings.

“(2) PUBLICATION.—The Director shall make the report required under paragraph (1) publicly available on an Internet Web site, except that the Director shall not make publicly available on an Internet Web site the findings described in subparagraph (F) of paragraph (1).

“(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—Except as provided in subsection (d), the Director of National Intelligence shall annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

“(1) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of the number of targets of such orders;

“(2) the total number of orders issued pursuant to section 702 and a good faith estimate of—

“(A) the number of search terms concerning a known United States person used to retrieve the unminimized contents of electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of search terms used to prevent the return of information concerning a United States person; and

“(B) the number of queries concerning a known United States person of unminimized noncontents information relating to electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of queries containing information used to prevent the return of information concerning a United States person;

“(3) the total number of orders issued pursuant to title IV and a good faith estimate of—

“(A) the number of targets of such orders; and

“(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

“(4) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

“(A) the number of targets of such orders; and

“(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

“(5) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

“(A) the number of targets of such orders;

“(B) the number of unique identifiers used to communicate information collected pursuant to such orders; and

“(C) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and

“(6) the total number of national security letters issued and the number of requests for information contained within such national security letters.

“(c) TIMING.—The annual reports required by subsections (a) and (b) shall be made publicly available during April of each year and include information relating to the previous calendar year.

“(d) EXCEPTIONS.—

“(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of paragraphs (3), (4), or (5) of subsection (b) is fewer than 500, it shall be expressed as a numerical

range of 'fewer than 500' and shall not be expressed as an individual number.

“(2) NONAPPLICABILITY TO CERTAIN INFORMATION.—

“(A) FEDERAL BUREAU OF INVESTIGATION.—Paragraphs (2)(A), (2)(B), and (5)(C) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

“(B) ELECTRONIC MAIL ADDRESS AND TELEPHONE NUMBERS.—Paragraph (3)(B) of subsection (b) shall not apply to orders resulting in the acquisition of information by the Federal Bureau of Investigation that does not include electronic mail addresses or telephone numbers.

“(3) CERTIFICATION.—

“(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subsection (b)(2)(B) cannot be determined accurately because some but not all of the relevant elements of the intelligence community are able to provide such good faith estimate, the Director shall—

“(i) certify that conclusion in writing to the Select Committee on Intelligence and the Committee on the Judiciary of the Senate and the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives;

“(ii) report the good faith estimate for those relevant elements able to provide such good faith estimate;

“(iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and

“(iv) make such certification publicly available on an Internet Web site.

“(B) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

“(C) TIMING.—If the Director of National Intelligence continues to conclude that the good faith estimates described in this paragraph cannot be determined accurately, the Director shall annually submit a certification in accordance with this paragraph.

“(e) DEFINITIONS.—In this section:

“(1) CONTENTS.—The term ‘contents’ has the meaning given that term under section 2510 of title 18, United States Code.

“(2) ELECTRONIC COMMUNICATION.—The term ‘electronic communication’ has the meaning given that term under section 2510 of title 18, United States Code.

“(3) NATIONAL SECURITY LETTER.—The term ‘national security letter’ means a request for a report, records, or other information under—

“(A) section 2709 of title 18, United States Code;

“(B) section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A));

“(C) subsection (a) or (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u(a), 1681u(b)); or

“(D) section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).

“(4) UNITED STATES PERSON.—The term ‘United States person’ means a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

“(5) WIRE COMMUNICATION.—The term ‘wire communication’ has the meaning given that term under section 2510 of title 18, United States Code.”

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents, as amended by section 402 of this Act, is further amended by inserting after the item relating to section 602, as added by section 402 of this Act, the following new item:

“Sec. 603. Annual reports.”.

(c) PUBLIC REPORTING ON NATIONAL SECURITY LETTERS.—Section 118(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 3511 note) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking “United States”; and

(B) in subparagraph (A), by striking “, excluding the number of requests for subscriber information”;

(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following:

“(2) CONTENT.—

“(A) IN GENERAL.—Except as provided in subparagraph (B), each report required under this subsection shall include a good faith estimate of the total number of requests described in paragraph (1) requiring disclosure of information concerning—

“(i) United States persons; and

“(ii) persons who are not United States persons.

“(B) EXCEPTION.—With respect to the number of requests for subscriber information under section 2709 of title 18, United States Code, a report required under this subsection need not separate the number of requests into each of the categories described in subparagraph (A).”.

(d) STORED COMMUNICATIONS.—Section 2702(d) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking “; and” and inserting a semicolon;

(2) in paragraph (2)(B), by striking the period and inserting “; and”; and

(3) by adding at the end the following new paragraph:

“(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).”.

SEC. 603. PUBLIC REPORTING BY PERSONS SUBJECT TO FISA ORDERS.

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by sections 402 and 602 of this Act, is further amended by adding at the end the following new section:

“SEC. 604. PUBLIC REPORTING BY PERSONS SUBJECT TO ORDERS.

“(a) REPORTING.—A person subject to a nondisclosure requirement accompanying an order or directive under this Act or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

“(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

“(A) the number of national security letters received, reported in bands of 1000 starting with 0-999;

“(B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0-999;

“(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 1000 starting with 0-999;

“(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents reported in bands of 1000 starting with 0-999;

“(E) the number of orders received under this Act for noncontents, reported in bands of 1000 starting with 0-999; and

“(F) the number of customer selectors targeted under orders under this Act for noncontents, reported in bands of 1000 starting with 0-999, pursuant to—

“(i) title IV;

“(ii) title V with respect to applications described in section 501(b)(2)(B); and

“(iii) title V with respect to applications described in section 501(b)(2)(C).

“(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

“(A) the number of national security letters received, reported in bands of 500 starting with 0-499;

“(B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0-499;

“(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0-499;

“(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0-499;

“(E) the number of orders received under this Act for noncontents, reported in bands of 500 starting with 0-499; and

“(F) the number of customer selectors targeted under orders received under this Act for noncontents, reported in bands of 500 starting with 0-499.

“(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply in the into separate categories of—

“(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0-249; and

“(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0-249.

“(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of—

“(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0-99; and

“(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0-99.

“(b) PERIOD OF TIME COVERED BY REPORTS.—

“(1) A report described in paragraph (1) or (2) of subsection (a) shall include only information—

“(A) relating to national security letters for the previous 180 days; and

“(B) relating to authorities under this Act for the 180-day period of time ending on the date that is not less than 180 days prior to the date of the publication of such report, except that with respect to a platform, product, or service for which a person did not previously receive an order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received.

“(2) A report described in paragraph (3) of subsection (a) shall include only information relating to the previous 180 days.

“(3) A report described in paragraph (4) of subsection (a) shall include only information for the 1-year period of time ending on the date that is not less than 1 year prior to the date of the publication of such report.

“(c) OTHER FORMS OF AGREED TO PUBLICATION.—Nothing in this section prohibits the Government and any person from jointly agreeing to the publication of information referred to in this subsection in a time, form, or manner other than as described in this section.

“(d) DEFINITIONS.—In this section:

“(1) CONTENTS.—The term ‘contents’ has the meaning given that term under section 2510 of title 18, United States Code.

“(2) NATIONAL SECURITY LETTER.—The term ‘national security letter’ has the meaning given that term under section 603.”.

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents, as amended by sections 402 and 602 of this Act, is further amended by inserting after the item relating to section 603, as added by section 602 of this Act, the following new item:

“Sec. 604. Public reporting by persons subject to orders.”.

SEC. 604. REPORTING REQUIREMENTS FOR DECISIONS, ORDERS, AND OPINIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.

Section 601(c)(1) (50 U.S.C. 1871(c)(1)) is amended to read as follows:

“(1) not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues a decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act, a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion; and”.

SEC. 605. SUBMISSION OF REPORTS UNDER FISA.

(a) ELECTRONIC SURVEILLANCE.—Section 108(a)(1) (50 U.S.C. 1808(a)(1)) is amended by striking “the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate,” and inserting “the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate”.

(b) PHYSICAL SEARCHES.—The matter preceding paragraph (1) of section 306 (50 U.S.C. 1826) is amended—

(1) in the first sentence, by striking “Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the Senate,” and inserting “Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate”; and

(2) in the second sentence, by striking “and the Committee on the Judiciary of the House of Representatives”.

(c) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 406(b) (50 U.S.C. 1846(b)) is amended—

(1) in paragraph (2), by striking “; and” and inserting a semicolon;

(2) in paragraph (3), by striking the period and inserting a semicolon; and

(3) by adding at the end the following new paragraphs:

“(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing

or approving the installation and use of a pen register or trap and trace device under this title; and

“(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3).”.

(d) ACCESS TO CERTAIN BUSINESS RECORDS AND OTHER TANGIBLE THINGS.—Section 502(a) (50 U.S.C. 1862(a)) is amended by striking “Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate” and inserting “Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate”.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

SEC. 701. EMERGENCIES INVOLVING NON-UNITED STATES PERSONS.

(a) IN GENERAL.—Section 105 (50 U.S.C. 1805) is amended—

(1) by redesignating subsections (f), (g), (h), and (i) as subsections (g), (h), (i), and (j), respectively; and

(2) by inserting after subsection (e) the following:

“(f)(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-United States person previously believed to be located outside the United States for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this title or to title III of this Act, provided that the head of an element of the intelligence community—

“(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person;

“(B) promptly notifies the Attorney General of a determination under subparagraph (A); and

“(C) requests, as soon as practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), as warranted.

“(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

“(A) The employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e).

“(B) An issuance of a court order under this title or title III of this Act.

“(C) The Attorney General provides direction that the acquisition be terminated.

“(D) The head of the element of the intelligence community conducting the acquisition determines that a request under paragraph (1)(C) is not warranted.

“(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

“(3) Nonpublicly available information concerning unconsenting United States persons acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

“(4) If the Attorney General declines to authorize the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical

search pursuant to section 304(e), or a court order is not obtained under this title or title III of this Act, information obtained during the 72 hour acquisition time period under paragraph (1) shall not be retained, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(5) Paragraphs (5) and (6) of subsection (e) shall apply to this subsection.”.

(b) NOTIFICATION OF EMERGENCY EMPLOYMENT OF ELECTRONIC SURVEILLANCE.—Section 106(j) (50 U.S.C. 1806(j)) is amended by striking “section 105(e)” and inserting “subsection (e) or (f) of section 105”.

(c) REPORT TO CONGRESS.—Section 108(a)(2) (50 U.S.C. 1808(a)(2)) is amended—

(1) in subparagraph (B), by striking “and” at the end;

(2) in subparagraph (C), by striking the period at the end and inserting “; and”; and

(3) by adding at the end the following:

“(D) the total number of authorizations under section 105(f) and the total number of subsequent emergency employments of electronic surveillance under section 105(e) or emergency physical searches pursuant to section 301(e).”.

SEC. 702. PRESERVATION OF TREATMENT OF NON-UNITED STATES PERSONS TRAVELING OUTSIDE THE UNITED STATES AS AGENTS OF FOREIGN POWERS.

Section 101(b)(1) is amended—

(1) in subparagraph (A), by inserting before the semicolon at the end the following: “, irrespective of whether the person is inside the United States”; and

(2) in subparagraph (B)—

(A) by striking “of such person’s presence in the United States”; and

(B) by striking “such activities in the United States” and inserting “such activities”.

SEC. 703. IMPROVEMENT TO INVESTIGATIONS OF INTERNATIONAL PROLIFERATION OF WEAPONS OF MASS DESTRUCTION.

Section 101(b)(1) is further amended by striking subparagraph (E) and inserting the following new subparagraph (E):

“(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or”.

SEC. 704. INCREASE IN PENALTIES FOR MATERIAL SUPPORT OF FOREIGN TERRORIST ORGANIZATIONS.

Section 2339B(a)(1) of title 18, United States Code, is amended by striking “15 years” and inserting “20 years”.

SEC. 705. SUNSETS.

(a) USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005.—Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note) is amended by striking “June 1, 2015” and inserting “December 15, 2019”.

(b) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.—Section 6001(b)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 1801 note) is amended by striking “June 1, 2015” and inserting “December 15, 2019”.

(c) CONFORMING AMENDMENT.—Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note), as amended by subsection (a), is further amended by striking “sections 501, 502, and” and inserting “title V and section”.

TITLE VIII—SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A—Safety of Maritime Navigation

SEC. 801. AMENDMENT TO SECTION 2280 OF TITLE 18, UNITED STATES CODE.

Section 2280 of title 18, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1)(A)(i), by striking “a ship flying the flag of the United States” and inserting “a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46)”;

(B) in paragraph (1)(A)(ii), by inserting “, including the territorial seas” after “in the United States”; and

(C) in paragraph (1)(A)(iii), by inserting “, by a United States corporation or legal entity,” after “by a national of the United States”;

(2) in subsection (c), by striking “section 2(c)” and inserting “section 13(c)”;

(3) by striking subsection (d);

(4) by striking subsection (e) and inserting after subsection (c) the following:

“(d) **DEFINITIONS.**—As used in this section, section 2280a, section 2281, and section 2281a, the term—

“(1) ‘applicable treaty’ means—

“(A) the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;

“(B) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;

“(C) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;

“(D) International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;

“(E) the Convention on the Physical Protection of Nuclear Material, done at Vienna on 26 October 1979;

“(F) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;

“(G) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988;

“(H) International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997; and

“(I) International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9 December 1999;

“(2) ‘armed conflict’ does not include internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature;

“(3) ‘biological weapon’ means—

“(A) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes; or

“(B) weapons, equipment, or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict;

“(4) ‘chemical weapon’ means, together or separately—

“(A) toxic chemicals and their precursors, except where intended for—

“(i) industrial, agricultural, research, medical, pharmaceutical, or other peaceful purposes;

“(ii) protective purposes, namely those purposes directly related to protection against toxic chemicals and to protection against chemical weapons;

“(iii) military purposes not connected with the use of chemical weapons and not dependent on the use of the toxic properties of chemicals as a method of warfare; or

“(iv) law enforcement including domestic riot control purposes,

as long as the types and quantities are consistent with such purposes;

“(B) munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals specified in subparagraph (A), which would be released as a result of the employment of such munitions and devices; and

“(C) any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in subparagraph (B);

“(5) ‘covered ship’ means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country’s territorial sea with an adjacent country;

“(6) ‘explosive material’ has the meaning given the term in section 841(c) and includes explosive as defined in section 844(j) of this title;

“(7) ‘infrastructure facility’ has the meaning given the term in section 2332f(e)(5) of this title;

“(8) ‘international organization’ has the meaning given the term in section 831(f)(3) of this title;

“(9) ‘military forces of a state’ means the armed forces of a state which are organized, trained, and equipped under its internal law for the primary purpose of national defense or security, and persons acting in support of those armed forces who are under their formal command, control, and responsibility;

“(10) ‘national of the United States’ has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

“(11) ‘Non-Proliferation Treaty’ means the Treaty on the Non-Proliferation of Nuclear Weapons, done at Washington, London, and Moscow on 1 July 1968;

“(12) ‘Non-Proliferation Treaty State Party’ means any State Party to the Non-Proliferation Treaty, to include Taiwan, which shall be considered to have the obligations under the Non-Proliferation Treaty of a party to that treaty other than a Nuclear Weapon State Party to the Non-Proliferation Treaty;

“(13) ‘Nuclear Weapon State Party to the Non-Proliferation Treaty’ means a State Party to the Non-Proliferation Treaty that is a nuclear-weapon State, as that term is defined in Article IX(3) of the Non-Proliferation Treaty;

“(14) ‘place of public use’ has the meaning given the term in section 2332f(e)(6) of this title;

“(15) ‘precursor’ has the meaning given the term in section 229F(6)(A) of this title;

“(16) ‘public transport system’ has the meaning given the term in section 2332f(e)(7) of this title;

“(17) ‘serious injury or damage’ means—

“(A) serious bodily injury,

“(B) extensive destruction of a place of public use, State or government facility, infrastructure facility, or public transportation system, resulting in major economic loss, or

“(C) substantial damage to the environment, including air, soil, water, fauna, or flora;

“(18) ‘ship’ means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up;

“(19) ‘source material’ has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

“(20) ‘special fissionable material’ has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

“(21) ‘territorial sea of the United States’ means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law;

“(22) ‘toxic chemical’ has the meaning given the term in section 229F(8)(A) of this title;

“(23) ‘transport’ means to initiate, arrange or exercise effective control, including decisionmaking authority, over the movement of a person or item; and

“(24) ‘United States’, when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and all territories and possessions of the United States.”; and

(5) by inserting after subsection (d) (as added by paragraph (4) of this section) the following:

“(e) **EXCEPTIONS.**—This section shall not apply to—

“(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

“(2) activities undertaken by military forces of a state in the exercise of their official duties.

“(f) **DELIVERY OF SUSPECTED OFFENDER.**—The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under section 2280 or section 2280a may deliver such person to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. Before delivering such person to the authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney General as to what action to take. When delivering the person to a country which is a state party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master’s intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master’s possession that pertains to the alleged offense.

“(g)(1) **CIVIL FORFEITURE.**—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

“(2) **APPLICABLE PROCEDURES.**—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers,

agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.”.

SEC. 802. NEW SECTION 2280A OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding after section 2280 the following new section:

“§ 2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction

“(a) OFFENSES.—

“(1) IN GENERAL.—Subject to the exceptions in subsection (c), a person who unlawfully and intentionally—

“(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

“(i) uses against or on a ship or discharges from a ship any explosive or radioactive material, biological, chemical, or nuclear weapon or other nuclear explosive device in a manner that causes or is likely to cause death to any person or serious injury or damage;

“(ii) discharges from a ship oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death to any person or serious injury or damage; or

“(iii) uses a ship in a manner that causes death to any person or serious injury or damage;

“(B) transports on board a ship—

“(i) any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, death to any person or serious injury or damage for the purpose of intimidating a population, or compelling a government or an international organization to do or to abstain from doing any act;

“(ii) any biological, chemical, or nuclear weapon or other nuclear explosive device, knowing it to be a biological, chemical, or nuclear weapon or other nuclear explosive device;

“(iii) any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an International Atomic Energy Agency comprehensive safeguards agreement, except where—

“(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

“(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of the Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

“(iv) any equipment, materials, or software or related technology that significantly contributes to the design or manufacture of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

“(I) the country to the territory of which or under the control of which such item is transferred is a Nuclear Weapon State Party to the Non-Proliferation Treaty; and

“(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of a Non-Proliferation Treaty State Party from which, to the terri-

tory of which, or otherwise under the control of which such item is transferred;

“(v) any equipment, materials, or software or related technology that significantly contributes to the delivery of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

“(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

“(II) such item is intended for the delivery system of a nuclear weapon or other nuclear explosive device of a Nuclear Weapon State Party to the Non-Proliferation Treaty; or

“(vi) any equipment, materials, or software or related technology that significantly contributes to the design, manufacture, or delivery of a biological or chemical weapon, with the intention that it will be used for such purpose;

“(C) transports another person on board a ship knowing that the person has committed an act that constitutes an offense under section 2280 or subparagraph (A), (B), (D), or (E) of this section or an offense set forth in an applicable treaty, as specified in section 2280(d)(1), and intending to assist that person to evade criminal prosecution;

“(D) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (C), or subsection (a)(2), to the extent that the subsection (a)(2) offense pertains to subparagraph (A); or

“(E) attempts to do any act prohibited under subparagraph (A), (B) or (D), or conspires to do any act prohibited by subparagraphs (A) through (E) or subsection (a)(2), shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

“(2) THREATS.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A) shall be fined under this title, imprisoned not more than 5 years, or both.

“(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a)—

“(1) in the case of a covered ship, if—

“(A) such activity is committed—

“(i) against or on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) at the time the prohibited activity is committed;

“(ii) in the United States, including the territorial seas; or

“(iii) by a national of the United States, by a United States corporation or legal entity, or by a stateless person whose habitual residence is in the United States;

“(B) during the commission of such activity, a national of the United States is seized, threatened, injured, or killed; or

“(C) the offender is later found in the United States after such activity is committed;

“(2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; or

“(3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act.

“(c) EXCEPTIONS.—This section shall not apply to—

“(1) the activities of armed forces during an armed conflict, as those terms are under-

stood under the law of war, which are governed by that law; or

“(2) activities undertaken by military forces of a state in the exercise of their official duties.

“(d)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

“(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.”.

(b) CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 111 of title 18, United States Code, is amended by adding after the item relating to section 2280 the following new item:

“2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction.”.

SEC. 803. AMENDMENTS TO SECTION 2281 OF TITLE 18, UNITED STATES CODE.

Section 2281 of title 18, United States Code, is amended—

(1) in subsection (c), by striking “section 2(c)” and inserting “section 13(c)”;

(2) in subsection (d), by striking the definitions of “national of the United States,” “territorial sea of the United States,” and “United States”; and

(3) by inserting after subsection (d) the following:

“(e) EXCEPTIONS.—This section does not apply to—

“(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

“(2) activities undertaken by military forces of a state in the exercise of their official duties.”.

SEC. 804. NEW SECTION 2281A OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding after section 2281 the following new section:

“§ 2281a. Additional offenses against maritime fixed platforms

“(a) OFFENSES.—

“(1) IN GENERAL.—A person who unlawfully and intentionally—

“(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

“(i) uses against or on a fixed platform or discharges from a fixed platform any explosive or radioactive material, biological, chemical, or nuclear weapon in a manner that causes or is likely to cause death or serious injury or damage; or

“(ii) discharges from a fixed platform oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death or serious injury or damage;

“(B) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraph (A); or

“(C) attempts or conspires to do anything prohibited under subparagraph (A) or (B),

shall be fined under this title, imprisoned not more than 20 years, or both; and if death results to any person from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

“(2) **THREAT TO SAFETY.**—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A), shall be fined under this title, imprisoned not more than 5 years, or both.

“(b) **JURISDICTION.**—There is jurisdiction over the activity prohibited in subsection (a) if—

“(1) such activity is committed against or on board a fixed platform—

“(A) that is located on the continental shelf of the United States;

“(B) that is located on the continental shelf of another country, by a national of the United States or by a stateless person whose habitual residence is in the United States; or

“(C) in an attempt to compel the United States to do or abstain from doing any act;

“(2) during the commission of such activity against or on board a fixed platform located on a continental shelf, a national of the United States is seized, threatened, injured, or killed; or

“(3) such activity is committed against or on board a fixed platform located outside the United States and beyond the continental shelf of the United States and the offender is later found in the United States.

“(c) **EXCEPTIONS.**—This section does not apply to—

“(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

“(2) activities undertaken by military forces of a state in the exercise of their official duties.

“(d) **DEFINITIONS.**—In this section—

“(1) ‘continental shelf’ means the sea-bed and subsoil of the submarine areas that extend beyond a country’s territorial sea to the limits provided by customary international law as reflected in Article 76 of the 1982 Convention on the Law of the Sea; and

“(2) ‘fixed platform’ means an artificial island, installation, or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes.”

(b) **CONFORMING AMENDMENT.**—The table of sections at the beginning of chapter 111 of title 18, United States Code, is amended by adding after the item relating to section 2281 the following new item:

“2281a. Additional offenses against maritime fixed platforms.”

SEC. 805. ANCILLARY MEASURE.

Section 2332b(g)(5)(B) of title 18, United States Code, is amended by inserting “2280a (relating to maritime safety),” before “2281”, and by striking “2281” and inserting “2281 through 2281a”.

Subtitle B—Prevention of Nuclear Terrorism

SEC. 811. NEW SECTION 2332I OF TITLE 18, UNITED STATES CODE.

(a) **IN GENERAL.**—Chapter 113B of title 18, United States Code, is amended by adding after section 2332h the following:

“§ 2332i. Acts of nuclear terrorism

“(a) **OFFENSES.**—

“(1) **IN GENERAL.**—Whoever knowingly and unlawfully—

“(A) possesses radioactive material or makes or possesses a device—

“(i) with the intent to cause death or serious bodily injury; or

“(ii) with the intent to cause substantial damage to property or the environment; or

“(B) uses in any way radioactive material or a device, or uses or damages or interferes

with the operation of a nuclear facility in a manner that causes the release of or increases the risk of the release of radioactive material, or causes radioactive contamination or exposure to radiation—

“(i) with the intent to cause death or serious bodily injury or with the knowledge that such act is likely to cause death or serious bodily injury;

“(ii) with the intent to cause substantial damage to property or the environment or with the knowledge that such act is likely to cause substantial damage to property or the environment; or

“(iii) with the intent to compel a person, an international organization or a country to do or refrain from doing an act,

shall be punished as prescribed in subsection (c).

“(2) **THREATS.**—Whoever, under circumstances in which the threat may reasonably be believed, threatens to commit an offense under paragraph (1) shall be punished as prescribed in subsection (c). Whoever demands possession of or access to radioactive material, a device or a nuclear facility by threat or by use of force shall be punished as prescribed in subsection (c).

“(3) **ATTEMPTS AND CONSPIRACIES.**—Whoever attempts to commit an offense under paragraph (1) or conspires to commit an offense under paragraph (1) or (2) shall be punished as prescribed in subsection (c).

“(b) **JURISDICTION.**—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

“(1) the prohibited conduct takes place in the United States or the special aircraft jurisdiction of the United States;

“(2) the prohibited conduct takes place outside of the United States and—

“(A) is committed by a national of the United States, a United States corporation or legal entity or a stateless person whose habitual residence is in the United States;

“(B) is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed; or

“(C) is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States;

“(3) the prohibited conduct takes place outside of the United States and a victim or an intended victim is a national of the United States or a United States corporation or legal entity, or the offense is committed against any state or government facility of the United States; or

“(4) a perpetrator of the prohibited conduct is found in the United States.

“(c) **PENALTIES.**—Whoever violates this section shall be fined not more than \$2,000,000 and shall be imprisoned for any term of years or for life.

“(d) **NONAPPLICABILITY.**—This section does not apply to—

“(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

“(2) activities undertaken by military forces of a state in the exercise of their official duties.

“(e) **DEFINITIONS.**—As used in this section, the term—

“(1) ‘armed conflict’ has the meaning given that term in section 2332f(e)(11) of this title;

“(2) ‘device’ means:

“(A) any nuclear explosive device; or

“(B) any radioactive material dispersal or radiation-emitting device that may, owing to its radiological properties, cause death, serious bodily injury or substantial damage to property or the environment;

“(3) ‘international organization’ has the meaning given that term in section 831(f)(3) of this title;

“(4) ‘military forces of a state’ means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

“(5) ‘national of the United States’ has the meaning given that term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

“(6) ‘nuclear facility’ means:

“(A) any nuclear reactor, including reactors on vessels, vehicles, aircraft or space objects for use as an energy source in order to propel such vessels, vehicles, aircraft or space objects or for any other purpose;

“(B) any plant or conveyance being used for the production, storage, processing or transport of radioactive material; or

“(C) a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material;

“(7) ‘nuclear material’ has the meaning given that term in section 831(f)(1) of this title;

“(8) ‘radioactive material’ means nuclear material and other radioactive substances that contain nuclides that undergo spontaneous disintegration (a process accompanied by emission of one or more types of ionizing radiation, such as alpha-, beta-, neutron particles and gamma rays) and that may, owing to their radiological or fissile properties, cause death, serious bodily injury or substantial damage to property or to the environment;

“(9) ‘serious bodily injury’ has the meaning given that term in section 831(f)(4) of this title;

“(10) ‘state’ has the same meaning as that term has under international law, and includes all political subdivisions thereof;

“(11) ‘state or government facility’ has the meaning given that term in section 2332f(e)(3) of this title;

“(12) ‘United States corporation or legal entity’ means any corporation or other entity organized under the laws of the United States or any State, Commonwealth, territory, possession or district of the United States;

“(13) ‘vessel’ has the meaning given that term in section 1502(19) of title 33; and

“(14) ‘vessel of the United States’ has the meaning given that term in section 70502 of title 46.”

(b) **CLERICAL AMENDMENT.**—The table of sections at the beginning of chapter 113B of title 18, United States Code, is amended by inserting after the item relating to section 2332h the following:

“2332i. Acts of nuclear terrorism.”

(c) **DISCLAIMER.**—Nothing contained in this section is intended to affect the applicability of any other Federal or State law that might pertain to the underlying conduct.

(d) **INCLUSION IN DEFINITION OF FEDERAL CRIMES OF TERRORISM.**—Section 2332b(g)(5)(B) of title 18, United States Code, is amended by inserting “2332i (relating to acts of nuclear terrorism),” before “2339 (relating to harboring terrorists)”.

SEC. 812. AMENDMENT TO SECTION 831 OF TITLE 18, UNITED STATES CODE.

Section 831 of title 18, United States Code, is amended—

(a) in subsection (a)—

(1) by redesignating paragraphs (3) through (8) as paragraphs (4) through (9);

(2) by inserting after paragraph (2) the following:

“(3) without lawful authority, intentionally carries, sends or moves nuclear material into or out of a country;”;

(3) in paragraph (8), as redesignated, by striking “an offense under paragraph (1), (2), (3), or (4)” and inserting “any act prohibited under paragraphs (1) through (5);” and

(4) in paragraph (9), as redesignated, by striking “an offense under paragraph (1), (2), (3), or (4)” and inserting “any act prohibited under paragraphs (1) through (7);”;

(b) in subsection (b)—

(1) in paragraph (1), by striking “(7)” and inserting “(8);” and

(2) in paragraph (2), by striking “(8)” and inserting “(9);”;

(c) in subsection (c)—

(1) in subparagraph (2)(A), by adding after “United States” the following: “or a stateless person whose habitual residence is in the United States”;;

(2) by striking paragraph (5);

(3) in paragraph (4), by striking “or” at the end; and

(4) by inserting after paragraph (4), the following:

“(5) the offense is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed;

“(6) the offense is committed outside the United States and against any state or government facility of the United States; or

“(7) the offense is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States.”;

(d) by redesignating subsections (d) through (f) as (e) through (g), respectively;

(e) by inserting after subsection (c) the following:

“(d) NONAPPLICABILITY.—This section does not apply to—

“(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

“(2) activities undertaken by military forces of a state in the exercise of their official duties.”; and

(f) in subsection (g), as redesignated—

(1) in paragraph (6), by striking “and” at the end;

(2) in paragraph (7), by striking the period at the end and inserting a semicolon; and

(3) by inserting after paragraph (7), the following:

“(8) the term ‘armed conflict’ has the meaning given that term in section 2332f(e)(11) of this title;

“(9) the term ‘military forces of a state’ means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

“(10) the term ‘state’ has the same meaning as that term has under international law, and includes all political subdivisions thereof;

“(11) the term ‘state or government facility’ has the meaning given that term in section 2332f(e)(3) of this title; and

“(12) the term ‘vessel of the United States’ has the meaning given that term in section 70502 of title 46.”.

The SPEAKER pro tempore. The gentleman from Virginia (Mr. GOODLATTE) and the gentleman from Michigan (Mr. CONYERS) each will control 30 minutes.

The Chair recognizes the gentleman from Virginia.

GENERAL LEAVE

Mr. GOODLATTE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous materials on H.R. 2048, currently under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Virginia?

There was no objection.

Mr. GOODLATTE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, as we speak, thousands—no, millions—of telephone metadata records are flowing into the NSA on a daily basis, 24 hours a day, 7 days a week. Despite changes to the NSA bulk telephone metadata program announced by President Obama last year, the bulk collection of the records has not ceased and will not cease unless and until Congress acts to shut it down.

Not even last week’s decision by the Second Circuit Court of Appeals will end this collection. The responsibility falls to us, and today we must answer the call and the will of the American people to do just that.

When we set out to reform this program 1 year ago, I made the pledge to my colleagues in Congress and to the American people that Americans’ liberty and America’s security can coexist, that these fundamental concepts are not mutually exclusive. They are embedded in the very fabric that makes this Nation great and that makes this Nation an example for the world.

Mr. Speaker, the legislation before the House today—H.R. 2048, the USA FREEDOM Act—protects these pillars of American democracy. It affirmatively ends the indiscriminate bulk collection of telephone metadata. But it goes much further than this. It prohibits the bulk collection of all records under section 215 of the PATRIOT Act, as well as under the FISA pen register trap and trace device statute and the National Security Letter statutes.

In place of the current bulk telephone metadata program, the USA FREEDOM Act creates a targeted program that allows the intelligence community to collect non-content call detail records held by the telephone companies, but only with the prior approval of the FISA court and subject to the “special selection term” limitation. The records provided to the government in response to queries will be limited to two “hops,” and the government’s handling of any records it acquires will be governed by minimization procedures approved by the FISA court.

The USA FREEDOM Act prevents government overreach by strengthening the definition of “specific selection term”—the mechanism used to prohibit bulk collection—to ensure the

government can collect the information it needs to further a national security investigation while also prohibiting large-scale, indiscriminate collection, such as data from an entire State, city, or ZIP Code.

The USA FREEDOM Act strengthens civil liberties and privacy protections by authorizing the FISA court to appoint an individual to serve as amicus curiae from a pool of experts to advise the court on matters of privacy and civil liberties, communications technology, and other technical or legal matters. It also codifies important procedures for recipients of National Security Letters to challenge nondisclosure requests.

The bill increases transparency by requiring declassification of all significant FISA court opinions and provides procedures for certified questions of law to the FISA court of review and the United States Supreme Court.

Additionally, Mr. Speaker, H.R. 2048 requires the Attorney General and the Director of National Intelligence to provide the public with detailed information about how the intelligence community uses these national security authorities, and provides even more robust transparency reporting by America’s technology companies.

The USA FREEDOM Act enhances America’s national security by closing loopholes that make it difficult for the government to track foreign terrorists and spies as they enter or leave the country; clarifying the application of FISA to foreign targets who facilitate the international proliferation of weapons of mass destruction; increasing the maximum penalties for material support of a foreign terrorist organization; and expanding the sunsets of the expiring PATRIOT Act provisions to December 2019.

From beginning to end, this is a carefully crafted, bipartisan bill that enjoys wide support. I would like to thank the sponsor of this legislation, Crime, Terrorism, Homeland Security, and Investigations Subcommittee Chairman JIM SENSENBRENNER; full committee Ranking Member JOHN CONYERS; and Courts, Intellectual Property, and the Internet Subcommittee Ranking Member JERRY NADLER for working together with me on this important bipartisan legislation.

I also want to thank the staffs of these Members for the many hours, weeks, yes, even months of hard work they have put into this effort. Furthermore, I would like to thank my staff, Caroline Lynch, the chief counsel of the Crime, Terrorism, Homeland Security, and Investigations Subcommittee, and Jason Herring, as well as Aaron Hiller with Mr. CONYERS and Bart Forsyth with Mr. SENSENBRENNER for their long hours and steadfast dedication to this legislation.

I urge my colleagues to support this bipartisan bill, and I reserve the balance of my time.

HOUSE OF REPRESENTATIVES,
PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

Washington, DC, May 4, 2015.

Hon. BOB GOODLATTE,
Chairman, Committee on the Judiciary, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN GOODLATTE: On April 30, 2015, the Committee on the Judiciary ordered H.R. 2048, the USA Freedom Act of 2015, reported to the House.

As you know, H.R. 2048 contains provisions that amend the Foreign Intelligence Surveillance Act, which is within the jurisdiction of the Permanent Select Committee on Intelligence. As a result of your prior consultation with the Committee, and in order to expedite the House's consideration of H.R. 2048, the Permanent Select Committee on Intelligence will waive further consideration of the bill.

The Committee takes this action only with the understanding that this procedural route should not be construed to prejudice the jurisdictional interest of the House Permanent Select Committee on Intelligence over this bill or any similar bill. Furthermore, this waiver should not be considered as precedent for consideration of matters of jurisdictional interest to the Committee in the future, including in connection with any subsequent consideration of the bill by the House. The Permanent Select Committee on Intelligence will seek conferees on the bill during any House-Senate conference that may be convened on this legislation.

Finally, I would ask that you include a copy of our exchange of letters on this matter in the Congressional Record during the House debate on H.R. 2048. I appreciate the constructive work between our committees on this matter and thank you for your consideration.

Sincerely,

DEVIN NUNES,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, May 7, 2015.

Hon. DEVIN NUNES,
Chairman, Permanent Select Committee on Intelligence, Washington, DC.

DEAR CHAIRMAN NUNES: Thank you for your letter regarding H.R. 2048, the "U.S.A. Freedom Act of 2015." As you noted, the Permanent Select Committee on Intelligence was granted an additional referral on the bill.

I am most appreciative of your decision to waive further consideration of H.R. 2048 so that it may proceed expeditiously to the House floor. I acknowledge that although you waived formal consideration of the bill, the Permanent Select Committee on Intelligence is in no way waiving its jurisdiction over the subject matter contained in those provisions of the bill that fall within your Rule X jurisdiction. Further, I understand the Committee reserves the right to seek the appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, for which you will have my support.

I will include a copy of your letter and this response in the Committee Report as well as in the Congressional Record during floor consideration of H.R. 2048.

Sincerely,

BOB GOODLATTE,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC, May 8, 2015.

Hon. BOB GOODLATTE,
Chairman, Committee on the Judiciary, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN GOODLATTE: On April 30, 2015, the Committee on the Judiciary ordered H.R. 2048, the USA FREEDOM Act, to be reported favorably to the House. As a result of your having consulted with the Committee on Financial Services concerning provisions of the bill that fall within our Rule X jurisdiction, I agree to discharge our committee from further consideration of the bill so that it may proceed expeditiously to the House floor.

The Committee on Financial Services takes this action with our mutual understanding that, by foregoing consideration of H.R. 2048 at this time, we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and that our committee will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues that fall within our Rule X jurisdiction. Our committee also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, and requests your support for any such request.

Finally, I would appreciate your response to this letter confirming this understanding with respect to H.R. 2048 and would ask that a copy of our exchange of letters on this matter be included in your committee's report to accompany the legislation and/or in the Congressional Record during floor consideration thereof.

Sincerely,

JEB HENSARLING,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, May 11, 2015.

Hon. JEB HENSARLING,
Chairman, Committee on Financial Services, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN HENSARLING: Thank you for your letter regarding H.R. 2048, the "U.S.A. Freedom Act of 2015." As you noted, the Committee on Financial Services was granted an additional referral on the bill.

I am most appreciative of your decision to waive further consideration of H.R. 2048 so that it may proceed expeditiously to the House floor. I acknowledge that although you waived formal consideration of the bill, the Committee on Financial Services is in no way waiving its jurisdiction over the subject matter contained in those provisions of the bill that fall within your Rule X jurisdiction. Further, I understand the Committee reserves the right to seek the appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, for which you will have my support.

I will include a copy of your letter and this response in the Congressional Record during floor consideration of H.R. 2048.

Sincerely,

BOB GOODLATTE,
Chairman.

Mr. CONYERS. Mr. Speaker, I yield myself such time as I may consume.

Ladies and gentlemen, with the passage of the USA FREEDOM Act today, the House will have done its part to enact historic and sweeping reforms to the government's surveillance program and powers. This legislation ends bulk

collection, creates a panel of experts to guide the Foreign Intelligence Surveillance Court, and mandates extensive government reporting.

Today we have a rare opportunity to restore a measure of restraint to surveillance programs that have simply gone too far. For years the government has read section 215 of the PATRIOT Act to mean that it may collect all domestic telephone records merely because some of them may be relevant at some time in the future.

Last week, endorsing a view that I and many of my colleagues have held for years, the Second Circuit Court of Appeals held that "the text of section 215 cannot bear the weight the government asks us to assign it, and it does not authorize the telephone metadata program."

Now, with section 215 set to expire on June 1, we have the opportunity—and the obligation—to act clearly and decisively and end the program that has infringed on our rights for far too long.

A vote in favor of the USA FREEDOM Act is an explicit rejection of the government's unlawful interpretation of section 215 and similar statutes. Put another way, a vote in favor of this bill is a vote to end dragnet surveillance in the United States.

Mr. Speaker, the ban on bulk collection contained in this legislation turns on the idea of a "specific selection term" and requires the government to limit the scope of production as narrowly as possible. This definition is much improved from the version of this bill that passed the House last Congress.

The bill further requires the government to declassify and publish all novel and significant opinions of the Foreign Intelligence Surveillance Court.

□ 1430

It also creates a panel of experts to advise the court on the protection of privacy and civil liberties, communications technology, and other legal and technical matters.

These changes, along with robust reporting requirements for the government and flexible reporting options for private companies, create a new and inescapable level of that all-important consideration of transparency. The government may one day again attempt to expand its surveillance power by clever legal argument, but it will no longer be allowed to do so in secret.

Mr. Speaker, there are Members of the House and Senate who oppose this bill because it does not include every reform to surveillance law that we can create, and then there are others who oppose it because it includes any changes to existing surveillance programs.

This bill represents a reasonable consensus, and it will accomplish the most sweeping set of reforms to government surveillance in nearly 40 years.

H.R. 2048 has earned the support of privacy advocates, private industry,

the White House, and the intelligence community. It ends dragnet surveillance and does so without diminishing in any way our ability to protect this country.

I want to extend my sincere thanks to Chairman GOODLATTE, to Mr. SENSENBRENNER of Wisconsin, and to Mr. NADLER of New York for working with me to bring a stronger version of the USA FREEDOM Act to the floor. I think we succeeded. I also want to thank Chairman NUNES and Ranking Member SCHIFF for helping us to reach this point.

I urge all of my colleagues to support H.R. 2048, and I reserve the balance of my time.

Mr. GOODLATTE. Mr. Speaker, at this time, it is my pleasure to yield 5 minutes to the gentleman from Wisconsin (Mr. SENSENBRENNER), the chairman of the Crime, Terrorism, Homeland Security, and Investigation Subcommittee and the chief sponsor of this legislation.

Mr. SENSENBRENNER. Mr. Speaker, you know you have drafted a strong bill when you unite both national security hawks and civil libertarians. The USA FREEDOM Act has done that. It also has the support of privacy groups, tech companies, and the intelligence community.

This bill is an extremely well-drafted compromise, the product of nearly 2 years of work. It effectively protects America's civil liberties and our national security. I am very proud of the USA FREEDOM Act and am confident it is the most responsible path forward.

I do not fault my colleagues who wish that this bill went further to protect our civil liberties. For years, the government has violated the privacy of innocent Americans, and I share your anger, but letting section 215 and other surveillance authorities expire would not only threaten our national security, it would also mean less privacy protections. I emphasize it would also mean less privacy protections.

The USA FREEDOM Act also ends bulk collections across all domestic surveillance authorities, not just section 215. It also expands transparency with increased reporting from both government and private companies. If the administration finds a new way to circumvent the law, Congress and the public will know. The bill also requires the FISC to declassify significant legal decisions, bringing an end to secret laws.

If the PATRIOT Act authorities expire and the FISC approves bulk collection under a different authority, how will the public know? Without the USA FREEDOM Act, they will not. Allowing the PATRIOT Act authorities to expire sounds like a civil libertarian victory, but it will actually mean less privacy and more risk—less privacy and more risk.

Now, to my colleagues who oppose the USA FREEDOM Act because they don't believe it does enough for national security, this bill is a significant

improvement over the status quo. Americans will be safer post USA FREEDOM than they would be if Congress passes a clean reauthorization of the expiring provisions.

I am not ignorant to the threats we face, but a clean reauthorization would be irresponsible. Congress never intended section 215 to allow bulk collection. That program is illegal and based on a blatant misinterpretation of the law. That said, the FREEDOM Act gives the intelligence community new tools to combat terrorism in more targeted and effective ways.

Specifically, the bill replaces the administration's bulk metadata collection with a targeted program to collect only the records the government needs without compromising the privacy of innocent Americans.

It includes new authorities to allow the administration to expedite emergency requests under section 215 and fills holes in our surveillance law that require intelligence agencies to go dark on known terrorists or spies when they transit from outside to inside the U.S. or vice versa.

Under current law, the administration has to temporarily stop monitoring persons of interest as it shifts between domestic and international surveillance authorities. What is more likely to stop the next terrorist attack: the bulk collection of innocent Americans or the ability to track down a known terrorist as soon as he or she enters the United States?

If you answer that question the same way I do, then don't let the bluster and fear-mongering of the bill's opponents convince you we are safer with a clean reauthorization than we are with this bill.

Attorney General Lynch and Director of National Intelligence Clapper recognize this. In a recent letter of support, they wrote:

The significant reforms contained in this legislation will provide the public greater confidence in how our intelligence activities are carried out and in the oversight of those activities, while ensuring vital national security authorities remain in place.

Let's not kill these important reforms because we wish this bill did more. There is no perfect. Every bill we vote on could do more. I play the lottery. When I win, I don't throw away the winning ticket because I wish the jackpot were higher.

It is time to pass the USA FREEDOM Act. I am asking all my colleagues—Democrats and Republicans, security hawks, and civil libertarians—to vote for it. Let's speak with one voice in the House of Representatives and together urge the United States Senate to work quickly and adopt these important reforms.

Mr. CONYERS. Mr. Speaker, I am pleased now to yield 3 minutes to the gentleman from New York (Mr. NADLER), to recognize his indefatigable work, a senior member of the Judiciary Committee.

Mr. NADLER. Mr. Speaker, I thank the chairman.

Mr. Speaker, the USA FREEDOM Act represents a return to the basic principle of the Fourth Amendment, the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.

Before the government may search our homes, seize our persons, or intercept our communications, it must first make a showing of individualized suspicion. The intrusion it requests must be as targeted and as brief as circumstances allow. The Fourth Amendment demands no less.

That is why we are here today. We have learned that the government has engaged in unreasonable searches against all of us. It has gathered an enormous amount of information about every phone call in the United States. It has deemed all of our phone calls relevant to a terrorism investigation. It is intolerable to our sense of freedom.

Today, we are acting to stop it. The bill before us prohibits the intelligence community from engaging in bulk data collection within the United States.

This practice, the dragnet collection without a warrant of telephone records and Internet metadata, is the contemporary equivalent of the British writs of assistance that early American revolutionaries opposed and that the Fourth Amendment was drafted to outlaw. It has never complied with the Constitution and must be brought to an end without delay.

The legal theories that justified these programs were developed and approved in secret, and that practice must also come to an end. There must not be a body of secret law in the United States.

Section 215 says tangible things may be seized if they are relevant to a terrorism investigation. The government's interpretation that this means "everything" is obviously wrong, could only have been advanced in secret, and cannot withstand the public scrutiny to which it is now subjected. The Second Circuit Court of Appeals threw out this notion last week, and now, we must do so as well.

This bill further requires the government to promptly declassify and release each novel or significant opinion of the Foreign Intelligence Surveillance Court. In the future, if the government advances a similarly dubious legal claim, there will be an advocate in court to oppose it. If the court should agree with the novel claim, the public will know about it almost immediately, and the responsibility will lie with us to correct it just as quickly.

Before I close, I want to be clear. Not every reform I would have hoped to enact is included in this bill. We must do more to protect U.S. person information collected under section 702 of FISA. We must act to reform other authorities, many of them law enforcement rather than intelligence community authorities, to prevent indiscriminate searches in other circumstances.

I will continue to fight for these reforms, among others, and I know that I

will not be alone in taking up that challenge in the days to come, but I am grateful that we have the opportunity to take this first major step to restore the right of the people to be secure in their persons, houses, papers, and effects and to do so without in any way endangering national security.

I thank Chairman GOODLATTE, Chairman SENSENBRENNER, and Ranking Member CONYERS for their continued leadership on this legislation, and I urge every one of my colleagues to support this bill.

Mr. GOODLATTE. Mr. Speaker, I yield myself such time as I may consume.

Before I yield to the next speaker, I want to say to him and his colleagues on the House Intelligence Committee that they did marvelous work in protecting not only the national security, but the civil liberties of Americans.

They worked with the Judiciary Committee together to prove that we can have very high levels of civil liberty and very high levels of national security. I thank Chairman NUNES and his staff for that outstanding work.

Now, it is my pleasure to yield 3 minutes to the gentleman from California (Mr. NUNES), the chairman of the House Intelligence Committee.

Mr. NUNES. Mr. Speaker, I rise in support of H.R. 2048, the USA FREEDOM Act of 2015.

Ideally, we would reauthorize section 215 of the U.S. PATRIOT Act and other expiring FISA authorities without making any changes. These provisions authorize important counterterrorism programs, including the NSA bulk telephone metadata program.

What is more, they are constitutional, authorized by Congress, and subject to multiple layers of oversight from all three branches of government. As threats to Americans at home and abroad increase by the day, now is not the time to be weakening our national security with all the tragic consequences that may follow.

However, I also realize that some of my colleagues disagree. Despite the fact that the NSA bulk telephone metadata program has never been intentionally misused, many Members wish to make changes to increase confidence in the program and allow greater transparency into intelligence activities.

Like the bill the House passed last year with more than 300 votes, this bill would replace the bulk program that will expire on June 1 with a targeted authority. This new targeted authority will be slower and potentially less effective than the current program. Along with Ranking Member SCHIFF, I have worked with the Judiciary Committee to ensure these changes still allow as much operational flexibility as possible.

Chairman GOODLATTE, Ranking Member CONYERS, and Subcommittee Chairman SENSENBRENNER, thank you for the constructive work between our committees.

In addition, the USA FREEDOM Act of 2015 contains several significant measures to improve national security that were not part of last year's bill. It closes a loophole in current law that requires the government to stop monitoring the communications of foreign terrorists, including ISIL fighters from Syria and Iraq, when they enter the United States.

It streamlines the process for the government to track foreign spies who temporarily leave the United States. It helps the government investigate proliferators of weapons of mass destruction. It increases the maximum sentence for material support to a foreign terrorist organization.

Those changes are real improvements that will make it easier for our intelligence and law enforcement agencies to keep Americans safe.

Again, I would prefer a clean reauthorization, but the bill we consider today is the best way forward in the House to ensure Congress takes responsible action to protect national security. I urge my colleagues to support it.

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS,
Washington, DC, May 4, 2015.

Hon. DEVIN NUNES,
Chairman, Permanent Select Committee on Intelligence,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I write regarding H.R. 2048, the "USA Freedom Act," which was recently ordered reported by the Judiciary Committee, to provide perspectives on the legislation, particularly an assessment that the pending version of the bill could impede the effective operation of the Foreign Intelligence Surveillance Courts.

In letters to the Committee on January 13, 2014 and May 13, 2014, we commented on various proposed changes to the Foreign Intelligence Surveillance Act (FISA). Our comments focused on the operational impact of certain proposed changes on the Judicial Branch, particularly the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review (collectively "FISA Courts"), but did not express views on core policy choices that the political branches are considering regarding intelligence collection. In keeping with that approach, we offer views on aspects of H.R. 2048 that bear directly on the work of the FISA Courts and how that work is presented to the public. We sincerely appreciate the ongoing efforts of the bipartisan leadership of all the congressional committees of jurisdiction to listen to and attempt to accommodate our perspectives and concerns.

We respectfully request that, if possible, this letter be included with your Committee's report to the House on the bill.

SUMMARY OF CONCERNS

We have three main concerns. First, H.R. 2048 proposes a "panel of experts" for the FISA Courts which could, in our assessment, impair the courts' ability to protect civil liberties by impeding their receipt of complete and accurate information from the government (in contrast to the helpful amicus curiae approach contained in the FISA Improvements Act of 2013 ("FIA"), which was approved in similar form by the House in 2014). Second, we continue to have concerns with the prospect of public "summaries" of FISA Courts' opinions when the opinions themselves are not released to the public.

Third, we have a few other specific technical concerns with H.R. 2048 as drafted.

NATURE OF THE FISA COURTS

With the advent of a new Congress and newly proposed legislation, it seems helpful to restate briefly some key attributes of the work of the FISA Courts.

The vast majority of the work of the FISC involves individual applications in which experienced judges apply well-established law to a set of facts presented by the government—a process not dissimilar to the ex parte consideration of ordinary criminal search warrant applications. Review of entire programs of collection and applications involving bulk collection are a relatively small part of the docket, and applications involving novel legal questions, though obviously important, are rare.

In all matters, the FISA Courts currently depend on—and will always depend on—prompt and complete candor from the government in providing the courts with all relevant information because the government is typically the only source of such information.

A "read copy" practice—similar to the practices employed in some federal district courts for Title III wiretap applications—wherein the government provides the FISC with an advance draft of each planned application, is the major avenue for court modification of government-sought surveillance. About a quarter of "read copies" are modified or withdrawn at the instigation of the FISC before the government presents a final application—in contrast to the overwhelming majority of formal applications that are approved by the Court because modifications at the "read copy" stage have addressed the Court's concerns in cases where final applications are submitted.

The FISC typically operates in an environment where, for national security reasons and because of statutory requirements, time is of the essence, and collateral litigation, including for discovery, would generally be completely impractical.

At times, the FISA Courts are presented with challenging issues regarding how existing law applies to novel technologies. In these instances, the FISA Courts could benefit from a conveniently available explanation or evaluation of the technology from an informed non-government source. Congress could assist in this regard by clarifying the law to provide mechanisms for this to occur easily (e.g., by providing for pre-cleared experts with whom the Court can share and receive information to the extent it deems necessary).

THE "PANEL OF EXPERTS" APPROACH OF H.R. 2048 COULD IMPEDE THE FISA COURTS' WORK

H.R. 2048 provides for what proponents have referred to as a "panel of experts" and what in the bill is referred to as a group of at least five individuals who may serve as an "amicus curiae" in a particular matter. However, unlike a true amicus curiae, the FISA Courts would be required to appoint such an individual to participate in any case involving a "novel or significant interpretation of law" (emphasis added)—unless the court "issues a finding" that appointment is not appropriate. Once appointed, such amici are required to present to the court, "as appropriate," legal arguments in favor of privacy, information about technology, or other "relevant" information. Designated amici are required to have access to "all relevant" legal precedent, as well as certain other materials "the court determines are relevant."

Our assessment is that this "panel of experts" approach could impede the FISA Courts' role in protecting the civil liberties of Americans. We recognize this may not be the intent of the drafters, but nonetheless it

is our concern. As we have indicated, the full cooperation of rank-and-file government personnel in promptly conveying to the FISA Courts complete and candid factual information is critical. A perception on their part that the FISA process involves a “panel of experts” officially charged with opposing the government’s efforts could risk deterring the necessary and critical cooperation and candor. Specifically, our concern is that imposing the mandatory “duties”—contained in subparagraph (i)(4) of proposed section 401 (in combination with a quasi-mandatory appointment process)—could create such a perception within the government that a standing body exists to oppose intelligence activities.

Simply put, delays and difficulties in receiving full and accurate information from Executive Branch agencies (including, but not limited to, cases involving non-compliance) present greater challenges to the FISA Courts’ role in protecting civil liberties than does the lack of a non-governmental perspective on novel legal issues or technological developments. To be sure, we would welcome a means of facilitating the FISA Courts’ obtaining assistance from nongovernmental experts in unusual cases, but it is critically important that the means chosen to achieve that end do not impair the timely receipt of complete and accurate information from the government.

It is on this point especially that we believe the “panel of experts” system in H.R. 2048 may prove counterproductive. The information that the FISA Courts need to examine probable cause, evaluate minimization and targeting procedures, and determine and enforce compliance with court authorizations and orders is exclusively in the hands of the government—specifically, in the first instance, intelligence agency personnel. If disclosure of sensitive or adverse information to the FISA Courts came to be seen as a prelude to disclosure to a third party whose mission is to oppose or curtail the agency’s work, then the prompt receipt of complete and accurate information from the government would likely be impaired—ultimately to the detriment of the national security interest in expeditious action and the effective protection of privacy and civil liberties.

In contrast, a “true” *amicus curiae* approach, as adopted, for example, in the FIA, facilitates appointment of experts outside the government to serve as *amici curiae* and render any form of assistance needed by the court, without any implication that such experts are expected to oppose the intelligence activities proposed by the government. For that reason, we do not believe the FIA approach poses any similar risk to the courts’ obtaining relevant information.

“SUMMARIES” OF UNRELEASED FISA COURT
OPINIONS COULD MISLEAD THE PUBLIC

In our May 13, 2014, letter to the Committee on H.R. 3361, we shared the nature of our concerns regarding the creation of public “summaries” of court opinions that are not themselves released. The provisions in H.R. 2048 are similar and so are our concerns. To be clear, the FISA Courts have never objected to their opinions—whether in full or in redacted form—being released to the public to the maximum extent permitted by the Executive’s assessment of national security concerns. Likewise, the FISA Courts have always facilitated the provision of their full opinions to Congress. *See, e.g.,* FISC Rule of Procedure 62(c). Thus, we have no objection to the provisions in H.R. 2048 that call for maximum public release of court opinions. However, a formal practice of creating summaries of court opinions without the underlying opinion being available is unprece-

dented in American legal administration. Summaries of court opinions can be inadvertently incorrect or misleading, and may omit key considerations that can prove critical for those seeking to understand the import of the court’s full opinion. This is particularly likely to be a problem in the fact-focused area of FISA practice, under circumstances where the government has already decided that it cannot release the underlying opinion even in redacted form, presumably because the opinion’s legal analysis is inextricably intertwined with classified facts.

ADDITIONAL TECHNICAL COMMENTS ON H.R. 2048

The Judiciary, like the public, did not participate in the discussions between the Administration and congressional leaders that led to H.R. 2048 (publicly released on April 28, 2015 and reported by the Judiciary Committee without changes on April 30). In the few days we have had to review the bill, we have noted a few technical concerns that we hope can be addressed prior to finalization of the legislation, should Congress choose to enact it. These concerns (all in the *amicus curiae* subsection) include:

Proposed subparagraph (9) appears inadvertently to omit the ability of the FISA Courts to train and administer *amici* between the time they are designated and the time they are appointed.

Proposed subparagraph (6) dots not make any provision for a “true *amicus*” appointed under subparagraph (2)(B) to receive necessary information.

We are concerned that a lack of parallel construction in proposed clause (6)(A)(i) (apparently differentiating between access to legal precedent as opposed to access to other materials) could lead to confusion in its application.

We recommend adding additional language to clarify that the exercise of the duties under proposed subparagraph (4) would occur in the context of Court rules (for example, deadlines and service requirements).

We believe that slightly greater clarity could be provided regarding the nature of the obligations referred to in proposed subparagraph (10).

These concerns would generally be avoided or addressed by substituting the FIA approach. Furthermore, it bears emphasis that, even if H.R. 2048 were amended to address all of these technical points, our more fundamental concerns about the “panel of experts” approach would not be fully assuaged. Nonetheless, our staff stands ready to work with your staff to provide suggested textual changes to address each of these concerns.

Finally, although we have no particular objection to the requirement in this legislation of a report by the Director of the AO, Congress should be aware that the AO’s role would be to receive information from the FISA Courts and then simply transmit the report as directed by law.

For the sake of brevity, we are not restating here all the comments in our previous correspondence to Congress on proposed legislation similar to H.R. 2048. However, the issues raised in those letters continue to be of importance to us.

We hope these comments are helpful to the House of Representatives in its consideration of this legislation. If we may be of further assistance in this or any other matter, please contact me or our Office of Legislative Affairs.

Sincerely,

JAMES C. DUFF,
Director.

□ 1445

Mr. CONYERS. Mr. Speaker, I am pleased to yield 2½ minutes to the gen-

tlewoman from California (Ms. LOFGREN), an effective member of the House Judiciary Committee.

Ms. LOFGREN. Mr. Speaker, I believe this bill makes meaningful reform to a few of the surveillance programs, but it in no way stops all of the bulk collection of U.S. person communications currently occurring. This bill won’t stop the most egregious and widely reported privacy violations that occur under section 702 and Executive Order No. 12333.

In a declassified decision, the FISA court said that the NSA had been collecting substantially more U.S. person communications through its upstream collection program than it had originally told the court. With upstream collection, the NSA directly taps into international Internet cables to search through all of the communications that flow through it, looking for communications that map certain criteria.

Four years ago, the court found that the government was collecting tens of thousands of wholly domestic communications a year. Why? Because all of your data is everywhere. No accurate estimate can be given for the even larger number of communications collected in which a U.S. person was a party to the communication.

The Director of National Intelligence confirmed the government searches this vast amount of data, including the content of email and of telephone calls, without individualized suspicion, probable cause, and without a warrant. The Director of the FBI says they use information to build criminal cases against U.S. persons. This is an end run around the Fourth Amendment, and it has to stop.

This bill did not create those problems. However, this bill doesn’t correct those problems. During the markup of the bill, Chairman GOODLATTE stated that these issues would be next, but we can’t afford to wait until the final hour of expiration to take action like we did with this bill. To do so would mean at least another 2 years of the mass surveillance of Americans, which is unconscionable. Last year, the House voted 293–123 to close these backdoor loopholes, but the Rules Committee would not allow the House to vote today to put these fixes into this bill.

I voted in committee to advance this bill for a couple of reasons, and I do want to thank all of the members who worked on this but single out Congressman JIM SENSENBRENNER, who was the author of the bill and who has worked so hard to make sure that improvements are made. The bill is an improvement over a straight reauthorization of the bill. I also listened carefully to the verbal commitments that the 702 fix would be included, and I reserve the right to oppose this bill when it comes back from the Senate if we can’t close these loopholes.

Mr. GOODLATTE. Mr. Speaker, I am pleased to yield 2 minutes to the gentleman from Virginia (Mr. FORBES), a

member of the House Judiciary Committee and an original cosponsor of this legislation.

Mr. FORBES. I thank the chairman.

Mr. Speaker, I rise today in support of the USA FREEDOM Act, which passed the Judiciary Committee with bipartisan support just 2 weeks ago.

The bill accomplishes the twin goals of protecting our Nation from our enemies while safeguarding the civil liberties that our servicemembers fight for every day.

Americans across the country have called for the NSA to listen less and elected officials to listen more. The USA FREEDOM Act will end the NSA's bulk collection program, which was established under section 215 of the PATRIOT Act, and it will further protect Americans' Fourth Amendment rights by strengthening oversight and accountability of the intelligence community.

As a member of the House Armed Services Committee, I work with our servicemembers and military leaders daily to ensure our adversaries do not harm this great Nation. That is why I applaud Chairman GOODLATTE and Mr. SENSENBRENNER for including provisions in the bill to address the growing threat of ISIL.

With continued threats of terrorism, our Nation's intelligence community must be equipped to protect our Nation and national security interests. However, any intelligence framework must be confined within the boundaries of the United States Constitution. Striking this balance between safeguarding privacy and protecting Americans is a challenge in today's post-9/11 world, but it is one that should not tip towards allowing the government to trample on our constitutional rights. Security must not come at the cost of Americans' liberties. That is why I urge my colleagues today to support this bill.

Mr. CONYERS. Mr. Speaker, I am pleased to yield 2½ minutes to the distinguished gentlewoman from Texas (Ms. JACKSON LEE).

Ms. JACKSON LEE. Let me thank the ranking member and the chairman of the full committee. As my colleagues have done, let me also acknowledge the chairman of the Crime Subcommittee, Mr. SENSENBRENNER, on which I serve as the ranking member. As many have noted, let me acknowledge the work of Mr. GOODLATTE and Mr. CONYERS and their leadership on a very important statement on behalf of the American people.

Mr. Speaker, the USA FREEDOM Act is the House's unified response to the unauthorized disclosures and subsequent publication in the media in June 2013 regarding the National Security Agency's collection from Verizon of the phone records of all of its American customers which were authorized by the FISA court pursuant to section 215 of the PATRIOT Act.

You can imagine, Mr. Speaker, the public was not happy. There was jus-

tifiable concern on the part of the public and by a large percentage of the Members of this body that the extent and scale of the NSA data collection bundling, which, by orders of magnitude, exceeded anything previously authorized or contemplated, may have constituted an unwarranted invasion of privacy and a threat to the civil liberties of Americans.

Mr. Speaker, I have been a decade-plus-long member of the Homeland Security Committee. I do not in any way want to infringe upon the security of this Nation, but if we allow the terrorists to terrorize us, then we are in very bad shape, and I am glad the voices of opposition were raised.

To quell the growing controversy, the Director of National Intelligence declassified and released limited information about the program, but it did not, by any means, satisfy the concern raised by Americans. The DNI stated that the only type of information acquired under the court's order was telephone metadata, such as telephone numbers dialed and length of calls. That did not satisfy our concern.

I am very pleased that we are here on the floor of the House putting forward something that addresses the concerns but that does not undermine the security of America. For example, I introduced the FISA court in the Sunshine Act of 2013 in response to this. Without compromising national security, it was bipartisan legislation that gave much-needed transparency to the decision orders and opinions of the Foreign Intelligence Surveillance Court, or FISA.

My bill would require the Attorney General to disclose each decision. I am glad that, in this bill, we have positions and points where the Attorney General is conducting declassification review. I am also pleased that the bill before us contains an explicit prohibition and a restraint, pursuant to section 215, on the bulk collection of tangible things.

We are making a difference with the USA FREEDOM Act, and it is interesting that groups as different as the R Street Institute and the Human Rights Watch are, in essence, supporting this legislation.

Mr. Speaker, I believe that we can do what we need to do by passing this legislation and by then going to an amendment on section 702, which I will support. Security goes along with protection, and I believe this particular legislation does it.

Mr. Speaker, as a senior member of the Judiciary Committee and an original co-sponsor, I rise in strong support of H.R. 2048, the "USA Freedom Act," which stands for "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act."

I support the USA Freedom Act for several reasons:

1. The bill ends all bulk collection of business records under Section 215 and prohibits bulk collection under the FISA Pen Register/Trap and Trace Device authority and National Security Letter authorities.

2. The USA Freedom Act strengthens the definition of "specific selection term," the mechanism used to prohibit bulk collection, which prevents large-scale, indiscriminate data collection while at the same time ensuring the government can collect the information it needs to further a national security investigation.

3. The USA Freedom Act strengthens protections for civil liberties by creating a panel of experts to advise the FISA Court on matters of privacy and civil liberties, communications technology, and other technical or legal matters and also codifies important procedures for recipients of National Security Letters.

4. The bill increases transparency by requiring declassification of all significant opinions of the FISA Court and provides procedures for certified questions of law to the FISA Court of Review and the Supreme Court.

5. The USA Freedom Act requires the Attorney General and the Director of National Intelligence to provide the public with detailed guidance about how they can use these national security authorities, and provides even more reporting by America's technology companies.

6. The USA Freedom Act contains several important national security enhancements, including closing loopholes that make it difficult for the government to track foreign terrorists and spies as they enter or leave the country.

The USA Freedom Act is the House's unified response to the unauthorized disclosures and subsequent publication in the media in June 2013 regarding the National Security Agency's collection from Verizon of the phone records of all of its American customers, which was authorized by the FISA Court pursuant to Section 215 of the Patriot Act.

Public reaction to the news of this massive and secret data gathering operation was swift and negative.

There was justifiable concern on the part of the public and a large percentage of the Members of this body that the extent and scale of this NSA data collection operation, which exceeded by orders of magnitude anything previously authorized or contemplated, may constitute an unwarranted invasion of privacy and threat to the civil liberties of American citizens.

To quell the growing controversy, the Director of National Intelligence declassified and released limited information about this program. According to the DNI, the information acquired under this program did not include the content of any communications or the identity of any subscriber.

The DNI stated that "the only type of information acquired under the Court's order is telephony metadata, such as telephone numbers dialed and length of calls."

The assurance given by the DNI, to put it mildly, was not very reassuring.

In response, many Members of Congress, including the Ranking Member CONYERS, and Mr. SENSENBRENNER, and myself, introduced legislation in response to the disclosures to ensure that the law and the practices of the executive branch reflect the intent of Congress in passing the USA Patriot Act and subsequent amendments.

For example, I introduced H.R. 2440, the "FISA Court in the Sunshine Act of 2013," bipartisan legislation, that provided much needed transparency without compromising national security to the decisions, orders, and opinions of the Foreign Intelligence Surveillance Court or "FISA Court."

Specifically, my bill required the Attorney General to disclose each decision, order, or opinion of a Foreign Intelligence Surveillance Court (FISC), allowing Americans to know how broad of a legal authority the government is claiming under the PATRIOT ACT and Foreign Intelligence Surveillance Act to conduct the surveillance needed to keep Americans safe.

I am pleased that these requirements are incorporated in substantial part in the USA Freedom Act, which requires the Attorney General to conduct a declassification review of each decision, order, or opinion of the FISA court that includes a significant construction or interpretation of law and to submit a report to Congress within 45 days.

As I indicated, perhaps the most important reasons for supporting passage of H.R. 2048 is the bill's prohibition on domestic bulk collection, as well as its criteria for specifying the information to be collected, applies not only to Section 215 surveillance activities but also to other law enforcement communications interception authorities, such as national security letters.

Finally, I strongly support the USA Freedom Act because Section 301 of the bill continues to contain protections against "reverse targeting," which became law when an earlier Jackson Lee Amendment was included in H.R. 3773, the RESTORE Act of 2007.

"Reverse targeting," a concept well known to members of this Committee but not so well understood by those less steeped in the arcana of electronic surveillance, is the practice where the government targets foreigners without a warrant while its actual purpose is to collect information on certain U.S. persons.

One of the main concerns of libertarians and classical conservatives, as well as progressives and civil liberties organizations, in giving expanded authority to the executive branch was the temptation of national security agencies to engage in reverse targeting may be difficult to resist in the absence of strong safeguards to prevent it.

The Jackson Lee Amendment, preserved in Section 301 of the USA Freedom Act, reduces even further any such temptation to resort to reverse targeting by making any information concerning a United States person obtained improperly inadmissible in any federal, state, or local judicial, legal, executive, or administrative proceeding.

Mr. Speaker, I noted in an op-ed published way back in October 2007, that as Alexis DeTocqueville, the most astute student of American democracy, observed nearly two centuries ago, the reason democracies invariably prevail in any military conflict is because democracy is the governmental form that best rewards and encourages those traits that are indispensable to success: initiative, innovation, courage, and a love of justice.

I support the USA Freedom Act because it will help keep us true to the Bill of Rights and strikes the proper balance between cherished liberties and smart security.

I urge my colleagues to support the USA Freedom Act.

Mr. GOODLATTE. Mr. Speaker, it is my pleasure to yield 2 minutes to the gentlewoman from California (Mrs. MIMI WALTERS), a member of the House Judiciary Committee and an original cosponsor of this bill.

Mrs. MIMI WALTERS of California. Mr. Speaker, I rise today in support of

H.R. 2048, the USA FREEDOM Act, of which I am proud to be an original cosponsor.

This vital bill will reform our Nation's intelligence-gathering programs to end the bulk collection of data, strengthen Americans' civil liberties, and protect our homeland from those who wish to do us harm.

In passing this legislation, we can provide officials with the tools they need to combat terrorist groups, such as ISIL, by closing a current loophole that requires the government to stop tracking foreign terrorists upon their entering the United States.

This bill will also provide for the robust oversight of our intelligence agencies by requiring additional reporting standards on how FISA authorities are employed. Furthermore, H.R. 2048 will prevent government overreach and will increase privacy protections by ending the large-scale, indiscriminate collection of data, which includes all records from an entire State, city, or ZIP Code.

With section 215 of the PATRIOT Act set to expire soon, it is vital that Congress acts quickly to pass this bipartisan bill so that we can keep our country safe and so that we can work to restore the trust of the American people.

Mr. CONYERS. Mr. Speaker, I am pleased to yield 1 minute to the distinguished gentleman from New York (Mr. JEFFRIES).

Mr. JEFFRIES. I thank the distinguished gentleman from Michigan.

Mr. Speaker, in a democracy, there must be a balance between effective national security protection on the one hand and a healthy respect for privacy and civil liberties interests on the other. This is a balance that traces all the way back to the founding of the Republic. It is rooted most prominently in the Bill of Rights, in the Constitution, in the Fourth Amendment. Yet, in its zeal to protect the homeland, our national security apparatus overreached into the lives of everyday, hard-working Americans in a manner that was inconsistent with our traditional notions of privacy and civil liberties. This overreach was unnecessary, unacceptable, and unconstitutional.

By ending bulk collection through section 215, we have taken a substantial step in the right direction toward restoring the balance. More must be done, but I am going to support this legislation because of the meaningful effort that has been made to help strike the appropriate balance.

Mr. GOODLATTE. Mr. Speaker, it is my pleasure to yield 2 minutes to the gentleman from California (Mr. ISSA), who is the chairman of the Courts, Intellectual Property, and the Internet Subcommittee and a strong supporter of this legislation.

Mr. ISSA. I thank the chairman.

Mr. Speaker, each person who comes up here will talk to you about the painstaking work that the chairman and the ranking member went through to craft a bill that would both strengthen our security, following on

with things we have learned since the enactment of the PATRIOT Act, and also make changes based on both lessons learned of things the PATRIOT Act overdid and excesses by the Presidential usurping of the intent of Congress. We have achieved that by a 25-2 vote in our committee, a vote that is almost unheard of.

I think, most importantly, though, we are doing something the American people need to know, and that is we are bringing transparency to the process for the first time. Under this legislation, a FISA court, working in secrecy, that makes a decision to expand or to in some other way add more surveillance will have to publish those findings, declassify them, and make them available not just to Congress but to the American people.

We cannot guarantee that behind closed doors secret—and necessarily secret—judge actions would always be what we would like, but under this reform, we can ensure that Congress and the American people will have the transparency and oversight as to those actions, not by whom they were after but what they did. That is going to bring the true reform that has been needed in a process in which the trust of the American people has been in doubt since the Snowden revelation.

I, personally, want to thank the ranking member and the chairman. This could not have happened without bipartisan work and without the support of those who want to strengthen our security and of those who want to strengthen and retain our freedoms under the Fourth Amendment.

Mr. CONYERS. Mr. Speaker, I yield 1 minute to the distinguished gentlewoman from Washington (Ms. DELBENE).

Ms. DELBENE. Mr. Speaker, last week, the Second Circuit confirmed what a lot of Members have been saying for years: the NSA has brazenly exploited the PATRIOT Act to conduct surveillance far beyond what the law permits; but the court refrained from enforcing its decision, instead placing the burden on Congress to protect Americans from unwarranted mass surveillance.

That is why I am proud to be a cosponsor of this year's USA FREEDOM Act, a serious reform bill that would go a long way to protecting Americans' privacy by ending bulk collection and by creating greater transparency, oversight, and accountability.

□ 1500

After the House acts today, it is up to the Senate leaders to pass these reforms or let the expiring provisions of the PATRIOT Act sunset on June 1 because a clean reauthorization is absolutely unacceptable. I urge my colleagues in each Chamber to support this critical effort to end bulk collection and protect both Americans' privacy and America's security.

Mr. GOODLATTE. Mr. Speaker, at this time I yield 3 minutes to the gentleman from Texas (Mr. HURD).

Mr. HURD of Texas. I thank the chairman for yielding me this time.

Mr. Speaker, as a former CIA officer, I completely understand the need for the men and women in our intelligence agencies to have access to timely, vital information as they track down bad guys.

As an American citizen, I know how important our civil rights are and that it is the government's job to protect those rights, not infringe upon them. I believe that we, as a nation, as a government, as a people can do both, and that is why I am supporting the USA FREEDOM Act. Because it prioritizes both and strikes the right balance between privacy and security, Americans can rest assured that their private information isn't being subjected to bulk collection by the NSA. They can be confident that there are privacy experts advising the FISA court advocating for our civil liberties, and they can be proud of an intelligence community who works hard every day to make sure that our country is protected.

I have seen firsthand the value these programs bring, but I also know that if Americans don't feel they can trust their own government, we are losing the battle right here at home. It is my hope that this bill will increase transparency and accountability to the program so that our hard-working intelligence community can continue their job of defending the country, and American citizens can be confident that they are being protected from enemies both foreign and domestic. Upholding civil liberties are not burdens; they are what make all of us safer and stronger.

Mr. CONYERS. Mr. Speaker, I am pleased to yield 8 minutes to the gentleman from California (Mr. SCHIFF), who is the distinguished ranking member of the House Permanent Select Committee on Intelligence. I ask unanimous consent that he be permitted to manage that time.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

Mr. SCHIFF. Mr. Speaker, I thank the gentleman for yielding me the time, and I yield myself such time as I may consume.

First, let me say thank you to Chairman GOODLATTE and Ranking Member CONYERS as well as to my colleague, Chairman NUNES. We have worked this issue together for a long time, and I am very proud of the bipartisan legislation that we have produced. I also want to thank the administration that worked with us so long and hard, and the work done in the last Congress by former HPSCI Chairman Mike Rogers and former HPSCI Ranking Member DUTCH RUPPERSBERGER. I rise today in strong support of H.R. 2048.

This Nation was founded on the revolutionary principle that liberty need not be sacrificed to security, that public safety can and must coexist with in-

dividual liberty. Our Founders set out to create a lasting Union and a great Nation, one in which the people would be free to govern themselves, to express themselves, to worship for themselves, while also being secure in their homes, their papers, and their persons.

Nearly two-and-a-half centuries later, it is easy to forget that these freedoms were enshrined in the Constitution amidst great peril. Americans had only recently fought a war for independence and would be confronted by powerful and often hostile forces in the future, including the powerful empires of Britain, France, and Spain. Here were truly existential threats, and still the Founders said, We can be secure and we can be free. They were right; we can and we must.

So today, at another moment of national danger, we are challenged to reaffirm our commitment to these twin imperatives—security and liberty—and to prove again that we can find the right balance for our times. The USA FREEDOM Act strikes that delicate but vitally important balance.

On the side of freedom, it ends bulk collection, not just of telephone metadata under section 215, but of any bulk collection under any other authority. It creates a specific procedure for telephone metadata that allows the government, upon court approval, to query the data that the telephone companies already keep, something I have long advocated. It increases transparency by requiring a declassification review of all significant FISA court opinions and by requiring the government to provide the public with detailed information about how they use these national security authorities. And it provides for a panel of experts to advocate for privacy and civil liberties before the FISA court, also something that I have advocated for quite sometime.

At the same time, the USA FREEDOM Act of 2015 preserves important capabilities and makes further national security enhancements by closing loopholes that make it difficult for the government to track foreign terrorists and spies as they enter or leave the country, clarifying the application of FISA to those who facilitate the international proliferation of weapons of mass destruction and increasing the maximum penalties for those who provide material support for terrorism. This is a strong bill and should advance with such an overwhelming majority that it compels the Senate to act.

But this is not a one-and-done legislative fix or the end of our work. Rather, it is a reaffirmation of our commitment to constantly recalibrate our laws to make sure that privacy and security are coexisting and mutually reinforcing. While the public may have begun its debate on these programs 2 years ago, many of us—myself included—have been working these issues long before, and we will continue to work them long afterwards. That is our responsibility and the great obligation the Founders bequeathed to us.

I reserve the balance of my time.

Mr. GOODLATTE. Mr. Speaker, at this time I yield 2 minutes to the gentleman from North Carolina (Mr. HOLDING).

Mr. HOLDING. Mr. Speaker, I thank the gentleman from Virginia, the chair of the Committee on the Judiciary, for both the time today and for his diligent work on the USA FREEDOM Act of 2015.

Mr. Speaker, the world we live in is a dangerous place. Indeed, it is far more dangerous than it ever has been. Acts of terror reached a record level last year, and with the wickedness of groups like ISIS and Boko Haram showing continued, complete disregard for human life, our Nation must always remain prepared and vigilant.

The legislation before us today, Mr. Speaker, builds on the reforms from the legislation passed last Congress, championed by my friend Representative SENSENBRENNER, and it accounts for the absolute need to protect civil liberties while also remaining clear-eyed and vigilant about the real threats that we face every day around the world.

I thank the chairman and I thank the committee for their work. I urge support for H.R. 2048.

Mr. SCHIFF. Mr. Speaker, I yield 2 minutes to the gentleman from Maryland (Mr. RUPPERSBERGER).

Mr. RUPPERSBERGER. Mr. Speaker, I rise in strong support of the USA FREEDOM Act, which virtually deletes the National Security Agency's database of Americans' phone and email records. The bulk collection of what we know now as metadata will end.

Under this bill, the government will now have to seek court approval before petitioning private cell phone companies for records. The court will have to approve each application except in emergencies, and major court decisions will be made public.

It is very similar to legislation drafted and introduced last year by the Permanent Select Committee on Intelligence, under the leadership of former Chairman Rogers and myself, together with our colleagues on the Committee on the Judiciary, led by Congressmen GOODLATTE and CONYERS. That bill passed with an overwhelming bipartisan majority, and I want to thank Congressmen GOODLATTE and CONYERS, as well as Congressmen SCHIFF and NUNES, also with Congressmen SENSENBRENNER and NADLER and other Members who worked hard and continued the pursuit on this much-needed reform.

We need this bill, though, to keep our country safe. Section 215 of the PATRIOT Act, which is the part that legalizes much of NSA's critical work to protect us from terrorists, expires in less than 3 weeks, on June 1. If we do not reauthorize it with the reforms demanded by the public, essential capabilities to track legitimate terror suspects will expire also. That couldn't happen at a worse time. We live in a

dangerous world. The threats posed by ISIS and other terrorist groups are just the tip of the iceberg.

We also need strong defenses against increasingly aggressive cyberterrorists and the lone wolf terrorists who are often American citizens, for example. This bill restores Americans' confidence that the government is not snooping on its own citizens by improving the necessary checks and balances to our democracy. This bill balances the need to protect our country with the need to protect our constitutional rights and civil liberties.

Mr. GOODLATTE. Mr. Speaker, at this time I am pleased to yield 3 minutes to the gentleman from Pennsylvania (Mr. MARINO), chairman of our Regulatory Reform, Commercial and Antitrust Law Subcommittee and a strong supporter of this legislation.

Mr. MARINO. I thank the chairman for yielding me this time.

Mr. Speaker, I rise in support of the USA FREEDOM Act. I applaud my colleagues on both sides of the aisle for their hard work on a true compromise piece of legislation. It protects the privacy of American citizens, according to the Constitution, while ensuring our national security, which is a priority. I understand the importance of reauthorizing these important FISA provisions.

As a U.S. attorney, I had these tools at my disposal, and I used them to protect Americans in Pennsylvania and across the country. We needed them at the time, and we need them now. However, I equally understand the importance of also protecting the privacy interests of American citizens. The act ends bulk collection; it strengthens protections of civil liberties; it increases transparency; all while ensuring that our intelligence and national security agencies have the tools they need to fight terrorism abroad. In addition, the USA FREEDOM Act protects American citizens at home.

Mr. SCHIFF. Mr. Speaker, I am pleased to yield 2 minutes to the gentleman from Connecticut (Mr. HIMES).

Mr. HIMES. Mr. Speaker, let me begin by thanking the chairman and ranking member of the Committee on the Judiciary, as well as Chairman NUNES and Ranking Member SCHIFF of the Permanent Select Committee on Intelligence, for their good, bipartisan work on a bill that I think is long overdue.

The good work on this bill, Mr. Speaker, goes back to the fact that the PATRIOT Act, a piece of legislation crafted in haste and in fear after the tragic events of 9/11, in my opinion, pushed the boundaries too far on the government's ability to surveil and gather information on people, including American citizens.

The USA FREEDOM Act, which I stand today to support, goes a very long way to restoring an appropriate balance between the imperative of national security and the civil liberties which we hold so dear. This bill makes

important reforms to the FISA court, but, importantly, it prohibits—I will say again, prohibits—the bulk collection, under section 215, under the pen register authorities, and under National Security Letter statutes, of data on American citizens. Americans will now rest easy knowing that their calls or other records will not be warehoused by the government, no matter how careful that government is in the procedures it uses to access those files.

Mr. Speaker, whatever the legal interpretations, most recently definitively ruled upon by the Second Circuit Court of Appeals, whatever the legal interpretations, there is something about the idea of a government keeping extensive records on its free citizens which damages our intuitive sense of freedom and liberty. So whatever the law and whatever the legal interpretations—and I do believe those have been settled—what we do here today, which is to say that the government of the United States will not keep detailed call or other bulk records on its free citizens, I believe is an important step forward for this country.

I urge all of my colleagues to vote in favor of the USA FREEDOM Act.

Mr. GOODLATTE. Mr. Speaker, may I inquire how much time is remaining on each side?

The SPEAKER pro tempore. The gentleman from California has 30 seconds remaining, the gentleman from Virginia has 8½ minutes remaining, and the gentleman from Michigan has 6½ minutes remaining.

Mr. GOODLATTE. Mr. Speaker, 30 seconds, is that the total amount of time the other side has?

The SPEAKER pro tempore. The minority has 7 minutes total remaining.

Mr. GOODLATTE. Mr. Speaker, I reserve the balance of my time.

Mr. SCHIFF. Mr. Speaker, once again I want to thank my colleagues for their good work. I also want to acknowledge Mr. SENSENBRENNER for his strong advocacy on this measure.

With that, I yield back the balance of my time.

□ 1515

Mr. CONYERS. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker and Members of the House, I would like to simply ask my colleagues to reject an unlawful surveillance program, to restore limits to a range of surveillance authorities, to compel the government to act with some measure of transparency, and to end the practice of dragnet surveillance in the United States.

In addition, I would like to thank the staff who have worked so hard on this bill: Caroline Lynch, Jason Herring, Bart Forsyth, Lara Flint, Chan Park, Matthew Owen, and Aaron Hiller.

I close by thanking in advance my colleagues who, like many of us, are inclined to strongly support H.R. 2048.

I yield back the balance of my time.

Mr. GOODLATTE. Mr. Speaker, I yield myself such time as I may consume.

From the founding of the American Republic, this country has been engaged in a profound debate about the responsibilities and the limits of our Federal Government.

The tension between these two essential functions of the government did not suddenly spring into existence in this age of cyber attacks and terrorist plots. Americans have long grappled with their need for security and their innate desire to protect their personal liberty from government intrusion.

Benjamin Franklin is often quoted as saying:

Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.

After the horrific attacks on September 11, the country was determined not to allow such an attack to occur again. The changes we made then to our intelligence laws helped keep us safe from implacable enemies. Today, we renew our commitment to our Nation's security and the safety of the American people.

We also make this pledge that the United States of America will remain a nation whose government answers to the will of its people. This country must be what it always has been, a beacon of freedom to the world, a place where the principles of the Founders—including the commitment to individual liberties—will continue to live, protected and nourished for future generations.

Mr. Speaker, I urge my colleagues to support this important bipartisan legislation.

I yield back the balance of my time.

Mr. SANFORD. Mr. Speaker, last week a federal appeals court declared that the NSA's bulk data collection on American citizens over the past 14 years was illegal. So why is Congress considering a bill that would legalize a program already deemed illegal? Unfortunately, that is what the USA FREEDOM Act does, and I believe codifies a program that violates the Constitution. When the Fourth Amendment says that the American people have the right to be free from warrantless searches and seizures of themselves and their property, I think it's a pretty clear statement on the limits of governmental action. Unfortunately, the bill today does not fully protect that right and accordingly I don't support it. The bill's purpose was to rein in the NSA's bulk data collection program but failed on that front, and I wanted to offer a few thoughts as to why.

First, the bill uses broad language to define who and what the government can search, which means that it still could technically collect Americans' information in bulk—just not as much as before. The bill does this by leaving the door open for the government to search geographic regions instead of the entire country as it does now. For example, the government could require phone companies to turn over all the records of their customers in South Carolina or even in a town like Mt. Pleasant in my district. I don't think the Founding Fathers' intent of the Fourth Amendment was to have it apply only in cases of nationwide warrantless searches; rather it should apply to any search anywhere.

Second, the bill doesn't even address a part of the PATRIOT Act called Section 702 that covers data that crosses our borders. This section allows the government to sweep up the content of an American citizen's emails, instant messages and web browsing history just because they happen to be communicating with someone outside the U.S. In fact, the former NSA director General Keith Alexander admitted that the NSA specifically searches Section 702 data using "U.S. person identifiers." This so-called "back door search loophole" should have been closed in this bill because it violates the Fourth Amendment by getting around the warrant requirement. The notion that Americans' rights are contingent on the geography of where a call is directed is not consistent with the Constitution and highlights why this particular section needs to be changed.

Third, this bill does not require the government to destroy information obtained on Americans who are not connected to an investigation. The way this happens is the government stores the information it collected on a particular phone call, even if one of those individuals on the call is suspected of no wrongdoing. The Constitution I believe is rather clear in the principle that organizations like the NSA and the FBI should not be able to store information that is inadvertently collected on people who are not suspected of committing a crime, and at a very minimum the FREEDOM Act does not use this opportunity to shine a light on the problem.

Pericles, the Greek general of Athens, once said that "Freedom is the sure possession of those alone who have the courage to defend it." Ultimately, I believe this bill is another missed opportunity for Congress to address what the judiciary has now ruled to be the unconstitutional and unlawful actions of the Executive branch. It really matters the Second Circuit federal court in New York issued an opinion last week stating that the NSA has stretched the meaning of the text of the PATRIOT Act so that it no longer represents congressional intent and called the NSA's bulk data collection illegal. It really matters that this bill would codify actions of the NSA that were ruled to be outside the bounds of law. I think it also matters that the debate that is taking place is as old as civilization as there has always been a tension between security and freedom. And it really matters that historically those civilizations that have given up freedom in the interest of security have historically lost both. For all these reasons each one of us should care deeply about what happens next on bulk collections at the NSA—and the way this bill comes up short in protecting liberty's foundation, civil liberty.

Mr. THORNBERRY. Mr. Speaker, out of necessity to reauthorize the expiring intelligence gathering authorities, I reluctantly vote for H.R. 2048. A recent federal appeals court decision has increased our need to address these authorities. Unfortunately, their pending expiration is now forcing Congress to act hastily rather than take the necessary time to adequately analyze the court's decision and update the laws accordingly.

I recognize the distrust created by the Obama Administration's abuse of power, as well as the damage caused by recent intelligence leaks containing fragments, inaccuracies, and speculation. It is unfortunate that those actions will continue to make it more dif-

ficult to gather the information necessary to counter terrorism. It is even more alarming that this trend will inevitably make our country less safe.

Very few Americans will ever learn the full details of the considerable successes of the National Security Agency (NSA). But through the dedication and commitment of its men and women, the NSA has helped to keep our nation and its citizens safe. I remain confident in their professionalism as they strive to prevent future terrorist attacks and support our warfighters overseas.

I believe the first job of the federal government is to defend the country and protect our citizens within the framework of the Constitution, and I will continue to do all I can to contribute to that effort.

Mr. FARR. Mr. Speaker, tonight I must rise to voice my concerns with the USA Freedom Act. While I recognize the improvements this bill attempts to make with regard to mass surveillance and information gathering efforts, I simply cannot vote for this bill.

I was pleased to hear that the Second Circuit Court recently found metadata collection to be illegal and commend the bi-partisan work that resulted in a bill that attempts to adhere to the court's decision. I recognize that the USA Freedom Act includes positive changes such as tighter language dictating when the NSA can access a database of call records, new allowances that grant technology companies the right to disclose governmental inquiries to their users and increases penalties for people caught aiding in terrorist efforts.

Mr. Speaker, I am concerned that other provisions in the bill would continue to allow for large swaths of information gathering. Simply put, I cannot vote for a bill that does not protect the privacy enshrined in the Fourth Amendment and guaranteed to all Americans. The risk of faulty information collection is not a risk I am willing to take with any American's privacy. Upholding the U.S. Constitution is non-negotiable.

Mrs. CAPPS. Mr. Speaker, I would like to submit for the RECORD my strong support of H.R. 2048, the USA Freedom Act of 2015, which I am proud to cosponsor.

This bipartisan bill will go a long way to reign in the abusive bulk surveillance practices that have left many Americans concerned for their privacy protections.

Furthermore, this bill will establish additional civil liberty protections and increased transparency, accountability, and oversight for over our national security practices.

As a policymaker, I am proud to support legislation that will protect our values of privacy and civil liberties while also providing our national security officials with the targeted tools that they need to ensure the safety of all Americans.

This bill is also a testament to what we can accomplish when we come together to work in a bipartisan way to meet the needs of the American people.

I urge my colleagues to support H.R. 2048. The SPEAKER pro tempore. All time for debate has expired.

Pursuant to House Resolution 255, the previous question is ordered on the bill, as amended.

The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed and read a third time, and was read the third time.

The SPEAKER pro tempore. The question is on the passage of the bill.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. GOODLATTE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER. Pursuant to clause 8 of rule XX, further proceedings on this question will be postponed.

MESSAGE FROM THE PRESIDENT

A message in writing from the President of the United States was communicated to the House by Mr. Pate, one of his secretaries.

CONTINUATION OF THE NATIONAL EMERGENCY WITH RESPECT TO YEMEN—MESSAGE FROM THE PRESIDENT OF THE UNITED STATES (H. DOC. NO. 114-36)

The SPEAKER pro tempore laid before the House the following message from the President of the United States; which was read and, together with the accompanying papers, referred to the Committee on Foreign Affairs and ordered to be printed:

To the Congress of the United States:

Section 202(d) of the National Emergencies Act (50 U.S.C. 1622(d)) provides for the automatic termination of a national emergency unless, within 90 days prior to the anniversary date of its declaration, the President publishes in the *Federal Register* and transmits to the Congress a notice stating that the emergency is to continue in effect beyond the anniversary date. In accordance with this provision, I have sent to the *Federal Register* for publication the enclosed notice stating that the national emergency declared in Executive Order 13611 of May 16, 2012, with respect to Yemen is to continue in effect beyond May 16, 2015.

The actions and policies of certain members of the Government of Yemen and others continue to threaten Yemen's peace, security, and stability, including by obstructing the implementation of the agreement of November 23, 2011, between the Government of Yemen and those in opposition to it, which provided for a peaceful transition of power that meets the legitimate demands and aspirations of the Yemeni people for change, and by obstructing the political process in Yemen. For this reason, I have determined that it is necessary to continue the national emergency declared in Executive Order 13611 with respect to Yemen.

BARACK OBAMA.
THE WHITE HOUSE, May 13, 2015.

PAIN-CAPABLE UNBORN CHILD PROTECTION ACT

Mr. GOODLATTE. Mr. Speaker, pursuant to House Resolution 255, I call up the bill (H.R. 36) to amend title 18, United States Code, to protect pain-capable unborn children, and for other