113TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 113–452
Part 1

USA FREEDOM ACT

MAY 15, 2014.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. GOODLATTE, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 3361]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 3361) 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, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

39–006

The Amendment

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "USA FREEDOM Act".

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

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), 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 of call detail records created on or after the date of the application, 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 re-

quired under subparagraph (A) are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism; and

"(ii) there are facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power; 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 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);

"(iii) provide that the Government may require the production of call detail records—

"(I) using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii) as the basis for production; and

"(II) using the results of the production under subclause (I) as the basis for production;

"(iv) 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

"(v) direct the Government to destroy all call detail records produced under the order not later than 5 years after the date of the production of such records, except for records that are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism.".

SEC. 102. EMERGENCY AUTHORITY.

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

"(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 authorizes 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 this section.

"(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 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"; and

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

(2) in paragraph (2)—

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

(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;"; and

(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 OF MINIMIZATION PROCEDURES FOR THE PRODUCTION OF TANGIBLE THINGS.

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)".

SEC. 105. LIABILITY PROTECTION.

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

"(e) No cause of action shall lie in any court against a person who produces tangible things or provides information, facilities, or technical assistance pursuant to an order issued or an emergency production required under this section. Such production 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, at the prevailing rate, a person for producing tangible things or providing information, facilities, or assistance in accordance with an order issued or an emergency production required under this section.".

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) CALL DETAIL RECORD DEFINED.—The term 'call detail record'—

"(A) means session identifying information (including originating or terminating telephone number, International Mobile Subscriber Identity num-

ber, or 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 of any communication (as defined in section 2510(8) of title 18, United States Code);

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

"(iii) cell site location information.

"(2) SPECIFIC SELECTION TERM.—The term 'specific selection term' means a term used to uniquely describe a person, entity, or account.".

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";

(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;"; and

(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 December 31, 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 December 31, 2015, 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)"; and

(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"; and

(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)"; and

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

(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 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).".

SEC. 109. EFFECTIVE DATE.

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.

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 and inserting a semicolon; and

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

"(3) a specific selection term to be used as the basis for selecting the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and".

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

"(4) The term 'specific selection term' has the meaning given the term in section 501.".

SEC. 202. MINIMIZATION PROCEDURES.

(a) DEFINITION.—Section 401 (50 U.S.C. 1841), as amended by section 201 of this Act, is further amended by adding at the end the following new paragraph:

"(5) The term 'minimization procedures' means—

"(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the installation and use of a pen register or trap and trace device to minimize the retention and prohibit the dissemination of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

"(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

"(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.".

(b) APPLICATION.—Section 402(c) (50 U.S.C. 1842(c)), as amended by section 201 of this Act, is further amended by adding at the end the following new paragraph:

"(4) a statement of proposed minimization procedures.".

(c) ORDER.—Section 402(d) (50 U.S.C. 1842(d)) is amended—

(1) in paragraph (1), by inserting "and that the proposed minimization procedures meet the definition of minimization procedures under this title" before the period at the end; and

(2) in paragraph (2)(B)—

(A) in clause (ii)(II), by striking "; and" and inserting a semicolon; and
(B) by adding at the end the following new clause:
"(iv) the minimization procedures be followed; and".

(d) COMPLIANCE ASSESSMENT.—Section 402 (50 U.S.C. 1842) is amended by adding at the end the following new subsection:

"(h) At or before the end of the period of time for which the installation and use of a pen register or trap and trace device is approved under an order or an extension under this section, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was retained or disseminated.".

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

SEC. 301. PROHIBITION ON REVERSE TARGETING.

Section 702(b)(2) (50 U.S.C. 1881a(b)(2)) is amended by striking "the purpose" and inserting "a purpose".

SEC. 302. MINIMIZATION PROCEDURES.

Section 702(e)(1) (50 U.S.C. 1881a(e)(1)) is amended—

(1) by striking "that meet" and inserting the following: "that—
"(A) meet";

(2) in subparagraph (A) (as designated by paragraph (1) of this section), by striking the period and inserting "; and"; and

(3) by adding at the end the following new subparagraph:
"(B) consistent with such definition, minimize the acquisition, and prohibit the retention and dissemination, of any communication as to which the sender and all intended recipients are determined to be located in the United States and prohibit the use of any discrete, non-target communication that is determined to be to or from a United States person or a person who appears to be located in the United States, except to protect against an immediate threat to human life.".

SEC. 303. 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), no information obtained or evidence derived from an acquisition pursuant to a certification or targeting or minimization procedures subject to an order under subparagraph (B) 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 from the acquisition 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 acquired before the date of the correction under such minimization procedures as the Court shall establish 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 subsection:

"(i) AMICUS CURIAE.—

"(1) 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 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 written finding that such appointment is not appropriate; and

"(B) may appoint an individual to serve as amicus curiae in any other instance as such court deems appropriate.

"(2) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall jointly designate not less than 5 individuals to be eligible to serve as amicus curiae. Such individuals shall be persons who possess expertise in privacy and civil liberties, intelligence collection, telecommunications, or any other area of law that may lend legal or technical expertise to the courts and who have been determined by appropriate executive branch officials to be eligible for access to classified information.

"(3) DUTIES.—An individual appointed to serve as amicus curiae under paragraph (1) shall carry out the duties assigned by the appointing court. Such court may authorize the individual appointed to serve as amicus curiae to review any application, certification, petition, motion, or other submission that the court determines is relevant to the duties assigned by the court.

"(4) NOTIFICATION.—The presiding judges of the courts established under subsections (a) and (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (1).

"(5) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a non-reimbursable basis) the assistance of the executive branch in the implementation of this subsection.

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

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 Attorney General shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance 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 this Act and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

"(b) REDACTED FORM.—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 Attorney General may waive the requirement to declassify and make publicly available a particular decision, order, or opinion under subsection (a) if the Attorney General—

"(1) 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) makes publicly available an unclassified summary of such decision, order, or opinion.".

(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 specific selection term 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 specific selection term 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(a) of the Fair Credit Reporting Act (15 U.S.C. 1681u(a)) is amended by striking "that information," and inserting "that information that includes a specific selection term to be used as the basis for the production of that information,".

(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 a specific selection term to be used as the basis for the production of such information.".

(e) DEFINITIONS.—

(1) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(g) SPECIFIC SELECTION TERM DEFINED.—In this section, the term 'specific selection term' has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).".

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

"(e) In this section, the term 'specific selection term' has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).".

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

"(n) SPECIFIC SELECTION TERM DEFINED.—In this section, the term 'specific selection term' has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).".

(4) DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES OF CONSUMER REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended by adding at the end the following new subsection:

"(g) SPECIFIC SELECTION TERM DEFINED.—In this section, the term 'specific selection term' has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).".

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

SEC. 601. ADDITIONAL REPORTING ON ORDERS REQUIRING PRODUCTION OF BUSINESS RECORDS.

Section 502(b) (50 U.S.C. 1862(b)) is amended—

(1) by redesignating paragraphs (1), (2), and (3) as paragraphs (5), (6), and (7), respectively; and

(2) by inserting before paragraph (5) (as so redesignated) the following new paragraphs:

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

"(2) the total number of such orders either granted, modified, or denied;

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

"(4) the total number of such orders either granted, modified, or denied;".

SEC. 602. BUSINESS RECORDS COMPLIANCE REPORTS TO CONGRESS.

(a) BUSINESS RECORDS PRODUCTIONS.—Section 502(b) (50 U.S.C. 1862(b)), as amended by section 601 of this Act, is further amended—

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

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

"(1) any compliance reviews conducted by the Federal Government of the production of tangible things under section 501;".

(b) FISA AUTHORITIES IN GENERAL.—Section 601(a) (50 U.S.C. 1871(a)) is amended—

(1) in paragraph (4), by striking "; and" and inserting a semicolon;

(2) in paragraph (5), by striking the period and inserting "; and"; and

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

"(6) any compliance reviews conducted by the Federal Government of electronic surveillance, physical searches, the installation of pen register or trap and trace devices, access to records, or acquisitions conducted under this Act.".

SEC. 603. ANNUAL REPORT BY THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON ORDERS ENTERED.

(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 REPORT ON ORDERS ENTERED.

"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 and make publicly available on an Internet website—

"(1) the number of orders entered under each of sections 105, 304, 402, 501, 702, 703, and 704;

"(2) the number of orders modified under each of those sections;

"(3) the number of orders denied under each of those sections; and

"(4) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each individual appointed to serve as amicus curiae.".

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

"Sec. 603. Annual report on orders entered.".

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

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by section 603 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 may semiannually publicly report the following information with respect to the preceding half year using one of the following structures:

"(1) A report that aggregates the number of orders or directives the person was required to comply with in the following separate categories:

"(A) Criminal process, subject to no restrictions.

"(B) The number of national security letters received, reported in bands of 1000 starting with 0-999.

"(C) The number of customer accounts affected by national security letters, reported in bands of 1000 starting with 0-999.

"(D) The number of orders under this Act for content, reported in bands of 1000 starting with 0-999.

"(E) With respect to content orders under this Act, in bands of 1000 starting with 0-999—

"(i) the number of customer accounts affected under orders under title I; and

"(ii) the number of customer selectors targeted under orders under title VII.

"(F) The number of orders under this Act for non-content, reported in bands of 1000 starting with 0-999.

"(G) With respect to non-content orders under this Act, in bands of 1000 starting with 0-999—

"(i) the number of customer accounts affected under orders under—

"(I) title I;

"(II) title IV;

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

"(IV) title V with respect to applications described in section 501(b)(2)(C); and

"(ii) the number of customer selectors targeted under orders under title VII.

"(2) A report that aggregates the number of orders or directives the person was required to comply with in the following separate categories:

"(A) Criminal process, subject to no restrictions.

"(B) The total number of all national security process received, including all national security letters and orders under this Act, reported as a single number in a band of 0-249 and thereafter in bands of 250.

"(C) The total number of customer selectors targeted under all national security process received, including all national security letters and orders under this Act, reported as a single number in a band of 0-249 and thereafter in bands of 250.

"(3) A report that aggregates the number of orders or directives the person was required to comply with in the following separate categories:

"(A) Criminal process, subject to no restrictions.

"(B) The number of national security letters received, reported in bands of 500 starting with 0-499.

"(C) The number of customer accounts affected by national security letters, reported in bands of 500 starting with 0-499.

"(D) The number of orders under this Act for content, reported in bands of 500 starting with 0-499.

"(E) The number of customer selectors targeted under such orders, in bands of 500 starting with 0-499.

"(F) The number of orders under this Act for non-content, reported in bands of 500 starting with 0-499.

"(G) The number of customer selectors targeted under such orders, reported in bands of 500 starting with 0-499.

"(b) NATIONAL SECURITY LETTER DEFINED.—The term 'national security letter' means any of the following provisions:

"(1) Section 2709 of title 18, United States Code.

"(2) Section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A)).

"(3) Subsection (a) or (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u(a), 1681u(b)).

"(4) Section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).".

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

"Sec. 604. Public reporting by persons subject to orders.".

SEC. 605. REPORTING REQUIREMENTS FOR DECISIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.

Section 601(c)(1) (50 U.S.C. 1871(c)) 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 that includes a significant construction or interpretation of any provision of this Act or a denial of a request for an order or a modification of a request for an order, or results in a change of application of any provision of this Act or a new application of any provision of this Act—

"(A) a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion; and

"(B) with respect to such decision, order, or opinion, a brief statement of the relevant background factual information, questions of law, legal analysis, and decision rendered; and".

SEC. 606. 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.—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 REGISTER 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 Government has made application for orders approving the use of pen registers or trap and trace devices under this title; and

"(5) for each department or agency described in paragraph (4), a breakdown of the numbers required by 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 of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate".

TITLE VII—SUNSETS

SEC. 701. 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 31, 2017".

(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 31, 2017".

Purpose and Summary

H.R. 3361, the "USA FREEDOM Act," reforms Section 215 of the USA PATRIOT Act (Section 501 of the Foreign Intelligence Surveillance Act (FISA)), clarifies several other national security authorities, expands existing oversight provisions, and creates greater transparency of national security programs operated pursuant to FISA.

Background and Need for the Legislation

In June 2013, Edward Snowden, a former defense contractor and CIA employee, released classified material on top-secret National Security Agency (NSA) data collection programs, including a metadata program operated under Section 215 of the USA PATRIOT Act and a program called PRISM operated under Section 702 of the FISA Amendments Act, to the media. On June 5, 2013, it was reported that on April 25, 2013, the Foreign Intelligence Surveillance Court (FISC) granted an order requested by the FBI pursuant to Section 215 of the USA PATRIOT Act.[1] The order compels a telephone service provider, on an "ongoing, daily basis," to provide the NSA with "all call detail records or telephony metadata" for communications made via its systems, both within

[1] 50 U.S.C. § 1861.

the United States and between the U.S. and other countries.[2] "Telephony metadata" is broadly defined, and includes the numbers of both parties on a call, unique identifiers, and the time and duration of all calls. The order gave the government the authority to obtain the call detail records or "telephony metadata" for a 3-month period, ending on July 19, 2013.[3]

On June 6, 2013, classified information regarding a second program, the PRISM program, was reported by the *Guardian* and *Washington Post.*[4] PRISM was authorized by Section 702 of FISA,[5] which was reauthorized by Congress in 2012 and expires in December of 2017.[6] It allows the NSA to obtain data from electronic service providers regarding non-U.S. persons who reside outside the United States—including email, chat, photos, videos, stored data, and file transfers.

In the months that followed, the Director of National Intelligence (DNI) declassified numerous Foreign Intelligence Surveillance Court (FISC) opinions and orders. In addition, the DNI declassified minimization procedures and comprehensive reviews of programs operated under FISA.

On March 27, 2014, President Obama announced several changes to the conduct of foreign intelligence activities in response to the ongoing controversy arising from the unauthorized disclosure of classified information by Edward Snowden. The President announced changes that imposed both a substantive limit on the scope of NSA's access to telephony metadata as well as a procedural limit on when the NSA may access the data in the first place. The substantive limit restricts the results of queries of telephony metadata to two "hops" (a "hop" is a colloquial term for a connection between two telephone numbers). Prior to the President's speech, the program had been authorized to receive query results of up to three "hops."

The procedural limit also requires that the FISC approve queries of telephony metadata on a case-by-case basis and before any query is conducted. Under the bulk metadata collection program, the NSA was permitted to query the data without court approval and based on one of 22 NSA officials' determination that there was a reasonable articulable suspicion (RAS) that the selector is associated with an international terrorist organization. As described by the President, the new framework requires the FISC to approve each selector for use in queries. Such an arrangement was not unprecedented. For several months in 2009, the FISC had imposed a similar judicial pre-approval requirement after the government reported violations of the court-ordered privacy protections intended to prevent access to the metadata. This pre-approval requirement was subsequently lifted after the FISC was satisfied that sufficient changes had been made to correct the earlier compliance violations.

At the same time, the President announced that the government should no longer store telephone metadata in bulk; rather, the

---

[2] *See Verizon forced to hand over telephone data—full court ruling,* THE GUARDIAN, Jun. 5, 2013, *available at* http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[3] *Id.*

[4] Glenn Greenwald, "NSA Prism program taps in to user data of Apple, Google and others," *available at* http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[5] 50 U.S.C. § 1881a.

[6] *Id.; see also* Pub. L. No. 112–238 (December 30, 2012).

records should remain at the telephone companies for the length of time such records are stored in the ordinary course of business. Also, the President stated that the court-approved numbers could be used to query the data over a limited period of time without returning to the FISC for approval, the production of records would be ongoing and prospective, and the companies should be compelled by court order to provide technical assistance to ensure that the records can be queried and that results are transmitted to the government in a usable format and in a timely manner. [7]

Over the past year, the House Judiciary Committee has conducted aggressive oversight of these programs. In July 2013, the Committee held a public hearing at which testimony was received from officials with the Justice Department, the Office of the Director of National Intelligence, the NSA and the FBI and civil liberties groups. In September 2013, the Committee held a classified hearing where members were afforded the opportunity to further probe these programs with officials from DOJ, ODNI, NSA, and FBI. In February 2014, the Committee held a comprehensive hearing to examine the various recommendations to reform these programs offered by the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board.

In 1976, the Supreme Court held that an individual's bank account records did not fall within the protection of the Fourth Amendment's prohibition on unreasonable searches and seizures.[8] Subsequently, Congress passed laws protecting various types of transactional information, but built in exceptions providing some access to statutorily protected records for counter intelligence purposes. Similar statutory protections were also enacted for electronic communications records and credit bureau records.

As with financial records, these later statutes also included exceptions for access to records relevant to counterintelligence investigations. These exceptions comprise the authority for national security letters (NSLs), which can be used to compel the production of certain types of records. In 1998, Congress amended FISA to provide access to certain records that were not available through NSLs.[9] Specifically, it created a mechanism for Federal investigators to compel the production of records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[10] Applications for orders under this section had to be made by FBI agents with a rank of Assistant Special Agent in Charge or higher and investigations could not be conducted solely on the basis of activities protected by the First Amendment.[11]

Under these procedures the FISC would issue an order if the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." [12] Recipients of an order

---

[7] Press Release, The White House, Office of the Press Secretary, *Statement by the President on the Section 215 Bulk Metadata Program* (Mar. 27, 204), available at http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.

[8] *U.S. v. Miller,* 425 U.S. 435 (1976).

[9] P.L. 105–272, tit. VI, § 602.

[10] 50 U.S.C. § 1862(a) (2001).

[11] 50 U.S.C. § 1862(a)(1) (2001).

[12] 50 U.S.C. § 1862(b)(2)(B) (2001).

under this section were required to comply with it, and were also prohibited from disclosing to others that an order had been issued.[13]

In 2001, Section 215 of the USA PATRIOT Act made several changes to the procedures under FISA for obtaining business records.[14] Among these was an expansion of the scope of records that were subject to compulsory production. Prior to enactment of the USA PATRIOT Act, only records from four explicit categories of businesses could be obtained. Section 215 expanded business records to "any tangible things."[15]

This expanded scope drew strong opposition from the library community, so much so that Section 215 came to be known as the "library provision" despite the fact that the original text of the provision did not mention libraries. Opposition from this group was based upon the "chilling effect" such access might have on the exercise of First Amendment rights and purported intrusions into areas protected by the Fourth Amendment.[16]

In response to these concerns, a library-specific amendment was made to the Section 215 procedures by the USA PATRIOT Improvement and Reauthorization Act of 2005. Under this amendment, if the records sought were "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the application has to be approved by one of three high-ranking FBI officers.[17]

Section 215 of the USA PATRIOT Act also modified the standard that had to be met before an order compelling production of documents could issue from the FISC. Prior to enactment of Section 215, an applicant had to have "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[18] In contrast, under Section 215, the applicant only needed to "specify that the records concerned [were] sought for a [foreign intelligence investigation.]"[19]

As part of the 2005 reauthorization, Congress further amended FISA procedures for obtaining business records. The applicable standard was again changed to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence investigation.]"[20] Records are presumptively relevant if they pertain to:

- a foreign power or an agent of a foreign power;
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

---

[13] 50 U.S.C. § 1862(d)(1)–(2) (2001).
[14] P.L. 107–56, § 215 *codified at* 50 U.S.C. § 1862(a)–(b) (2008).
[15] 50 U.S.C. § 1861(a)(1) (2008).
[16] *See, e.g.,* AMERICAN LIBRARY ASSOCIATION, *Resolution on the USA PATRIOT Act and Related Measures That Infringe on the Rights of Library Users,* Jan. 29, 2003, available at http://www.ala.org.
[17] Applications for these records could be made only by the Director of the Federal Bureau of Investigation, the Deputy Director of the Federal Bureau of Investigation, or the Executive Assistant Director for National Security. This authority cannot be further delegated. 50 U.S.C. § 1861(a)(3) (2008).
[18] 50 U.S.C. § 1862(b)(2)(B) (2001).
[19] P.L. 107–56, § 215.
[20] P.L. 109–177, § 106(b).

- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation;

Orders issued under Section 215 are accompanied by nondisclosure orders prohibiting the recipients from disclosing that the FBI has sought or obtained any tangible things pursuant to a FISA order. However, the recipient may discuss the order with other persons as necessary to comply with the order, with an attorney to obtain legal advice or assistance, or with other persons as permitted by the FBI.[21] The recipient must identify persons to whom disclosure has been made, or is intended to be made, if the FBI requests, except that attorneys with whom the recipient has consulted do not need to be identified.[22]

The 2005 reauthorization also provided procedures for recipients of Section 215 orders to challenge the judicial review of orders compelling the production of business records.[23] Once a petition for review is submitted by a recipient, a FISC judge must determine whether the petition is frivolous within 72 hours.[24] If the petition is frivolous, it must be denied and the order affirmed.[25] Otherwise the order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[26] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[27]

On July 10, 2008, President Bush signed into law the FISA Amendments Act of 2008 (FAA), which passed with a bipartisan majority of Congress and broad support from the intelligence community. Among other things, the FAA provided for targeting non-U.S. persons overseas to acquire foreign intelligence information, subject to specific targeting and minimization procedures that are reviewed by the FISA Court. The FAA required the Attorney General and the DNI to assess compliance with those procedures every 6 months and to submit an assessment to the FISA Court and to Congress.

The FAA permited the Attorney General and DNI to obtain an annual certification from the FISC to target foreign persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information. Under exigent circumstances,[28] the Attorney General and DNI may immediately authorize such targeting based upon a determination that without immediate implementation of an authorization, intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order.

---

[21] 50 U.S.C. § 1861(d)(1) (2008).
[22] 50 U.S.C. § 1861(d)(2)(C) (2008).
[23] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).
[24] 50 U.S.C. § 1861(f)(2)(A)(ii) (2008).
[25] *Id.*
[26] 50 U.S.C. § 1861(f)(2)(B) (2008).
[27] 50 U.S.C. § 1861(f)(3) (2008).
[28] The use of the term "exigent circumstances" in this provision is not intended to implicate in any way the use of that term in criminal procedure jurisprudence as an exception to the Fourth Amendment warrant requirement. *See, e.g., U.S. v. Karo,* 468 U.S. 705 (1984); *Warden v. Hayden,* 387 U.S. 294 (1967); *McDonald v. U.S.,* 335 U.S. 451 (1948). Rather, section 702 defines its use of the term "exigent circumstances" for purposes of targeting a foreign person reasonably believed to be located outside the United States as those circumstances that will result in the loss or failure to timely acquire intelligence important to the national security of the United States and time does not permit the issuance of an authorization under this section.

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

The FAA expanded oversight by all three branches of government:

- Every 60 days, the Department of Justice and the Office of the Director of National Intelligence conduct on-site reviews of surveillance conducted pursuant to the FISA Amendments Act.
- The Attorney General and the DNI conduct detailed assessments of compliance with court-approved targeting and minimization procedures and provide these assessments to Congress twice a year.
- A semi-annual report to Congress is required from the Administration on certifications or orders obtained under the FAA, compliance reviews, and incidents of noncompliance.

The FAA amended an existing reporting requirement to require the Attorney General to submit to Congress a copy of any FISC order, opinion, or decision, and the accompanying pleadings, briefs, and other memoranda of law when the court's decision includes "significant construction or interpretation of any provision" of FISA. This expanded the amount of background and supporting material that the Committee could receive in connection with a significant decision by the FISC. Prior to enactment of the FISA Amendments Act in 2008, only "decisions and opinions" containing significant construction or interpretation of FISA were required to be submitted to Congress.

Hearings

The Committee on the Judiciary held no hearings on H.R. 3361.

Committee Consideration

On May 7, 2014, the Committee met in open session and ordered the bill H.R. 3361 favorably reported with an amendment, by a rollcall vote of 32 to 0, a quorum being present.

Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall votes occurred during the Committee's consideration of H.R. 3361:

1. An amendment by Mr. King to permit the government to contract with third parties for the retention of information. Defeated by a rollcall vote of 4 to 24.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman		X	
Mr. Sensenbrenner, Jr. (WI)		X	
Mr. Coble (NC)			

ROLLCALL NO. 1—Continued

	Ayes	Nays	Present
Mr. Smith (TX)	X		
Mr. Chabot (OH)		X	
Mr. Bachus (AL)		X	
Mr. Issa (CA)			
Mr. Forbes (VA)			
Mr. King (IA)	X		
Mr. Franks (AZ)			
Mr. Gohmert (TX)	X		
Mr. Jordan (OH)			
Mr. Poe (TX)			
Mr. Chaffetz (UT)			
Mr. Marino (PA)		X	
Mr. Gowdy (SC)			
Mr. Labrador (ID)		X	
Ms. Farenthold (TX)		X	
Mr. Holding (NC)	X		
Mr. Collins (GA)		X	
Mr. DeSantis (FL)		X	
Mr. Smith (MO)		X	
[Vacant]			
Mr. Conyers, Jr. (MI), Ranking Member		X	
Mr. Nadler (NY)		X	
Mr. Scott (VA)		X	
Ms. Lofgren (CA)		X	
Ms. Jackson Lee (TX)		X	
Mr. Cohen (TN)		X	
Mr. Johnson (GA)			
Mr. Pierluisi (PR)		X	
Ms. Chu (CA)		X	
Mr. Deutch (FL)		X	
Mr. Gutierrez (IL)		X	
Ms. Bass (CA)			
Mr. Richmond (LA)			
Ms. DelBene (WA)		X	
Mr. Garcia (FL)		X	
Mr. Jeffries (NY)		X	
Mr. Cicilline (RI)		X	
Total	4	24	

2. An amendment offered by Mr. Gohmert to amend Sections 501 and 402 of title 50 and Section 2709 of title 18 to change "clandestine intelligence activities" to 'clandestine intelligence activities by foreign individuals, foreign entities or foreign governments." Passed by a rollcall vote of 14 to 11. After the adoption of the Gohmert amendment, a motion to reconsider the vote on the amendment was agreed to, and the amendment was then defeated by voice vote.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman	X		
Mr. Sensenbrenner, Jr. (WI)		X	
Mr. Coble (NC)			
Mr. Smith (TX)			
Mr. Chabot (OH)		X	
Mr. Bachus (AL)		X	
Mr. Issa (CA)			
Mr. Forbes (VA)			
Mr. King (IA)	X		
Mr. Franks (AZ)			
Mr. Gohmert (TX)	X		
Mr. Jordan (OH)	X		
Mr. Poe (TX)	X		
Mr. Chaffetz (UT)			
Mr. Marino (PA)		X	
Mr. Gowdy (SC)			
Mr. Labrador (ID)	X		
Ms. Farenthold (TX)	X		
Mr. Holding (NC)		X	
Mr. Collins (GA)			
Mr. DeSantis (FL)			
Mr. Smith (MO)	X		
[Vacant]			
Mr. Conyers, Jr. (MI), Ranking Member		X	
Mr. Nadler (NY)		X	
Mr. Scott (VA)		X	
Ms. Lofgren (CA)	X		
Ms. Jackson Lee (TX)	X		
Mr. Cohen (TN)			
Mr. Johnson (GA)			
Mr. Pierluisi (PR)	X		
Ms. Chu (CA)		X	
Mr. Deutch (FL)		X	
Mr. Gutierrez (IL)			
Ms. Bass (CA)			
Mr. Richmond (LA)			
Ms. DelBene (WA)		X	
Mr. Garcia (FL)	X		
Mr. Jeffries (NY)	X		
Mr. Cicilline (RI)	X		
Total	14	11	

3. Motion to report H.R. 3361 favorably, as amended. Passed by a vote of 32 to 0.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Goodlatte (VA), Chairman	X		

ROLLCALL NO. 3—Continued

	Ayes	Nays	Present
Mr. Sensenbrenner, Jr. (WI)	X		
Mr. Coble (NC)			
Mr. Smith (TX)	X		
Mr. Chabot (OH)	X		
Mr. Bachus (AL)	X		
Mr. Issa (CA)			
Mr. Forbes (VA)			
Mr. King (IA)	X		
Mr. Franks (AZ)	X		
Mr. Gohmert (TX)			
Mr. Jordan (OH)			
Mr. Poe (TX)	X		
Mr. Chaffetz (UT)	X		
Mr. Marino (PA)	X		
Mr. Gowdy (SC)	X		
Mr. Labrador (ID)	X		
Ms. Farenthold (TX)	X		
Mr. Holding (NC)	X		
Mr. Collins (GA)	X		
Mr. DeSantis (FL)	X		
Mr. Smith (MO)	X		
[Vacant]			
Mr. Conyers, Jr. (MI), Ranking Member	X		
Mr. Nadler (NY)	X		
Mr. Scott (VA)	X		
Ms. Lofgren (CA)	X		
Ms. Jackson Lee (TX)	X		
Mr. Cohen (TN)	X		
Mr. Johnson (GA)	X		
Mr. Pierluisi (PR)	X		
Ms. Chu (CA)	X		
Mr. Deutch (FL)	X		
Mr. Gutierrez (IL)	X		
Ms. Bass (CA)			
Mr. Richmond (LA)			
Ms. DelBene (WA)	X		
Mr. Garcia (FL)	X		
Mr. Jeffries (NY)	X		
Mr. Cicilline (RI)	X		
Total	32	0	

Committee Oversight Findings

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

New Budget Authority and Tax Expenditures

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

Congressional Budget Office Cost Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 3361, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 14, 2014.

Hon. BOB GOODLATTE, CHAIRMAN,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3361, the "USA FREEDOM Act."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock, who can be reached at 226-2840.

Sincerely,

DOUGLAS W. ELMENDORF,
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 3361—USA FREEDOM Act.

As ordered reported by the House Committee on the Judiciary on May 7, 2014.

H.R. 3361 would make several amendments to investigative and surveillance authorities of the United States government, and would specify the conditions under which the Federal Government may conduct certain types of surveillance. CBO does not provide estimates for classified programs; therefore, this estimate addresses only the unclassified aspects of the bill. On that limited basis, CBO estimates implementing H.R. 3361 would cost approximately $15 million over the 2015–2019 period, subject to the appropriation of the necessary amounts.

Enacting H.R. 3361 also could affect direct spending and revenues; therefore, pay-as-you-go procedures apply. The bill could potentially result in additional criminal penalties because it would extend for 2 years the authority of the government to conduct surveillance in certain instances. Such penalties are recorded as revenues, deposited in the Crime Victims Fund, and later spent. How-

ever, CBO anticipates that any amounts collected would be minimal and the net impact would be insignificant.

EFFECTS ON THE FEDERAL BUDGET

The bill would amend the Foreign Intelligence Surveillance Act (FISA). Those amendments would affect the operations of the Foreign Intelligence Surveillance Court (FISC) and the Judiciary. First, H.R. 3361 would permit the FISC to appoint an *amicus curiae*, or "friend of the court," to assist the court when the government makes an application under FISA that presents a novel or significant interpretation of FISA. Second, the bill would limit collection of telephone call records, thereby requiring the intelligence agencies—acting through the Department of Justice—to seek additional warrants from the FISC to access such data. Finally, the bill would require an annual report by the Director of the Administrative Office of the U.S. Courts (AOUSC), providing data on certain types of FISA orders. Based on information from the AOUSC, CBO estimates that implementing those requirements would cost approximately $5 million over the 2015–2019 period, assuming appropriation of the necessary amounts.

In addition, the bill would require Federal agencies to conduct several program assessments and reviews, and would establish new reporting requirements. Section 108 would require the Inspectors General of the Justice Department and the Intelligence Community to assess the effectiveness of the surveillance programs affected by the bill; section 402 would require the Attorney General to conduct declassification reviews of certain court decisions, orders, and opinions related to FISA. CBO estimates that fulfilling these and other reporting requirements in the bill would cost approximately $10 million over the 2015–2019 period, assuming appropriation of the necessary amounts.

INTERGOVERNMENTAL AND PRIVATE-SECTOR MANDATES

The bill would impose two mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on both private and governmental entities. First, the bill would expand liability protections and limit the ability of plaintiffs to sue in cases where a defendant provides information to the Federal Government pursuant to a FISA order. Second, it would require entities, when compelled to provide information about telephone calls to Federal officials, to protect the secrecy of the records and to minimize any disruption of services.

CBO estimates that the costs of those mandates would be small. The change in expanded liability protection is a slight modification to current law, and CBO estimates that the elimination of any legal right of action for future plaintiffs would affect a limited number of potential lawsuits. Information from the Department of Justice indicates that public entities receive few requests for call records, and the cost to those entities of providing that information is negligible. In addition, since public and private entities already take action to protect private information in complying with requests from the Federal Government and such entities would be fully compensated by the government at the prevailing rate for the services they provide, the costs to those entities would be insignificant. Consequently, CBO estimates that the total costs of all mandates in the bill would fall well below the intergovernmental and

private-sector thresholds established in UMRA ($76 million and $152 million in 2014, respectively, adjusted annually for inflation).

PREVIOUS CBO ESTIMATE

On May 8, 2014, the House Permanent Select Committee on Intelligence ordered reported a similar version of H.R. 3361. CBO's cost estimates for both versions are the same.

STAFF CONTACTS

The CBO staff contacts for this estimate are Jason Wheelock (for Federal costs), J'nell L. Blanco (for the intergovernmental effects), and Elizabeth Bass (for the private-sector effects). This estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

Duplication of Federal Programs

No provision of H.R. 3361 establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

Disclosure of Directed Rule Makings

No provision of H.R. 3361 directs a specific rule making within the meaning of 5 U.S.C. § 551.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3361, the USA FREEDOM Act, reforms Section 215 of the USA PATRIOT Act (Section 501 of FISA), clarifies several other national security authorities, expands existing oversight provisions, and creates greater transparency of national security programs operated pursuant to FISA.

Advisory on Earmarks

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 3361 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

Section-by-Section Analysis

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

TITLE I—FISA BUSINESS RECORD REFORMS

Sec. 101—Additional requirements for call detail records. On March 27, 2014, President Obama announced the need for legislation to reform the NSA's telephone metadata program.[29] To that

[29] Press Release, The White House, Office of the Press Secretary, *Statement by the President on the Section 215 Bulk Metadata Program* (Mar. 27, 204), available at http://

end, the Act preserves traditional operational capabilities exercised by the government to collect foreign intelligence information under Section 501 of FISA. In addition, the Act prohibits the bulk collection of any business records under Section 501. The Act also creates a new, narrowly-tailored mechanism that prevents bulk collection of telephone metadata by the government but also preserves the government's ability to search telephone metadata for possible connections between foreign powers or agents of foreign powers and others, as part of an authorized investigation to protect against international terrorism and with the additional safeguards proposed by the President.

Under the Act, if the government can demonstrate a reasonable, articulable suspicion that a specific selection term is associated with a foreign power or an agent of a foreign power, the FISA court may issue an order for the production of call detail records created on or after the request for production and held by telephone companies in the normal course of business. The government may require the production of up to two "hops"—i.e., the call detail records associated with the initial seed and the call detail records associated with the records returned in the initial "hop." The prospective collection of call detail records (i.e., those created "after" the request for production) is limited to 180 days.

The Act defines "call detail record" to include "session identifying information (including originating or terminating telephone number, International Mobile Subscriber Identity number, or International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call." The Act explicitly excludes from that term the contents of any communication; the name, address, or financial information of a subscriber or customer; and cell site location information.

The Act requires the entities involved in the production of call detail records to provide the government with technical assistance. The Act also requires the destruction of call detail records within 5 years of production, except for records that remain relevant to an ongoing counterterrorism investigation.

The Act does not require any private entity to retain any record or information other than in the ordinary course of business. However, nothing in current law or this Act prohibits the government and telecommunications providers from agreeing voluntarily to retain records for periods longer than required for their business purposes.

This new authority—designed to allow the government to search telephone metadata for possible connections to international terrorism—does not preclude the government's use of "traditional" business record orders under Section 501 to compel the production of business records, including call detail records.

Sec. 102—Emergency authority. This section creates a new emergency authority in Section 215. The Attorney General may authorize the emergency production of tangible things, provided that such an application is presented to the court within 7 days. If the court subsequently denies an emergency application, the government may not use any of the information obtained under the emergency

---

www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.

authority except in instances of a threat of death or serious bodily harm.

Sec. 103. Prohibition on Bulk Collection of Tangible Things. The Act requires that each application for the production of tangible things include "a specific selection term to be used as the basis for the production." In so doing, the Act makes clear that the government may not engage in bulk collection under Section 501 of FISA.

The Act defines "specific selection term" to mean "a term used to uniquely describe a person, entity, or account."

This goes further than the President's plan in that it prohibits the bulk collection of all tangible things and not just telephone records. Section 501(b)(2)(A) of FISA will continue to require the government to make "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation. . . ."[30] The USA Freedom Act requires the government to provide a specific selection term as the basis for the production of the tangible things sought, thus ensuring that the government cannot collect tangible things based on the assertion that the requested collection "is thus relevant, because the success of [an] investigative tool depends on bulk collection."[31] These changes restore meaningful limits to the "relevance" requirement of Section 501.

Although this Act eliminates bulk collection, the Act does not limit the government's use of Section 501 as it was designed, as a mechanism for intelligence agencies to obtain information, based on a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a national security investigation.

Sec. 104—Judicial review of minimization procedures for the production of tangible things. This section provides that the court may evaluate the adequacy of minimization procedures under Section 215. Under current law, the court is only empowered to determine whether or not the government has minimization procedures in place.

Sec. 105—Liability protection. This section provides liability protections to third parties who provide information, facilities, or technical assistance to the government in compliance with an order issued under Section 215. This provision mirrors the liability provisions in Titles I and VII of FISA.

Sec. 106—Compensation for assistance. This section explicitly permits the government to compensate third parties for producing tangible things or providing information, facilities, or assistance in accordance with an order issue under Section 215. It is customary for the Government to enter into contractual agreements with third parties in order to compensate them for products and services provided to the Government.

Sec. 107—Definitions. This section provides definitions for "call detail records" and "specific selection term".

Sec. 108—Inspector general reports on business records orders. This section requires the Inspector General of the Department of

---

[30] 50 U.S.C. § 501(b)(2)(A).

[31] Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [redacted],* No. BR 13–09 (FISA Ct. Aug. 29, 2013), at 21 (citing Mem. of Law at 15, Docket No. BR 06–05).

Justice to conduct a comprehensive review of the use of Section 215 with respect to calendar years 2012 to 2014. It also requires the Inspector General of the Intelligence Community to assess the value and use of intelligence obtained under Section 215 over the same period.

Sec. 109—Effective date. This section provides that the new telephone metadata program, the new Section 215 emergency authority, and the prohibition on bulk collection of tangible things under Section 215 take effect 180 days after enactment.

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

Sec. 201—Prohibition on bulk collection. This section provides that the pen register and trap and trace device authority may not be used without a specific selection term as the basis for selecting the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.

Sec. 202—Minimization procedures. This section requires that the government adopt procedures that are reasonably designed to minimize the retention and prohibit the dissemination of nonpublic information about United States persons. It also explicitly authorizes the court to assess compliance with these procedures while a pen register or trap and trace device is in use.

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

Sec. 301. Restatement of Prohibition on Reverse Targeting. Section 702(b)(2) of FISA provides that the government "may not intentionally target a person reasonably believed to be located outside the United States if *the* purpose of such acquisition is to target a particular, known person reasonably believed to be within the United States."[32] The Act clarifies this prohibition to state that the government "may not intentionally target a person reasonably believed to be located outside the United States if *a* purpose of such acquisition is to target a particular, known person reasonably believed to be within the United States."

This change is meant to simply clarify and restate Congress' original intent in enacting Section 702 of the FISA Amendments Act that this authority cannot be used as a pretext to target U.S. persons inside the United States.

Sec. 302. Minimization Procedures. The Act codifies procedures already adopted by the government for the minimization of domestic communications. Specifically, the Act requires that the government minimize the acquisition, and prohibit the retention and dissemination, of any wholly domestic communication acquired by the government under Section 702. The Act also prohibits the government from using communications to or from a United States person or a person who appears to be located in the United States, except where the communication relates to a target under Section 702 or to protect against an immediate threat to human life.

Sec. 303—Limits on use of unlawfully obtained information. This section provides that the government may not use information ac-

[32] 50 U.S.C. § 1881a(b)(2) (emphasis ours).

quired outside the scope of court-approved targeting and minimization procedures.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

Sec. 401—Appointment of amicus curiae. This section provides that both the FISA court and the FISA Court of Review shall, if deemed appropriate, appoint an individual to serve as amicus curiae in a case involving a novel or significant interpretation of law. In addition, this section permits the court to appoint amicus curiae in any case.

The presiding judges of the courts will designate five individuals who are eligible to serve as amicus curiae. These individuals shall possess expertise in privacy and civil liberties, intelligence collection, telecommunications, or any other area of law that may lend legal or technical expertise to the courts, and shall possess appropriate security clearances.

Sec. 402—Declassification of decisions, orders, and opinions. This section 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. In the interest of national security, the Attorney General may provide a summary of the decision rather than a declassified copy.

TITLE V—NATIONAL SECURITY LETTER REFORM

Sec. 501—Prohibition on bulk collection. This section prohibits the use of various national security letter authorities without the use of a specific selection term as the basis for the national security letter request.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

Sec. 601—Additional reporting on orders requiring production of business records. In addition to existing annual reporting requirements, this section requires the government to report on the number of requests made for call detail records under the new telephone metadata program.

Sec. 602—Business records compliance reports to Congress. This section requires the government to provide to Congress any compliance reports related to the use of Section 215.

Sec. 603—Annual report by the Director of the Administrative Office of the United States Courts on orders Entered. This section requires the Director of the Administrative Office of the United States Court to make an annual report on the number of orders issued under sections 105, 304, 402, 501, 702, 703, and 704 of FISA, as well as the number of appointments of individuals to serve as amicus curiae to the FISA court.

Sec. 604—Reporting requirements for decisions of the Foreign Intelligence Surveillance Court. This section requires the Attorney General to provide to the relevant committees, within 45 days of each decision, order, or opinion that includes a significant construction or interpretation, a copy of each such decision and a brief statement of the relevant background.

Sec. 605—Submission of reports under FISA. This section includes the House Judiciary Committee in several existing reporting requirements.

TITLE VII—SUNSETS

Sec. 701—USA PATRIOT Improvement and Reauthorization Act of 2005. This section aligns the sunset of the three sun-setting provisions of the USA PATRIOT Act with the sunset of the FISA Amendment Act on December 31, 2017.

Agency Views

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS

HONORABLE JOHN D. BATES
Director

WASHINGTON, D.C. 20544

May 13, 2014

Honorable Bob Goodlatte
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On behalf of the Judicial Branch, I am writing to the Committee regarding H.R. 3361, the "USA Freedom Act," which was recently ordered reported by your Committee, to recommend that three elements of the bill be adjusted.

In a letter to the Committee on January 13, 2014, we expressed views of the Judiciary 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 and the Foreign Intelligence Surveillance Court of Review ("FISA Courts"), and did not express views on policy choices that the political branches are considering. We emphasized the potential for greater demands on judicial resources. In keeping with that approach, this letter focuses narrowly on three provisions of H.R. 3361 that bear directly on the work of the FISA Courts and how that work is presented to the public: the provisions regarding amicus curiae participation, public summaries of unreleased FISA Court opinions, and public reporting by the Judiciary on FISA Court orders.

We respectfully request that, if possible, this letter be included with your Committee's report to the House on the bill.

The amicus curiae provisions in Section 401 of the bill are generally in keeping with the views set forth in the January 13 letter. Section 401 would facilitate the FISA Courts' receiving briefing or other assistance from a legal or technical expert outside the Executive Branch in particular matters where such assistance would be helpful, while not creating a permanent institution of a public advocate or imposing an adversarial process in the general run of cases where it would be unnecessary and even counterproductive to do so. We would recommend

adjusting the language in H.R. 3361 to slightly clarify the breadth of the FISA Courts' discretion to appoint amici in any needed circumstance by deleting the words "of law" in the paragraph labeled "Designation."

Section 401 largely leaves it to the discretion of the FISA Courts when to appoint an amicus. We believe that this general approach is correct because those courts, operating in the context of specific cases, are best positioned to assess when amicus participation would be helpful. We do, however, question the need for providing that an amicus "shall" be appointed in any case "that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a written finding that such appointment is not appropriate." Section 401 (proposed Section 103(i)(1) of FISA). Not every novel or significant issue is necessarily difficult for a court to resolve, and the judges of the FISA Courts would have every incentive to appoint amici when they believe that their deliberations would benefit from doing so. The bill drafters seem to acknowledge this likelihood by allowing the FISA courts to provide, in the alternative, a written statement justifying the decision not to appoint an amicus.

Section 402 would create a presumption that the FISA Courts' significant decisions be released to the public in redacted form by the Attorney General. In those cases where the Attorney General determines that even a redacted release would harm national security, the Attorney General would be required to make an unclassified summary of the opinion available to the public. Section 7 (proposed Section 602(c)(2) of FISA). For the following reasons, we recommend eliminating the requirement for unclassified summaries of unreleased opinions.

To be sure, summaries of federal court opinions are sometimes prepared for the convenience of readers. But in those situations the full opinion is also public. Any ambiguity or imprecision in the summary is unlikely to confuse or mislead readers because the opinion itself can be consulted and is understood to be authoritative. In contrast, a summary that is made public *instead of* a court's opinion, and is intended to convey some information about the opinion while concealing the rest, is much more likely to result in misunderstanding of the opinion's reasoning and result.

In the January 13 letter, we explained why it can be challenging to release FISA Court opinions in a form that is both informative to the public and adequately protective of sensitive national security information. For example, the subject of an opinion might be "how to apply FISA's four-part definition of 'electronic surveillance,' *see* 50 U.S.C. § 1801(f), to a proposed surveillance method for a new communications technology." January 13, 2014, Letter at 14. It may be necessary to withhold from the public details about how the surveillance is effected "so that valid intelligence targets are not given a lesson in how to evade it." *Id.* On the other hand, however, releasing the opinion with that information redacted may not enhance public understanding.

Notwithstanding these challenges, recent experience shows that the preparation and release of redacted opinions can, in some cases, contribute to public understanding of the FISA Courts' work. Our concern is with proposed Section 602(c)(2), which would require the

preparation and publication of unclassified summaries for those opinions that cannot be released – even in redacted form – without harming national security. By its terms, this requirement would apply to the subset of opinions in which national security information is inextricably intertwined with the opinion's entire line of reasoning – otherwise, redaction and partial release would be feasible. For the same reasons that a redacted release could not be accomplished for those opinions, attempts to "summarize" them without disclosing the operative facts are likely to fall short in one of two ways. The summary may be so conclusory as to be minimally informative ("The Court held that a novel surveillance technique fell within the definition of 'electronic surveillance' under 50 U.S.C. § 1801(f), such that the application to use that technique was within its jurisdiction."). Or, in a well-meaning attempt to say more without disclosing classified information, the summary may describe the opinion's reasoning abstractly and incompletely, divorced from the relevant facts. Such a summary is more likely to distort, rather than illuminate, the opinion for which it is substituted.

Finally, although we do not object to the reporting requirements in Section 603, the Committee should be aware that such information might in the future include material that the Executive Branch considers to be sensitive for national security purposes. This could potentially place the Judiciary in an awkward position of addressing a statutory command for public distribution of such information when the Executive Branch regards it as classified. (The sharing of classified information among authorized persons in other branches of government does not raise the same concerns.) We recommend that this possibility be addressed in the legislation, by, for example, making more explicit the Executive Branch's responsibility for making any classification or declassification determinations as to such information, or excusing the Judiciary from the public release of information the Executive Branch deems to be classified.

We thank the Committees for their previously expressed interest in our perspectives on these matters. I hope these further comments are helpful to Congress in its deliberations on potential legislation. If we can be of further assistance to you, please do not hesitate to contact us through our Office of Legislative Affairs at 202-502-1700.

Sincerely,

John D. Bates
Director

cc: Honorable John A. Boehner
Honorable Eric Cantor

Identical letter sent to: Honorable John Conyers, Jr.
Honorable Mike Rogers
Honorable C. A. Dutch Ruppersberger

Changes in Existing Law Made by the Bill, as Reported

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

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

* * * * * * *

[TITLE VI—REPORTING REQUIREMENT]

TITLE VI—OVERSIGHT

* * * * * * *

Sec. 602. Declassification of significant decisions, orders, and opinions.
Sec. 603. Annual report on orders entered.
Sec. 604. Public reporting by persons subject to orders.

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

DESIGNATION OF JUDGES

SEC. 103. (a) * * *

* * * * * * *

(i) AMICUS CURIAE.—

(1) 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 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 written finding that such appointment is not appropriate; and

(B) may appoint an individual to serve as amicus curiae in any other instance as such court deems appropriate.

(2) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall jointly designate not less than 5 individuals to be eligible to serve as amicus curiae. Such individuals shall be persons who possess expertise in privacy and civil liberties, intelligence collection, telecommunications, or any other area of law that may lend legal or technical expertise to the courts and who have been determined by appropriate executive branch officials to be eligible for access to classified information.

(3) DUTIES.—An individual appointed to serve as amicus curiae under paragraph (1) shall carry out the duties assigned by the appointing court. Such court may authorize the individual appointed to serve as amicus curiae to review any application, certification, petition, motion, or other submission that the court determines is relevant to the duties assigned by the court.

(4) NOTIFICATION.—The presiding judges of the courts established under subsections (a) and (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (1).

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

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

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 108. (a)(1) On a semiannual basis the Attorney General shall fully inform **[**the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate,**]** *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* concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

* * * * * * *

TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 306. On a semiannual basis the Attorney General shall fully inform the **[**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,**]** *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* concerning all physical searches conducted pursuant

to this title. On a semiannual basis the Attorney General shall also provide to those committees [and the Committee on the Judiciary of the House of Representatives] a report setting forth with respect to the preceding six-month period—

(1) * * *

* * * * * * *

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 401. As used in this title:

(1) * * *

* * * * * * *

(4) The term "specific selection term" has the meaning given the term in section 501.

(5) The term "minimization procedures" means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the installation and use of a pen register or trap and trace device to minimize the retention and prohibit the dissemination of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

SEC. 402. (a) * * *

* * * * * * *

(c) Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include—

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application[; and]*;*

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation

of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution[.]*;*

(3) a specific selection term to be used as the basis for selecting the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(4) a statement of proposed minimization procedures.

(d)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section *and that the proposed minimization procedures meet the definition of minimization procedures under this title*.

(2) An order issued under this section—

(A) * * *

(B) shall direct that—

(i) * * *

(ii) such provider, landlord, custodian, or other person—

(I) * * *

(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 105(b)(2)(C) of this Act, any records concerning the pen register or trap and trace device or the aid furnished[; and]*;*

* * * * * * *

(iv) the minimization procedures be followed; and

* * * * * * *

(h) At or before the end of the period of time for which the installation and use of a pen register or trap and trace device is approved under an order or an extension under this section, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was retained or disseminated.

* * * * * * *

CONGRESSIONAL OVERSIGHT

SEC. 406. (a) * * *

(b) On a semiannual basis, the Attorney General shall also provide to the committees referred to in subsection (a) and to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

(1) * * *

(2) the total number of such orders either granted, modified, or denied[; and]*;*

(3) the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under section 403, and the total number of subsequent orders approving or denying the installation and use of such pen registers and trap and trace devices[.]*;*

(4) each department or agency on behalf of which the Government has made application for orders approving the use of pen registers or trap and trace devices under this title; and

(5) for each department or agency described in paragraph (4), a breakdown of the numbers required by paragraphs (1), (2), and (3).

TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES

SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a) * * *

(b) Each application under this section—

(1) * * *

(2) shall include—

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

[(A) a statement**]** *(B) in the case of an application other than an application described in subparagraph (C), a statement* of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

(i) * * *

* * * * * * *

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation**[**; and**]***;*

(C) in the case of an application for the production of call detail records created on or after the date of the application, 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 an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism; and

(ii) there are facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power; and

[(B)**]** *(D)* an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of In-

vestigation based on the order requested in such application.

(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) *and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g)*, the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

(2) An order under this subsection—

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified**[**;**]***, including each specific selection term to be used as the basis for the production;*

* * * * * * *

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things**[**; and**]***;*

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a)**[**.**]***; and*

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

(i) authorize the production 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);

(iii) provide that the Government may require the production of call detail records—

(I) using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii) as the basis for production; and

(II) using the results of the production under subclause (I) as the basis for production;

(iv) 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

(v) direct the Government to destroy all call detail records produced under the order not later than 5 years after the date of the production of such records, except for records that are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism.

(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).

(d)(1) No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things [pursuant to an order] *pursuant to an order issued or an emergency production required* under this section, other than to—

(A) those persons to whom disclosure is necessary to comply with [such order] *such order or such emergency production*;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to [the order] *the order or the emergency production*; or

* * * * * * *

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom [an order] *an order or emergency production* is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to [an order] *an order or emergency production* under this section shall notify such person of the nondisclosure requirements of this subsection.

* * * * * * *

[(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.]

(e) No cause of action shall lie in any court against a person who produces tangible things or provides information, facilities, or technical assistance pursuant to an order issued or an emergency production required under this section. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

* * * * * * *

(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 tan-

gible 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 authorizes 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 this section.

(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 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).

(j) COMPENSATION.—The Government shall compensate, at the prevailing rate, a person for producing tangible things or providing information, facilities, or assistance in accordance with an order issued or an emergency production required under this section.

(k) DEFINITIONS.—In this section:

(1) CALL DETAIL RECORD DEFINED.—The term "call detail record"—

(A) means session identifying information (including originating or terminating telephone number, International Mobile Subscriber Identity number, or 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 of any communication (as defined in section 2510(8) of title 18, United States Code);

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

(iii) cell site location information.

(2) SPECIFIC SELECTION TERM.—The term "specific selection term" means a term used to uniquely describe a person, entity, or account.

SEC. 502. CONGRESSIONAL OVERSIGHT.

(a) On an annual basis, the Attorney General shall fully inform the [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] *Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate* concerning all requests for the production of tangible things under section 501.

(b) In April of each year, the Attorney General shall submit to the House and Senate Committees on the Judiciary and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence a report setting forth with respect to the preceding calendar year—

(1) any compliance reviews conducted by the Federal Government of 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;

[(1)] *(6)* the total number of applications made for orders approving requests for the production of tangible things under section 501;

[(2)] *(7)* the total number of such orders either granted, modified, or denied; and

[(3)] *(8)* the number of such orders either granted, modified, or denied for the production of each of the following:

(A) * * *

* * * * * * *

TITLE VI—[REPORTING REQUIREMENT] *OVERSIGHT*

SEC. 601. SEMIANNUAL REPORT OF THE ATTORNEY GENERAL.

(a) REPORT.—On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security, a report setting forth with respect to the preceding 6-month period—

(1) * * *

* * * * * * *

(4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice[; and]*;*

(5) copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this Act[.]*; and*

(6) any compliance reviews conducted by the Federal Government of electronic surveillance, physical searches, the installation of pen register or trap and trace devices, access to records, or acquisitions conducted under this Act.

* * * * * * *

(c) SUBMISSIONS TO CONGRESS.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)—

[(1) a copy of any decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes significant construction or interpretation of any provision of this Act, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, not later than 45 days after such decision, order, or opinion is issued; and]

(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 that includes a significant construction or interpretation of any provision of this Act or a denial of a request for an order or a modification of a request for an order, or results in a change of application of any provision of this Act or a new application of any provision of this Act—

(A) a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion; and

(B) with respect to such decision, order, or opinion, a brief statement of the relevant background factual information, questions of law, legal analysis, and decision rendered; and

* * * * * * *

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

(a) DECLASSIFICATION REQUIRED.—Subject to subsection (b), the Attorney General shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance 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 this Act and, consistent with

that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

(b) REDACTED FORM.—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 Attorney General may waive the requirement to declassify and make publicly available a particular decision, order, or opinion under subsection (a) if the Attorney General—

(1) 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) makes publicly available an unclassified summary of such decision, order, or opinion.

SEC. 603. ANNUAL REPORT ON ORDERS ENTERED.

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 and make publicly available on an Internet website—

(1) the number of orders entered under each of sections 105, 304, 402, 501, 702, 703, and 704;

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

(3) the number of orders denied under each of those sections; and

(4) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each individual appointed to serve as amicus curiae.

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

(a) REPORTING.—A person may semiannually publicly report the following information with respect to the preceding half year using one of the following structures:

(1) A report that aggregates the number of orders or directives the person was required to comply with in the following separate categories:

(A) Criminal process, subject to no restrictions.

(B) The number of national security letters received, reported in bands of 1000 starting with 0-999.

(C) The number of customer accounts affected by national security letters, reported in bands of 1000 starting with 0-999.

(D) The number of orders under this Act for content, reported in bands of 1000 starting with 0-999.

(E) With respect to content orders under this Act, in bands of 1000 starting with 0-999—

(i) the number of customer accounts affected under orders under title I; and

(ii) the number of customer selectors targeted under orders under title VII.

(F) The number of orders under this Act for non-content, reported in bands of 1000 starting with 0-999.

(G) With respect to non-content orders under this Act, in bands of 1000 starting with 0-999—

(i) the number of customer accounts affected under orders under—

(I) title I;

(II) title IV;

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

(IV) title V with respect to applications described in section 501(b)(2)(C); and

(ii) the number of customer selectors targeted under orders under title VII.

(2) A report that aggregates the number of orders or directives the person was required to comply with in the following separate categories:

(A) Criminal process, subject to no restrictions.

(B) The total number of all national security process received, including all national security letters and orders under this Act, reported as a single number in a band of 0-249 and thereafter in bands of 250.

(C) The total number of customer selectors targeted under all national security process received, including all national security letters and orders under this Act, reported as a single number in a band of 0-249 and thereafter in bands of 250.

(3) A report that aggregates the number of orders or directives the person was required to comply with in the following separate categories:

(A) Criminal process, subject to no restrictions.

(B) The number of national security letters received, reported in bands of 500 starting with 0-499.

(C) The number of customer accounts affected by national security letters, reported in bands of 500 starting with 0-499.

(D) The number of orders under this Act for content, reported in bands of 500 starting with 0-499.

(E) The number of customer selectors targeted under such orders, in bands of 500 starting with 0-499.

(F) The number of orders under this Act for non-content, reported in bands of 500 starting with 0-499.

(G) The number of customer selectors targeted under such orders, reported in bands of 500 starting with 0-499.

(b) NATIONAL SECURITY LETTER DEFINED.—The term "national security letter" means any of the following provisions:

(1) Section 2709 of title 18, United States Code.

(2) Section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A)).

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

(4) Section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).

TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

* * * * * * *

SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.

(a) * * *

(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

(1) * * *

(2) may not intentionally target a person reasonably believed to be located outside the United States if [the purpose] *a purpose* of such acquisition is to target a particular, known person reasonably believed to be in the United States;

* * * * * * *

(e) MINIMIZATION PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures [that meet] *that*—

(A) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a)[.]*; and*

(B) consistent with such definition, minimize the acquisition, and prohibit the retention and dissemination, of any communication as to which the sender and all intended recipients are determined to be located in the United States and prohibit the use of any discrete, non-target communication that is determined to be to or from a United States person or a person who appears to be located in the United States, except to protect against an immediate threat to human life.

* * * * * * *

(i) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

(1) * * *

* * * * * * *

(3) ORDERS.—

(A) * * *

* * * * * * *

(D) LIMITATION ON USE OF INFORMATION.—

(i) IN GENERAL.—Except as provided in clause (ii), no information obtained or evidence derived from an acquisition pursuant to a certification or targeting or minimization procedures subject to an order under subparagraph (B) 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 from the acquisition 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 acquired before the date of the correction under such minimization procedures as the Court shall establish for purposes of this clause.

* * * * * * *

USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005

* * * * * * *

TITLE I—USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT

* * * * * * *

SEC. 102. USA PATRIOT ACT SUNSET PROVISIONS.

(a) * * *

(b) SECTIONS 206 AND 215 SUNSET.—

(1) IN GENERAL.—Effective **[**June 1, 2015**]** *December 31, 2017*, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.

* * * * * * *

SEC. 106A. AUDIT ON ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES.

(a) * * *

(b) REQUIREMENTS.—The audit required under subsection (a) shall include—

(1) an examination of each instance in which the Attorney General, any other officer, employee, or agent of the Department of Justice, the Director of the Federal Bureau of Investigation, or a designee of the Director, submitted an application to the Foreign Intelligence Surveillance Court (as such term is defined in section 301(3) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821(3))) for an order under section 501 of such Act during the calendar years of 2002 through 2006 *and calendar years 2012 through 2014*, including—

(A) * * *

* * * * * * *

[(2) the justification for the failure of the Attorney General to issue implementing procedures governing requests for the production of tangible things under such section in a timely

fashion, including whether such delay harmed national security;

[(3) whether bureaucratic or procedural impediments to the use of such requests for production prevent the Federal Bureau of Investigation from taking full advantage of the authorities provided under section 501 of such Act;]

[(4)] *(2)* any noteworthy facts or circumstances relating to orders under such section, including any improper or illegal use of the authority provided under such section; and

[(5)] *(3)* an examination of the effectiveness of such section as an investigative tool, including—

(A) * * *

* * * * * * *

[(C) with respect to calendar year 2006, an examination of the minimization procedures adopted by the Attorney General under section 501(g) of such Act and whether such minimization procedures protect the constitutional rights of United States persons;]

(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;

(D) whether, and how often, the Federal Bureau of Investigation utilized information acquired pursuant to an order under section 501 of such Act to produce an analytical intelligence product for distribution within the Federal Bureau of Investigation, to the intelligence community [(as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)))], or to other Federal, State, local, or tribal government Departments, agencies, or instrumentalities; and

* * * * * * *

(c) SUBMISSION DATES.—

(1) * * *

* * * * * * *

(3) CALENDAR YEARS 2012 THROUGH 2014.— Not later than December 31, 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.

(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 December 31, 2015, 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.

[(d)**]** *(e)* PRIOR NOTICE TO ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE; COMMENTS.—

(1) NOTICE.—Not less than 30 days before the submission of **[**a report under subsection (c)(1) or (c)(2)**]** *any report under subsection (c) or (d)*, the **[**Inspector General of the Department of Justice**]** *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* shall provide such report to the Attorney General and the Director of National Intelligence.

(2) COMMENTS.—The Attorney General or the Director of National Intelligence may provide comments to be included in **[**the reports submitted under subsections (c)(1) and (c)(2)**]** *any report submitted under subsection (c) or (d)* as the Attorney General or the Director of National Intelligence may consider necessary.

[(e)**]** *(f)* UNCLASSIFIED FORM.—**[**The reports submitted under subsections (c)(1) and (c)(2)**]** *Each report submitted under subsection (c)* and any comments included under **[**subsection (d)(2)**]** *subsection (e)(2)* shall be in unclassified form, but may include a classified annex.

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

* * * * * * *

TITLE 18, UNITED STATES CODE

PART I—CRIMES

* * * * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

* * * * * * *

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) * * *

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation, or his 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, [may] *may, using a specific selection term as the basis for a request—*

(1) * * *

* * * * * * *

(g) SPECIFIC SELECTION TERM DEFINED.—In this section, the term "specific selection term" has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).

* * * * * * *

RIGHT TO FINANCIAL PRIVACY ACT OF 1978

* * * * * * *

TITLE XI—RIGHT TO FINANCIAL PRIVACY

* * * * * * *

SPECIAL PROCEDURES

SEC. 1114. (a)(1) * * *

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 1103(b) signed by a supervisory official of a rank designated by the head of the Government authority[.] *and a specific selection term to be used as the basis for the production and disclosure of financial records.*

* * * * * * *

(e) In this section, the term "specific selection term" has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).

FAIR CREDIT REPORTING ACT

* * * * * * *

TITLE VI—CONSUMER CREDIT REPORTING

* * * * * * *

§ 626. Disclosures to FBI for counterintelligence purposes

(a) IDENTITY OF FINANCIAL INSTITUTIONS.—Notwithstanding section 604 or any other provision of this title, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 1101 of the Right to Financial Privacy Act of 1978) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for [that information,] *that information that includes a specific selection term to be used as the basis for the production of that information,* signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

* * * * * * *

(n) SPECIFIC SELECTION TERM DEFINED.—In this section, the term "specific selection term" has the meaning given the term in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).

§ 627. Disclosures to governmental agencies for counterterrorism purposes

(a) DISCLOSURE.—Notwithstanding section 604 or any other provision of this title, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or [analysis.] *analysis and a specific selection term to be used as the basis for the production of such information.*

* * * * * * *

(g) SPECIFIC SELECTION TERM DEFINED.—In this section, the term "specific selection term" has the meaning given the term in sec-

tion 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861).

* * * * * * *

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

* * * * * * *

TITLE VI—TERRORISM PREVENTION

Subtitle A—Individual Terrorists as Agents of Foreign Powers

SEC. 6001. INDIVIDUAL TERRORISTS AS AGENTS OF FOREIGN POWERS.

(a) * * *

(b) SUNSET.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendment made by subsection (a) shall cease to have effect on [June 1, 2015] *December 31, 2017*.

* * * * * * *

ADDITIONAL VIEWS

The USA FREEDOM Act as reported by the Judiciary Committee is a step in the right direction in protecting Americans' right to privacy, but falls short of what Congress should do to protect the Fourth Amendment rights of Americans. The bill as introduced provided important substantive reforms that not only ended bulk data collection under section 215, but also fixed a loophole in section 702 that allowed intelligence agencies to search communications of Americans without a warrant.

Unfortunately, the reforms offered by the USA FREEDOM Act were scaled back by a Manager's amendment that was a result of negotiations between the Judiciary and the Intelligence Committees. While I recognize the value of reaching compromise that advances respect for the Constitution by American Intelligence agencies, I believe the Act as reported has a number of deficiencies that may be improved by further amendments.

I offered five amendments during the mark-up of this bill. One was withdrawn with a promise by the Chairman to further examine what I perceived as a drafting error, the rest were all defeated by voice vote.

One of the most important amendments I offered would have closed the loophole found in section 702 of The Foreign Intelligence Surveillance Act (FISA).[1] The NSA has admitted to using this loophole,[2] which is inconsistent with the rest of Title VII that requires probable cause when dealing with U.S. persons' communications. FISA was originally enacted in response to unchecked spying by Federal intelligence agencies on U.S. citizens for political purposes.[3] It is ironic that a law designed to prevent inappropriate domestic spying is today susceptible to this kind of abuse. My amendment required that a warrant be obtained to search the database for communications of U.S. persons collected under section 702. This provision was included in the USA FREEDOM Act as originally introduced. During markup it was suggested that the minimization procedures in this act make the need for Fourth Amendment protection of Americans unnecessary. I believe this assertion to be incorrect, and that the Fourth Amendment rights of Americans need the protection that the probable cause standard would provide. Moreover, minimization standards do not prevent the search and collection of the information in the first place.

I also offered an amendment to require a probable cause warrant before obtaining data of Americans under Section 215. During the markup debate it was stated that to date no court has given content held by third parties Fourth Amendment protection. It is cor-

[1] 50 USC § 1181a.
[2] Director James Clapper's March 28, 2014 letter to Senator Ron Wyden.
[3] Mitra Ebadolahi, Warrantless Wiretapping Under the FISA Amendments Act, ABA Human Rights Magazine Vol. 39 No. 3.

rect that the majority of courts have not recognized a Fourth Amendment right to privacy for information held by third parties but at least one has.

The Sixth Circuit Court of Appeals ruled in 2010 that warrantless email searches violate the Fourth Amendment.[4] The court found that "government agents violated [defendant's] Fourth Amendment rights by compelling [defendant's ISP] to turn over the emails without first obtaining a warrant based on probable cause."[5]

Additionally, albeit in the context of a claim of marital privilege, rather than a Fourth Amendment claim, the Fourth Circuit endorsed the notion of a reasonable expectation of privacy in email, stating: "[E]mails today, 'in common experience,' are confidential."[6] It is long established Supreme Court precedent that "a Fourth Amendment search occurs when the government violates a *subjective expectation of privacy that society recognizes as reasonable."*[7] The trend of what society deems as a reasonable expectation of privacy is clear.

It was Justice Brandeis' dissent in the seminal case of *Olmstead v. U.S.* that formed the foundation of how to think about privacy and the Fourth Amendment in the modern era. In it, he tried to craft a general right to privacy based on an integration of the principles of the Fourth and Fifth Amendments.[8] He argued that "the progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions."[9]

He could not have written more prophetically. The government may now reproduce documents "without removing papers from secret drawers"[10] through the technological mechanism of cloud storage. The analysis of metadata and other data collected in bulk has brought "means of exploring unexpressed beliefs."[11] Brandeis recognized that the Fourth Amendment was crafted in a particular moment in history, very different from the technologically sophisticated era in which we live. However the Fourth Amendment guarantees security in our persons, papers and effects. This security is deeply undermined when old doctrines are reflexively imported into a technological context that the founders could never have anticipated.

More recently, in his decision in *Kyllo v. United States,* Justice Antonin Scalia recognized the need for the law to adapt to preserve traditional expectations of privacy from technological advances in

---

[4] *United States v. Warshak*, 631 F.3d 266.
[5] *Id.* at 274.
[6] *United States v. Hamilton,* 701 F.3d 404 (Fourth Cir. 2012) at 408 (citation omitted)
[7] *Kyllo v. United States*, 533 U. S. 27, 33 (emphasis added)
[8] *Olmstead v. United States*, 277 U.S. 438, 471 (1928) JUSTICE BRANDEIS, dissenting.
[9] *Id.* at 474
[10] *Id.*
[11] *Id.*

a ruling that found that a thermal imaging device that measured heat emanating from a house constituted a search.[12]

In order to take up Justice Brandeis' challenge to preserve the right to privacy as technology develops we must acknowledge that this right does not fit neatly into one silo in the digital world. Information that generally has no Fourth Amendment protection as a consequence of the doctrine that there is a lack of privacy expectations in records held by a third party may still intuitively fall within what Americans consider the private realm. In order to preserve any private realm in modern society, we must rethink the level of protection afforded to business records, and the expectation of privacy regarding information held by third parties.

The amendment I offered would have ensured that the private information contained in business records and communications metadata required a showing of probable cause before being obtained. Section 215 of the Patriot Act allows for the collection of business records and phone metadata if there are reasonable grounds to believe that the information being sought is relevant to an authorized investigation. While the USA FREEDOM Act as amended does take steps to prevent the bulk collection of business records under section 215, it leaves the current standard of "reasonable grounds" untouched for everything but telephone metadata, which uses the modestly higher standard of "reasonable articulable suspicion."

In his testimony before the Senate Judiciary Committee, Princeton Computer Science professor Edward Felten said: "Metadata can now yield startling insights about individuals and groups, particularly when collected in large quantities across the population. It is no longer safe to assume that this 'summary' or 'non-content' information is less revealing or less sensitive than the content it describes . . ."[13] and ". . . newfound data storage capacity has led to new ways of exploiting the digital record. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behavior."[14]

Professor Felten went on to explain that "although the metadata might, on first impression seem to be little more than 'information concerning the numbers dialed' analysis of telephony metadata often reveals information that could traditionally, only be obtained by examining the content of communications. [That is], Metadata is often a proxy for content."[15]

Indeed, former NSA general counsel Stewart Baker stated "Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content . . ."[16]

That this is the case is clear when we consider the kinds and amount of information collected in the ordinary course of business today. In the age of big data, mobile computing and the "internet

---

[12] *Kyllo v. United States*, 533 U.S. 27, 40 (2001)

[13] Written Testimony of Edward W. Felten Professor of Computer Science and Public Affairs, Princeton University United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act October 2, 2013, at 1.

[14] *Id.* At 5.

[15] *Id.* At 8

[16] Alan Rudsbridger, The Snowden Leaks and the Public, The New York Review of Books, Nov. 21, 2013 quoting Steward Baker.

of things," your cell phone knows everywhere you go, search engines know your deepest thoughts and most embarrassing questions, online advertisers know everywhere you go, and thanks to the advances in cheap storage and computing power that underlie the big data revolution all of this information can be processed, indexed, and combined with other sources of mass data to tell you more about a person than they know about themselves.

Entire companies are built today on the premise that they can know what you want before you do. This trend will only increase as technology becomes more and more sophisticated and processors and wireless internet connections are added to our thermostats, our refrigerators, even our door locks. It is for this reason that a real discussion about requiring probable cause to obtain business records needs to take place.

However, it is important that discussions about privacy protections that should be offered to third party held data also consider how it's stored and where. It's long been accepted that the Constitution governs the United States, not the rest of the world. Where one would need a warrant to search a place within the physical borders of the United States, a warrant is not required—or even available to apply for or to receive—to search outside of the physical boundaries of the United States.

But does that doctrine still make sense? If the servers of Internet providers are scattered across the globe, and the private data of Americans held within them, can it be argued that the mere location of the servers that make up the "cloud" are the defining element of how American privacy is to be protected? If the American government could legally vacuum up the emails, address books and stored communications of Americans because the data was accessible in Europe or Asia instead of North Dakota or Utah, does that make a difference in reality as compared to law? As the Court in *Katz* said "the Fourth Amendment protects people, not places."[17]

I also offered two amendments that sought to restrict how communications were targeted and under what subject matter using section 702 authority was appropriate. Congress and our country has been told repeatedly that surveillance is being deployed to prevent terrorists from harming our country. However, in a process sanctioned by the FISA Courts, the NSA currently sweeps up not only communications to or from an intelligence target, but also all communications "about" the target. False positives and intentional uses of vague "about" criteria can create the opportunity for the massive collection of U.S. persons' communications. My amendment would prevent this by limiting the collection communications to only when one of the parties to that communication is the target of an authorized investigation.

The subject matter jurisdiction that gives rise to surveillance activity under the act is "foreign intelligence information," which includes "foreign policy," not terrorism. I offered an amendment that removed "foreign policy" from the definition of "foreign intelligence information" to clarify that 702 in particular is only for counterterrorism, proliferation of WMDs, or to protect armed forces. Absent this clarification, the diminution of freedom represented by the For-

[17] *Katz* at 351.

eign Intelligence Surveillance Act may be used not just to protect against terrorists or to advance military interests, but simply to advance goals related to foreign policy, including trade and related endeavors. That is not the bargain struck by the American people to protect their safety, and calls out for a tighter definition.

The last amendment I offered clarified what I hope was a drafting error in the Manager's Amendment. The Manager's Amendment states that telephone metadata did not include the content of calls. An ambiguity may have been created as to whether business records under section 215 could include the content of other communications since a similar prohibition is not directed toward those records. Is it the Committee's intent that content generated by Americans held by third parties as business records—other than telephonic metadata—be available under the low evidentiary standards of Section 215? If not, a clarification on this point would be helpful. I withdrew this amendment with the assurance of the Chairman of the committee that this potential clerical error would be further examined.

Finally, as legislators we can do our best to enact clear restrictions on obtaining Americans' private data, but without transparency it is difficult to know whether those restrictions are ultimately effective. An amendment offered by Rep. Delbene fixed a defect in the Manager's Amendment and will allow recipients of surveillance orders to issue reports regarding the number of orders received and user accounts affected by those orders. However, Members on both sides of the aisle, including Rep. Delbenne agreed that even more accurate reporting would improve the amendment adopted during mark up. The USA FREEDOM Act provided for reporting in "bands" of 100 and incorporated my bill, the Surveillance Order Reporting Act, which outlined the more precise reporting opportunities. These narrower bands should be included in this measure as the bill moves forward in the legislative process. More accurate reporting would allow businesses who receive surveillance orders to serve as our "canary in the coal mine," so that it does not take another historic national security data breach to learn that intelligence agencies are violating the privacy of our citizens.

I support the improvements to the status quo offered by the USA FREEDOM Act as amended, but I believe that our obligation to support the Fourth Amendment should lead us to do more. The USA FREEDOM Act should be just the beginning of this discussion, rather than its conclusion. I hope to have the opportunity to offer amendments not adopted by the Judiciary Committee when the full House considers this matter.

ZOE LOFGREN.

○