118TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 118–307
Part 1

PROTECT LIBERTY AND END WARRANTLESS SURVEILLANCE ACT OF 2023

DECEMBER 11, 2023.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

[To accompany H.R. 6570]

The Committee on the Judiciary, to whom was referred the bill (H.R. 6570) to amend the Foreign Intelligence Surveillance Act of 1978 to reform certain authorities and to provide greater transparency and oversight, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all that follows after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protect Liberty and End Warrantless Surveillance Act of 2023".

SEC. 2. QUERY PROCEDURE REFORM.

(a) LIMITATION ON ELIGIBILITY TO CONDUCT QUERIES.—Section 702(f)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)(1)) is amended by adding at the end the following:

"(D) LIMITATION ON ELIGIBILITY OF FBI PERSONNEL TO CONDUCT UNITED STATES PERSON QUERIES.—The Attorney General shall ensure that the procedures adopted under subparagraph (A) limit the authority to conduct queries such that—

"(i) for each field office of the Federal Bureau of Investigation, the most senior official whose primary duty station is that field office is authorized to designate not more than five individuals whose primary duty station is that field office who are eligible to conduct a query using a United States person query term; and

"(ii) for the headquarters of the Federal Bureau of Investigation, the Director of the Federal Bureau of Investigation is authorized to designate not more than five individuals whose primary duty station is the Headquarters of the Federal Bureau of Investigation who are eligible to conduct a query using a United States person query term.".

(b) PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.—Section 702(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)), as amended by subsection (a), is further amended—

(1) in paragraph (1)—

(A) in subparagraph (A), by inserting "and the limitations and requirements in paragraph (2)" after "Constitution of the United States"; and

(B) in subparagraph (B), by striking "United States person query term used for a query" and inserting "term for a United States person or person reasonably believed to be in the United States used for a query as required by paragraph (3)";

(2) by redesignating paragraph (3) as paragraph (6); and

(3) by striking paragraph (2) and inserting the following:

"(2) PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS AND OTHER INFORMATION OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.—

"(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C), no officer or employee of the United States may conduct a query of information acquired under this section in an effort to find communications or information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States, of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information.

"(B) EXCEPTIONS FOR CONCURRENT AUTHORIZATION, CONSENT, EMERGENCY SITUATIONS, AND CERTAIN DEFENSIVE CYBERSECURITY QUERIES.—

"(i) IN GENERAL.—Subparagraph (A) shall not apply to a query related to a United States person or person reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information if—

"(I) such person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105 or 304 of this Act, or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction authorizing the conduct of the query;

"(II)(aa) the officer or employee carrying out the query has a reasonable belief that—

"(AA) an emergency exists involving an imminent threat of death or serious bodily harm; and

"(BB) in order to prevent or mitigate this threat, the query must be conducted before authorization pursuant to subparagraph (I) can, with due diligence, be obtained; and

"(bb) a description of the query is provided to the Foreign Intelligence Surveillance Court and the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and of the Senate in a timely manner;

"(III) such person or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person, has provided consent to the query on a case-by-case basis; or

"(IV)(aa) the query uses a known cybersecurity threat signature as a query term;

"(bb) the query is conducted, and the results of the query are used, for the sole purpose of identifying targeted recipients of malicious software and preventing or mitigating harm from such malicious software;

"(cc) no additional contents of communications retrieved as a result of the query are accessed or reviewed; and

"(dd) all such queries are reported to the Foreign Intelligence Surveillance Court.

"(ii) LIMITATIONS.—

"(I) USE IN SUBSEQUENT PROCEEDINGS AND INVESTIGATIONS.—No information retrieved pursuant to a query authorized by clause (i)(II) or information derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, 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, except in proceedings or investigations that arise from the threat that prompted the query.

"(II) ASSESSMENT OF COMPLIANCE.—The Attorney General shall not less frequently than annually assess compliance with the requirements under subclause (I).

"(C) MATTERS RELATING TO EMERGENCY QUERIES.—

"(i) TREATMENT OF DENIALS.—In the event that a query for communications or information, the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States, of or about 1 more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information is conducted pursuant to an emergency authorization described in subparagraph (B)(i)(I) and the application for such emergency authorization is denied, or in any other case in which the query has been conducted and no order is issued approving the query—

"(I) no information obtained or evidence derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, 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

"(II) no information concerning any United States person or person reasonably believed to be located in the United States at the time of the query or the time of the communication or the creation of the information acquired from such query may subsequently be used or disclosed in any other manner 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.

"(ii) ASSESSMENT OF COMPLIANCE.—The Attorney General shall not less frequently than annually assess compliance with the requirements under clause (i).

"(D) FOREIGN INTELLIGENCE PURPOSE.—Except as provided in subparagraph (B)(i), no officer or employee of the United States may conduct a query of information acquired under this section in an effort to find information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information unless the query is reasonably likely to retrieve foreign intelligence information.

"(3) DOCUMENTATION.—No officer or employee of the United States may conduct a query of information acquired under this section in an effort to find information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of query or the time of the communication or the creation of the information, unless first an electronic record is created, and a system, mechanism, or business practice is in place to maintain such record, that includes the following:

"(A) Each term used for the conduct of the query.

"(B) The date of the query.

"(C) The identifier of the officer or employee.

"(D) A statement of facts showing that the use of each query term included under subparagraph (A) is—

"(i) reasonably likely to retrieve foreign intelligence information; or

"(ii) in furtherance of the exceptions described in paragraph (2)(B)(i).

"(4) PROHIBITION ON RESULTS OF METADATA QUERY AS A BASIS FOR ACCESS TO COMMUNICATIONS AND OTHER PROTECTED INFORMATION.—If a query of information acquired under this section is conducted in an effort to find communications metadata of 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or communication and the query returns such metadata, the results of the query shall not be used as a basis for reviewing communications or information a query for which is otherwise prohibited under this section.

"(5) FEDERATED DATASETS.—The prohibitions and requirements in this section shall apply to queries of federated and mixed datasets that include information acquired under this section, unless a mechanism exists to limit the query to information not acquired under this section.".

SEC. 3. LIMITATION ON USE OF INFORMATION OBTAINED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 RELATING TO UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES IN CRIMINAL, CIVIL, AND ADMINISTRATIVE ACTIONS.

Paragraph (2) of section 706(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881e(a)) is amended to read as follows:

"(2) LIMITATION ON USE IN CRIMINAL, CIVIL, AND ADMINISTRATIVE PROCEEDINGS AND INVESTIGATIONS.—No information acquired pursuant to section 702(f) of or about a United States person or person reasonably believed to be located in the United States at the time of acquisition or communication may be introduced as evidence against such person in any criminal, civil, or administrative proceeding or used as part of any criminal, civil, or administrative investigation, except—

"(A) with the prior approval of the Attorney General; and

"(B) in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat of—

"(i) the commission of a Federal crime of terrorism under any of clauses (i) through (iii) of section 2332b(g)(5)(B) of title 18, United States Code;

"(ii) actions necessitating counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003));

"(iii) the proliferation or the use of a weapon of mass destruction (as defined in section 2332a(c) of title 18, United States Code);

"(iv) a cybersecurity breach or attack from a foreign country;

"(v) incapacitation or destruction of critical infrastructure (as defined in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)));

"(vi) an attack against the armed forces of the United States or an ally of the United States or to other personnel of the United States Government or a government of an ally of the United States; or

"(vii) international narcotics trafficking.".

SEC. 4. REPEAL OF AUTHORITY FOR THE RESUMPTION OF ABOUTS COLLECTION.

(a) IN GENERAL.—Section 702(b)(5) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(b)(5)) is amended by striking ", except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017".

(b) CONFORMING AMENDMENTS.—

(1) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—Section 702(m) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(m)) is amended—

(A) in the subsection heading, by striking "REVIEWS, AND REPORTING" and inserting "AND REVIEWS"; and

(B) by striking paragraph (4).

(2) FISA AMENDMENTS REAUTHORIZATION ACT OF 2017.—Section 103 of the FISA Amendments Reauthorization Act of 2017 (Public Law 115–118; 50 U.S.C. 1881a note) is amended—

(A) by striking subsection (b); and

(B) by striking "(a) IN GENERAL.—".

SEC. 5. FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORM.

(a) REQUIREMENT FOR SAME JUDGE TO HEAR RENEWAL APPLICATIONS.—Section 103(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)(1))

is amended by adding at the end the following: "To the extent practicable, no judge designated under this subsection shall hear a renewal application for electronic surveillance under this Act, which application was previously granted by another judge designated under this subsection, unless the term of the judge who granted the application has expired, or that judge is otherwise no longer serving on the court.".

(b) USE OF AMICI CURIAE IN FOREIGN INTELLIGENCE SURVEILLANCE COURT PROCEEDINGS.—

(1) EXPANSION OF APPOINTMENT AUTHORITY.—

(A) IN GENERAL.—Section 103(i)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)) is amended—

(i) by striking subparagraph (A) and inserting the following:

"(A) shall, unless the court issues a finding that appointment is not appropriate, appoint 1 or more individuals who have been designated under paragraph (1), not fewer than 1 of whom possesses privacy and civil liberties expertise, unless the court finds that such a qualification is inappropriate, to serve as amicus curiae to assist the court in the consideration of any application or motion for an order or review that, in the opinion of the court—

"(i) presents a novel or significant interpretation of the law;

"(ii) presents significant concerns with respect to the activities of a United States person that are protected by the first amendment to the Constitution of the United States;

"(iii) presents or involves a sensitive investigative matter;

"(iv) presents a request for approval of a new program, a new technology, or a new use of existing technology;

"(v) presents a request for reauthorization of programmatic surveillance;

"(vi) otherwise presents novel or significant civil liberties issues; or

"(vii) otherwise involves the activities of a United States person; and"; and

(ii) in subparagraph (B), by striking "an individual or organization" each place the term appears and inserting "1 or more individuals or organizations".

(B) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—Section 103(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)) is amended by adding at the end the following:

"(12) DEFINITION.—In this subsection, the term 'sensitive investigative matter' means—

"(A) an investigative matter involving the activities of—

"(i) a domestic public official or political candidate, or an individual serving on the staff of such an official or candidate;

"(ii) a domestic religious or political organization, or a known or suspected United States person prominent in such an organization; or

"(iii) the domestic news media; or

"(B) any other investigative matter involving a domestic entity or a known or suspected United States person that, in the judgment of the applicable court established under subsection (a) or (b), is as sensitive as an investigative matter described in subparagraph (A).".

(2) AUTHORITY TO SEEK REVIEW.—Section 103(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)), as amended by subsection (a) of this section, is amended—

(A) in paragraph (4)—

(i) in the paragraph heading, by inserting "; AUTHORITY" after "DUTIES";

(ii) by redesignating subparagraphs (A), (B), and (C) as clauses (i), (ii), and (iii), respectively, and adjusting the margins accordingly;

(iii) in the matter preceding clause (i), as so redesignated, by striking "the amicus curiae shall" and inserting the following: "the amicus curiae—

"(A) shall";

(iv) in subparagraph (A)(i), as so redesignated, by inserting before the semicolon at the end the following: ", including legal arguments regarding any privacy or civil liberties interest of any United States person that would be significantly impacted by the application or motion"; and

(v) by striking the period at the end and inserting the following: "; and

"(B) may seek leave to raise any novel or significant privacy or civil liberties issue relevant to the application or motion or other issue directly im-

pacting the legality of the proposed electronic surveillance with the court, regardless of whether the court has requested assistance on that issue.";

(B) by redesignating paragraphs (7) through (12) as paragraphs (8) through (13), respectively; and

(C) by inserting after paragraph (6) the following:

"(7) AUTHORITY TO SEEK REVIEW OF DECISIONS.—

"(A) FISA COURT DECISIONS.—

"(i) PETITION.—Following issuance of an order under this Act by the Foreign Intelligence Surveillance Court, an amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court to certify for review to the Foreign Intelligence Surveillance Court of Review a question of law pursuant to subsection (j).

"(ii) WRITTEN STATEMENT OF REASONS.—If the Foreign Intelligence Surveillance Court denies a petition under this subparagraph, the Foreign Intelligence Surveillance Court shall provide for the record a written statement of the reasons for the denial.

"(iii) APPOINTMENT.—Upon certification of any question of law pursuant to this subparagraph, the Court of Review shall appoint the amicus curiae to assist the Court of Review in its consideration of the certified question, unless the Court of Review issues a finding that such appointment is not appropriate.

"(B) FISA COURT OF REVIEW DECISIONS.—An amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court of Review to certify for review to the Supreme Court of the United States any question of law pursuant to section 1254(2) of title 28, United States Code.

"(C) DECLASSIFICATION OF REFERRALS.—For purposes of section 602, a petition filed under subparagraph (A) or (B) of this paragraph and all of its content shall be considered a decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review described in paragraph (2) of section 602(a).".

(3) ACCESS TO INFORMATION.—

(A) APPLICATION AND MATERIALS.—Section 103(i)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(6)) is amended by striking subparagraph (A) and inserting the following:

"(A) IN GENERAL.—

"(i) RIGHT OF AMICUS.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

"(I) shall have access, to the extent such information is available to the Government, to—

"(aa) the application, certification, petition, motion, and other information and supporting materials, including any information described in section 901, submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed, including access to any relevant legal precedent (including any such precedent that is cited by the Government, including in such an application);

"(bb) an unredacted copy of each relevant decision made by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review in which the court decides a question of law, without regard to whether the decision is classified; and

"(cc) any other information or materials that the court determines are relevant to the duties of the amicus curiae; and

"(II) may make a submission to the court requesting access to any other particular materials or information (or category of materials or information) that the amicus curiae believes to be relevant to the duties of the amicus curiae.

"(ii) SUPPORTING DOCUMENTATION REGARDING ACCURACY.—The Foreign Intelligence Surveillance Court, upon the motion of an amicus curiae appointed under paragraph (2) or upon its own motion, may require the Government to make available the supporting documentation described in section 902.".

(B) CLARIFICATION OF ACCESS TO CERTAIN INFORMATION.—Section 103(i)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(6)) is amended—

(i) in subparagraph (B), by striking "may" and inserting "shall"; and

(ii) by striking subparagraph (C) and inserting the following:

"(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court shall have access, to the extent such information is available to the Government, to unredacted copies of each opinion, order, transcript, pleading, or other document of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review, including, if the individual is eligible for access to classified information, any classified documents, information, and other materials or proceedings.".

(4) EFFECTIVE DATE.—The amendments made by this section shall take effect on the date of enactment of this Act and shall apply with respect to proceedings under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) that take place on or after, or are pending on, that date.

SEC. 6. APPLICATION FOR AN ORDER APPROVING ELECTRONIC SURVEILLANCE.

(a) DISCLOSURE REQUIREMENT.—Section 104(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804(a)) is amended—

(1) in paragraph (6)(E)(ii), by inserting before the semicolon at the end "(and a description of such techniques)";

(2) in paragraph (8), by striking "and" at the end;

(3) in paragraph (9), by striking the period at the end and inserting "; and" ; and

(4) by inserting after paragraph (9) the following:

"(10) all information material to the application, including any information that tends to rebut—

"(A) any allegation set forth in the application; or

"(B) the existence of probable cause to believe that—

"(i) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

"(ii) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.".

(b) PROHIBITION ON USE OF CERTAIN INFORMATION.—Section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended by adding at the end the following:

"(e) The statement of facts and circumstances under subsection (a)(3) may only include information obtained from the content of a media source or information gathered by a political campaign if—

"(1) such information is disclosed in the application as having been so obtained or gathered; and

"(2) such information is not the sole source of the information used to justify the applicant's belief described in subsection (a)(3).".

(c) LIMITATION ON ISSUANCE OF ORDER.—Section 105(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(a)) is amended—

(1) in paragraph (3), by striking "; and" and inserting a semicolon;

(2) in paragraph (4), by striking the period and inserting "; and"; and

(3) by adding at the end the following:

"(5) the statement of facts and circumstances under subsection (a)(3) may only include information obtained from the content of a media source or information gathered by a political campaign if—

"(A) such information is disclosed in the application as having been so obtained or gathered; and

"(B) such information is not the sole source of the information used to justify the applicant's belief described in subsection (a)(3).".

SEC. 7. PUBLIC DISCLOSURE AND DECLASSIFICATION OF CERTAIN DOCUMENTS.

(a) SUBMISSION TO CONGRESS.—Section 601(c)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(c)) is amended by inserting ", including declassified copies that have undergone review under section 602" before "; and".

(b) TIMELINE FOR DECLASSIFICATION REVIEW.—Section 602(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1872(a)) is amended—

(1) by inserting after "shall conduct a declassification review" the following: ", to be concluded not later than 45 days after the commencement of such review,"; and

(2) by inserting after "a significant construction or interpretation of any provision of law" the following: "or results in a change of application of any provision of this Act or a novel application of any provision of this Act".

SEC. 8. TRANSCRIPTIONS OF PROCEEDINGS; ATTENDANCE OF CERTAIN CONGRESSIONAL OFFICIALS AT CERTAIN PROCEEDINGS.

Section 103(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(c)) is amended—

(1) by striking "Proceedings under this Act" and inserting the following: "(1) Proceedings under this Act";

(2) by striking "including applications made and orders granted" and inserting "including applications made, orders granted, and transcriptions of proceedings,"; and

(3) by adding at the end:

"(2) The chair and ranking minority member of each of the congressional intelligence committees and of the Committees on the Judiciary of the House of Representatives and of the Senate shall be entitled to attend any proceeding of the Foreign Intelligence Surveillance Court or any proceeding of the Foreign Intelligence Surveillance Court of Review. Each person entitled to attend a proceeding pursuant to this paragraph may designate not more than 2 Members of Congress and not more than 2 staff members of such committee to attend on their behalf, pursuant to such procedures as the Attorney General, in consultation with the Director of National Intelligence may establish. Not later than 45 days after any such proceeding, a copy of any application made, order granted, or transcription of the proceeding shall be made available for review to each person who is entitled to attend a proceeding pursuant to this paragraph or who is designated under this paragraph. Terms used in this paragraph have the meanings given such terms in section 701(b).".

SEC. 9. ANNUAL AUDIT OF FISA COMPLIANCE BY INSPECTOR GENERAL.

(a) REPORT REQUIRED.—Title VI of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871 et seq.) is amended by adding at the end the following:

"SEC. 605. ANNUAL AUDIT OF FISA COMPLIANCE BY INSPECTOR GENERAL.

"Beginning with the first calendar year that begins after the effective date of this section, by not later than June 30th of that year and each year thereafter, the Inspector General of the Department of Justice shall conduct an audit on alleged violations and failures to comply with the requirements of this Act and any procedures established pursuant to this Act, and submit a report thereon to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and of the Senate.".

(b) CLERICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding at the end the following:

"605. Annual audit of FISA compliance by Inspector General.".

SEC. 10. REPORTING ON ACCURACY AND COMPLETENESS OF APPLICATIONS.

Section 603 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873) is amended—

(1) in subsection (a)(1)—

(A) by redesignating subparagraphs (B) through (F) as subparagraphs (C) through (G) respectively; and

(B) by inserting after subparagraph (A) the following:

"(B) an analysis of the accuracy and completeness of such applications and certifications submitted;"; and

(2) in subsection (a)(2), by striking "subparagraph (F)" and inserting "subparagraph (G)".

SEC. 11. ANNUAL REPORT OF THE FEDERAL BUREAU OF INVESTIGATION.

(a) REPORT REQUIRED.—Title VI of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871 et seq.), as amended by this Act, is further amended by adding at the end the following:

"SEC. 606. ANNUAL REPORT OF THE FEDERAL BUREAU OF INVESTIGATION.

"Not later than 1 year after the date of enactment of this section, and annually thereafter, the Director of the Federal Bureau of Investigation shall submit to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and of the Senate—

"(1) a report on disciplinary activities taken by the Director to address violations of the requirements of law or the procedures established under this Act, including a comprehensive account of disciplinary investigations, including—

"(A) all such investigations ongoing as of the date the report is submitted;

"(B) the adjudications of such investigations when concluded; and

"(C) disciplinary actions taken as a result of such adjudications; and

"(2) a report on the conduct of queries conducted under section 702 for the preceding year using a United States person query term, including—

"(A) the number of such queries conducted;

"(B) what terms were used;

"(C) the number of warrants issued and denied under section 702(f)(1); and

"(D) the number of times exceptions were alleged under 702(f)(2).".

(b) CLERICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by this Act, is further amended by adding at the end the following:

"606. Annual report of the Federal Bureau of Investigation.".

SEC. 12. EXTENSION OF TITLE VII OF FISA; EXPIRATION OF FISA AUTHORITIES; EFFECTIVE DATES.

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

(1) in paragraph (1)—

(A) by striking "December 31, 2023" and inserting "December 31, 2026"; and

(B) by striking ", as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017," and inserting ", as most recently amended,"; and

(2) in paragraph (2) in the matter preceding subparagraph (A), by striking "December 31, 2023" and inserting "December 31, 2026".

(b) CONFORMING AMENDMENTS.—Section 404(b) of the FISA Amendments Act of 2008 (Public Law 110–261; 122 Stat. 2476), is amended—

(1) in paragraph (1)—

(A) in the heading, by striking "DECEMBER 31, 2023" and inserting "DECEMBER 31, 2026"; and

(B) by striking ", as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017," and inserting ", as most recently amended,";

(2) in paragraph (2), by striking ", as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017," and inserting ", as most recently amended,"; and

(3) in paragraph (4)—

(A) by striking ", as added by section 101(a) and amended by the FISA Amendments Reauthorization Act of 2017," both places it appears and inserting ", as added by section 101(a) and as most recently amended,"; and

(B) by striking ", as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017," and inserting ", as most recently amended," both places it appears.

SEC. 13. CRIMINAL PENALTIES FOR VIOLATIONS OF FISA.

(a) IN GENERAL.—Section 109 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809) is amended as follows:

(1) ADDITIONAL OFFENSES.—In subsection (a)—

(A) in the matter preceding paragraph (1), by striking "intentionally";

(B) in paragraph (1)—

(i) by inserting "intentionally" before "engages in"; and

(ii) by striking "or" at the end;

(C) in paragraph (2)—

(i) by inserting "intentionally" before "disclose or uses"; and

(ii) by striking the period at the end and inserting a semicolon; and

(D) by adding at the end the following:

"(3) knowingly submits any document to or makes any false statement before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, knowing such document or statement to contain—

"(A) a false material declaration; or

"(B) a material omission; or

"(4) knowingly discloses the existence of an application for an order authorizing surveillance under this title, or any information contained therein, to any person not authorized to receive such information.".

(2) ENHANCED PENALTIES.—In subsection (c), is amended to read as follows:

"(c) PENALTIES.—In the case of an offense under any of paragraphs (1) through (4) of subsection (a), the offense is punishable by a fine of not more than $10,000 or imprisonment for not more than 8 years, or both.".

(b) RULE OF CONSTRUCTION.—This Act and the amendments made by this Act may not be construed to interfere with the enforcement of section 798 of title 18, United States Code, or any other provision of law regarding the unlawful disclosure of classified information.

SEC. 14. CONTEMPT POWER OF FISC AND FISC–R.

(a) IN GENERAL.—Chapter 21 of title 18, United States Code, is amended—

(1) in section 402, by inserting after "any district court of the United States" the following: ", the Foreign Intelligence Surveillance Court, the Foreign Intelligence Surveillance Court of Review,"; and

(2) by adding at the end the following:

"§ 404. Definitions

"For purposes of this chapter—

"(1) the term 'court of the United States' includes the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review; and

"(2) the terms 'Foreign Intelligence Surveillance Court' and 'Foreign Intelligence Surveillance Court of Review' have the meanings given such terms in section 601(e) of the Foreign Intelligence Surveillance Act of 1978.".

(b) CLERICAL AMENDMENT.—The table of sections for such chapter is amended by inserting after the item pertaining to section 403 the following:

"404. Definitions.".

(c) REPORT.—Not later than one year after the date of enactment, and annually thereafter the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review (as such terms are defined in section 601(e) of the Foreign Intelligence Surveillance Act of 1978) shall jointly submit to Congress a report on the exercise of authority under chapter 21 of title 18, United States Code, by such courts during the previous year.

SEC. 15. INCREASED PENALTIES FOR CIVIL ACTIONS.

(a) INCREASED PENALTIES.—Section 110(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1810(a)) is amended to read as follows:

"(a) actual damages, but not less than liquidated damages equal to the greater of—

"(1) if the aggrieved person is a United States person, $10,000 or $1,000 per day for each day of violation; or

"(2) for any other aggrieved person, $1,000 or $100 per day for each day of violation;".

(b) REPORTING REQUIREMENT.—Title I of the Foreign Intelligence Surveillance Act of 1978 is amended by inserting after section 110 the following:

"SEC. 110A. REPORTING REQUIREMENTS FOR CIVIL ACTIONS.

"(a) REPORT TO CONGRESS.—If a court finds that a person has violated this Act in a civil action under section 110, the head of the agency that employs that person shall report to Congress on the administrative action taken against that person pursuant to section 607 or any other provision of law.

"(b) FISC.—If a court finds that a person has violated this Act in a civil action under section 110, the head of the agency that employs that person shall report the name of such person to the Foreign Intelligence Surveillance Court. The Foreign Intelligence Surveillance Court shall maintain a list of each person about whom it received a report under this subsection.".

SEC. 16. ACCOUNTABILITY PROCEDURES FOR INCIDENTS RELATING TO QUERIES CONDUCTED BY THE FEDERAL BUREAU OF INVESTIGATION.

(a) IN GENERAL.—Title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.) is amended by adding at the end the following:

"SEC. 709. ACCOUNTABILITY PROCEDURES FOR INCIDENTS RELATING TO QUERIES CONDUCTED BY THE FEDERAL BUREAU OF INVESTIGATION.

"(a) IN GENERAL.—The Director of the Federal Bureau of Investigation shall establish procedures to hold employees of the Federal Bureau of Investigation accountable for violations of law, guidance, and procedure governing queries of information acquired pursuant to section 702.

"(b) ELEMENTS.—The procedures established under subsection (a) shall include the following:

"(1) Centralized tracking of individual employee performance incidents involving negligent violations of law, guidance, and procedure described in subsection (a), over time.

"(2) Escalating consequences for such incidents, including—

"(A) consequences for initial incidents, including, at a minimum—

"(i) suspension of access to information acquired under this Act; and

"(ii) documentation of the incident in the personnel file of each employee responsible for the violation; and

"(B) consequences for subsequent incidents, including, at a minimum—

"(i) possible indefinite suspension of access to information acquired under this Act;

"(ii) reassignment of each employee responsible for the violation; and

"(iii) referral of the incident to the Inspection Division of the Federal Bureau of Investigation for review of potentially reckless conduct.

"(3) Clarification of requirements for referring intentional misconduct and reckless conduct to the Inspection Division of the Federal Bureau of Investigation for investigation and disciplinary action by the Office of Professional Responsibility of the Federal Bureau of Investigation.".

(b) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 708 the following:

"709. Accountability procedures for incidents relating to queries conducted by the Federal Bureau of Investigation.".

(c) REPORT REQUIRED.—

(1) INITIAL REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of the Federal Bureau of Investigation shall submit to the Committees on the Judiciary of the House of Representatives and of the Senate and to the congressional intelligence committees (as such term is defined in section 801 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1885)) a report detailing the procedures established under section 709 of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (a).

(2) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Federal Bureau of Investigation shall submit to the Committees on the Judiciary of the House of Representatives and of the Senate and to the congressional intelligence committees (as such term is defined in section 801 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1885)) a report on any disciplinary actions taken pursuant to the procedures established under section 709 of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (a), including a description of the circumstances surrounding each such disciplinary action, and the results of each such disciplinary action.

(3) FORM.—The reports required under paragraphs (1) and (2) shall be submitted in unclassified form, but may include a classified annex to the extent necessary to protect sources and methods.

SEC. 17. AGENCY PROCEDURES TO ENSURE COMPLIANCE.

(a) AGENCY PROCEDURES TO ENSURE COMPLIANCE.—Title VI of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871 et seq.), as amended by this Act, is further amended by adding at the end the following:

"SEC. 607. AGENCY PROCEDURES TO ENSURE COMPLIANCE.

"The head of each Federal department or agency authorized to acquire foreign intelligence information under this Act shall establish procedures—

"(1) setting forth clear rules on what constitutes a violation of this Act by an officer or employee of that department or agency; and

"(2) for taking appropriate adverse personnel action against any officer or employee of the department or agency who engages in such a violation, including more severe adverse actions for any subsequent violation.".

(b) CLERICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by this Act, is further amended by adding at the end the following:

"607. Agency procedures to ensure compliance.".

(c) REPORT.—Not later than 3 months after the date of enactment of this Act, the head of each Federal department or agency that is required to establish procedures under section 607 of the Foreign Intelligence Surveillance Act of 1978 shall report to Congress on such procedures.

SEC. 18. PROTECTION OF RECORDS HELD BY DATA BROKERS.

Section 2702 of title 18, United States Code, is amended by adding at the end the following:

"(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR ANYTHING OF VALUE CERTAIN RECORDS AND INFORMATION BY LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.—

"(1) DEFINITIONS.—In this subsection—

"(A) the term 'covered customer or subscriber record' means a covered record that is—

"(i) disclosed to a third party by—

"(I) a provider of an electronic communication service to the public or a provider of a remote computing service of which the covered person with respect to the covered record is a subscriber or customer; or

"(II) an intermediary service provider that delivers, stores, or processes communications of such covered person;

"(ii) collected by a third party from an online account of a covered person; or

"(iii) collected by a third party from or about an electronic device of a covered person;

"(B) the term 'covered person' means—

"(i) a person who is located inside the United States; or

"(ii) a person—

"(I) who is located outside the United States or whose location cannot be determined; and

"(II) who is a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

"(C) the term 'covered record' means a record or other information that—

"(i) pertains to a covered person; and

"(ii) is—

"(I) a record or other information described in the matter preceding paragraph (1) of subsection (c);

"(II) the contents of a communication; or

"(III) location information;

"(D) the term 'electronic device' has the meaning given the term 'computer' in section 1030(e);

"(E) the term 'illegitimately obtained information' means a covered record that—

"(i) was obtained—

"(I) from a provider of an electronic communication service to the public or a provider of a remote computing service in a manner that—

"(aa) violates the service agreement between the provider and customers or subscribers of the provider; or

"(bb) is inconsistent with the privacy policy of the provider;

"(II) by deceiving the covered person whose covered record was obtained; or

"(III) through the unauthorized accessing of an electronic device or online account; or

"(ii) was—

"(I) obtained from a provider of an electronic communication service to the public, a provider of a remote computing service, or an intermediary service provider; and

"(II) collected, processed, or shared in violation of a contract relating to the covered record;

"(F) 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);

"(G) the term 'location information' means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, or device;

"(H) the term 'obtain in exchange for anything of value' means to obtain by purchasing, to receive in connection with services being provided for consideration, or to otherwise obtain in exchange for consideration, including an access fee, service fee, maintenance fee, or licensing fee;

"(I) the term 'online account' means an online account with an electronic communication service to the public or remote computing service;

"(J) the term 'pertain', with respect to a person, means—

"(i) information that is linked to the identity of a person; or

"(ii) information—

"(I) that has been anonymized to remove links to the identity of a person; and

"(II) that, if combined with other information, could be used to identify a person; and

"(K) the term 'third party' means a person who—

"(i) is not a governmental entity; and

"(ii) in connection with the collection, disclosure, obtaining, processing, or sharing of the covered record at issue, was not acting as—

"(I) a provider of an electronic communication service to the public; or

"(II) a provider of a remote computing service.

"(2) LIMITATION.—

"(A) IN GENERAL.—A law enforcement agency of a governmental entity and an element of the intelligence community may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information.

"(B) INDIRECTLY ACQUIRED RECORDS AND INFORMATION.—The limitation under subparagraph (A) shall apply without regard to whether the third party possessing the covered customer or subscriber record or illegitimately obtained information is the third party that initially obtained or collected, or is the third party that initially received the disclosure of, the covered customer or subscriber record or illegitimately obtained information.

"(3) LIMIT ON SHARING BETWEEN AGENCIES.—An agency of a governmental entity that is not a law enforcement agency or an element of the intelligence community may not provide to a law enforcement agency of a governmental entity or an element of the intelligence community a covered customer or subscriber record or illegitimately obtained information that was obtained from a third party in exchange for anything of value.

"(4) PROHIBITION ON USE AS EVIDENCE.—A covered customer or subscriber record or illegitimately obtained information obtained by or provided to a law enforcement agency of a governmental entity or an element of the intelligence community in violation of paragraph (2) or (3), and any evidence derived therefrom, may not be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

"(5) MINIMIZATION PROCEDURES.—

"(A) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of information pertaining to a covered person that is acquired in violation of paragraph (2) or (3).

"(B) USE BY AGENCIES.—If a law enforcement agency of a governmental entity or element of the intelligence community acquires information pertaining to a covered person in violation of paragraph (2) or (3), the law enforcement agency of a governmental entity or element of the intelligence community shall minimize the acquisition and retention, and prohibit the dissemination, of the information in accordance with the procedures adopted under subparagraph (A).".

SEC. 19. REQUIRED DISCLOSURE.

Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(i) COVERED CUSTOMER OR SUBSCRIBER RECORDS AND ILLEGITIMATELY OBTAINED INFORMATION.—

"(1) DEFINITIONS.—In this subsection, the terms 'covered customer or subscriber record', 'illegitimately obtained information', and 'third party' have the meanings given such terms in section 2702(e).

"(2) LIMITATION.—Unless a governmental entity obtains an order in accordance with paragraph (3), the governmental entity may not require a third party to disclose a covered customer or subscriber record or any illegitimately obtained information if a court order would be required for the governmental entity to require a provider of remote computing service or a provider of electronic communication service to the public to disclose such a covered customer or subscriber record or illegitimately obtained information that is a record of a customer or subscriber of the provider.

"(3) ORDERS.—

"(A) IN GENERAL.—A court may only issue an order requiring a third party to disclose a covered customer or subscriber record or any illegitimately obtained information on the same basis and subject to the same limitations as would apply to a court order to require disclosure by a provider of remote computing service or a provider of electronic communication service to the public of a record of a customer or subscriber of the provider.

"(B) STANDARD.—For purposes of subparagraph (A), a court shall apply the most stringent standard under Federal statute or the Constitution of the United States that would be applicable to a request for a court order to require a comparable disclosure by a provider of remote computing service or a provider of electronic communication service to the public of a record of a customer or subscriber of the provider.".

SEC. 20. INTERMEDIARY SERVICE PROVIDERS.

(a) DEFINITION.—Section 2711 of title 18, United States Code, is amended—

(1) in paragraph (3), by striking "and" at the end;

(2) in paragraph (4), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(5) the term 'intermediary service provider' means an entity or facilities owner or operator that directly or indirectly delivers, stores, or processes communications for or on behalf of a provider of electronic communication service to the public or a provider of remote computing service.".

(b) PROHIBITION.—Section 2702(a) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking "and" at the end;

(2) in paragraph (2), by striking "and" at the end;

(3) in paragraph (3), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following:

"(4) an intermediary service provider shall not knowingly divulge—

"(A) to any person or entity the contents of a communication while in electronic storage by that provider; or

"(B) to any governmental entity a record or other information pertaining to a subscriber to or customer of, a recipient of a communication from a subscriber to or customer of, or the sender of a communication to a subscriber to or customer of, the provider of electronic communication service to the public or the provider of remote computing service for, or on behalf of, which the intermediary service provider directly or indirectly delivers, transmits, stores, or processes communications.".

SEC. 21. LIMITS ON SURVEILLANCE CONDUCTED FOR FOREIGN INTELLIGENCE PURPOSES OTHER THAN UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) IN GENERAL.—Section 2511(2)(f) of title 18, United States Code, is amended to read as follows:

"(f)(i)(A) Nothing contained in this chapter, chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934 (47 U.S.C. 151 et seq.) shall be deemed to affect an acquisition or activity described in clause (B) that is carried out utilizing a means other than electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(B) An acquisition or activity described in this clause is—

"(I) an acquisition by the United States Government of foreign intelligence information from international or foreign communications that—

"(aa) is acquired pursuant to express statutory authority; or

"(bb) only includes information of persons who are not United States persons and are located outside the United States; or

"(II) a foreign intelligence activity involving a foreign electronic communications system that—

"(aa) is conducted pursuant to express statutory authority; or

"(bb) only involves the acquisition by the United States Government of information of persons who are not United States persons and are located outside the United States.

"(ii) The procedures in this chapter, chapter 121, and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.".

(b) EXCLUSIVE MEANS RELATED TO COMMUNICATIONS RECORDS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic communications transactions records, call detail records, or other information from communications of United States persons or persons inside the United States are acquired for foreign intelligence purposes inside the United States or from a person or entity located in the United States that provides telecommunications, electronic communication, or remote computing services.

(c) EXCLUSIVE MEANS RELATED TO LOCATION INFORMATION, WEB BROWSING HISTORY, AND INTERNET SEARCH HISTORY.—

(1) DEFINITION.—In this subsection, the term "location information" has the meaning given that term in subsection (e) of section 2702 of title 18, United States Code, as added by section 2 of this Act.

(2) EXCLUSIVE MEANS.—Title I and sections 303, 304, 703, 704, and 705 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq., 1823, 1824, 1881b, 1881c, 1881d) shall be the exclusive means by which location information, web browsing history, and internet search history of United States persons or persons inside the United States are acquired for foreign intelligence purposes inside the United States or from a person or entity located in the United States.

(d) EXCLUSIVE MEANS RELATED TO FOURTH AMENDMENT-PROTECTED INFORMATION.—Title I and sections 303, 304, 703, 704, and 705 of the Foreign Intelligence

Surveillance Act of 1978 (50 U.S.C. 1801 et seq., 1823, 1824, 1881b, 1881c, 1881d) shall be the exclusive means by which any information, records, data, or tangible things are acquired for foreign intelligence purposes from a person or entity located in the United States if the compelled production of such information, records, data, or tangible things would require a warrant for law enforcement purposes.

(e) DEFINITION.—In this section, 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. 22. LIMIT ON CIVIL IMMUNITY FOR PROVIDING INFORMATION, FACILITIES, OR TECHNICAL ASSISTANCE TO THE GOVERNMENT ABSENT A COURT ORDER.

Section 2511(2)(a) of title 18, United States Code, is amended—

(1) in subparagraph (ii), by striking clause (B) and inserting the following:

"(B) a certification in writing—

"(I) by a person specified in section 2518(7) or the Attorney General of the United States;

"(II) that the requirements for an emergency authorization to intercept a wire, oral, or electronic communication under section 2518(7) have been met; and

"(III) that the specified assistance is required,"; and

(2) by striking subparagraph (iii) and inserting the following:

"(iii) For assistance provided pursuant to a certification under subparagraph (ii)(B), the limitation on causes of action under the last sentence of the matter following subparagraph (ii)(B) shall only apply to the extent that the assistance ceased at the earliest of the time the application for a court order was denied, the time the communication sought was obtained, or 48 hours after the interception began.".

SEC. 23. PROHIBITION ON REVERSE TARGETING OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

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

(1) in subsection (b)(2)—

(A) by striking "may not intentionally" and inserting the following: "may not—

"(A) intentionally"; and

(B) in subparagraph (A), as designated by subparagraph (A) of this paragraph, by striking "if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;" and inserting the following: "if a significant purpose of such acquisition is to acquire the information of 1 or more United States persons or persons reasonably believed to be located in the United States at the time of acquisition or communication, unless—

"(i)(I) there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm to such United States person or person reasonably believed to be located in the United States at the time of the query or the time of acquisition or communication;

"(II) the information is sought for the purpose of assisting that person; and

"(III) a description of the targeting is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress in a timely manner; or

"(ii) the United States person or persons reasonably believed to be located in the United States at the time of acquisition or communication has provided consent to the targeting, or if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person has provided consent; and

"(B) in the case of information acquired pursuant to subparagraph (A)(i) or evidence derived from such targeting, be used, received in evidence, or otherwise disseminated in any investigation, 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, except in proceedings or investigations that arise from the threat that prompted the targeting;";

(2) in subsection (d)(1), by amending subparagraph (A) to read as follows:

"(A) ensure that—

"(i) any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

"(ii) except as provided in subsection (b)(2), a significant purpose of an acquisition is not to acquire the information of 1 or more United States persons or persons reasonably believed to be in the United States at the time of acquisition or communication; and";

(3) in subsection (h)(2)(A)(i), by amending subclause (I) to read as follows:

"(I) ensure that—

"(aa) an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

"(bb) except as provided in subsection (b)(2), a significant purpose of an acquisition is not to acquire the information of 1 or more United States persons or persons reasonably believed to be in the United States at the time of acquisition or communication; and"; and

(4) in subsection (j)(2)(B), by amending clause (i) to read as follows:

"(i) ensure that—

"(I) an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

"(II) except as provided in subsection (b)(2), a significant purpose of an acquisition is not to acquire the information of 1 or more United States persons or persons reasonably believed to be in the United States at the time of acquisition or communication; and".

SEC. 24. REQUIRED DISCLOSURE OF RELEVANT INFORMATION IN FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 APPLICATIONS.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by adding at the end the following:

"TITLE IX—CERTIFICATION REGARDING ACCURACY PROCEDURES

"SEC. 901. CERTIFICATION REGARDING ACCURACY PROCEDURES.

"(a) DEFINITION OF ACCURACY PROCEDURES.—In this section, the term 'accuracy procedures' means specific procedures, adopted by the Attorney General, to ensure that an application for a court order under this Act, including any application for renewal of an existing order, is accurate and complete, including procedures that ensure, at a minimum, that—

"(1) the application reflects all information that might reasonably call into question the accuracy of the information or the reasonableness of any assessment in the application, or otherwise raises doubts about the requested findings;

"(2) the application reflects all material information that might reasonably call into question the reliability and reporting of any information from a confidential human source that is used in the application;

"(3) a complete file documenting each factual assertion in an application is maintained;

"(4) the applicant coordinates with the appropriate elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), concerning any prior or existing relationship with the target of any surveillance, search, or other means of investigation, and discloses any such relationship in the application;

"(5) before any application targeting a United States person is made, the applicant Federal officer shall document that the officer has collected and reviewed for accuracy and completeness supporting documentation for each factual assertion in the application; and

"(6) the applicant Federal agency establish compliance and auditing mechanisms on an annual basis to assess the efficacy of the accuracy procedures that have been adopted and report such findings to the Attorney General.

"(b) STATEMENT AND CERTIFICATION OF ACCURACY PROCEDURES.—Any Federal officer making an application for a court order under this Act shall include with the application—

"(1) a description of the accuracy procedures employed by the officer or the officer's designee; and

"(2) a certification that the officer or the officer's designee has collected and reviewed for accuracy and completeness—

"(A) supporting documentation for each factual assertion contained in the application;

"(B) all information that might reasonably call into question the accuracy of the information or the reasonableness of any assessment in the application, or otherwise raises doubts about the requested findings; and

"(C) all material information that might reasonably call into question the reliability and reporting of any information from any confidential human source that is used in the application.

"(c) NECESSARY FINDING FOR COURT ORDERS.—A judge may not enter an order under this Act unless the judge finds, in addition to any other findings required under this Act, that the accuracy procedures described in the application for the order, as required under subsection (b)(1), are actually accuracy procedures as defined in this section.".

(b) CLERICAL AMENDMENT.—The table of contents of the Foreign Intelligence Surveillance Act of 1978 is amended by adding at the end the following:

"TITLE IX—CERTIFICATION REGARDING ACCURACY PROCEDURES

"Sec. 901. Certification regarding accuracy procedures.".

SEC. 25. ENHANCED ANNUAL REPORTS BY DIRECTOR OF NATIONAL INTELLIGENCE.

(a) IN GENERAL.—Subsection (b) of section 603 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873(b)) is amended—

(1) in paragraph (2)(C), by striking the semicolon and inserting "; and";

(2) by redesignating paragraphs (3) through (7) as paragraphs (6) through (10), respectively;

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

"(3) a description of the subject matter of each of the certifications provided under section 702(h);

"(4) statistics revealing the number of persons and identifiers targeted under section 702(a), disaggregated by certification under which the person or identifier was targeted;

"(5) the total number of directives issued pursuant to section 702(i)(1), disaggregated by each type of electronic communication service provider described in subparagraphs (A) through (E) of section 701(b)(4);";

(4) in paragraph (9) (as redesignated in paragraph (2) of this subsection), by striking "and" at the end;

(5) in paragraph (10) (as redesignated in paragraph (2) of this subsection), by striking the period at the end and inserting a semicolon;

(6) by adding at the end the following:

"(11)(A) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons regardless of whether the identities of the United States persons were openly included or masked;

"(B) the total number of disseminated intelligence reports derived from collection not authorized by this Act containing the identities of United States persons regardless of whether the identities of the United States persons were openly included or masked;

"(C) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were masked;

"(D) the total number of disseminated intelligence reports derived from collection not authorized by this Act containing the identities of United States persons in which the identities of the United States persons were masked;

"(E) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were openly included; and

"(F) the total number of disseminated intelligence reports derived from collection not authorized by this Act containing the identities of United States persons in which the identities of the United States persons were openly included;

"(12) the number of queries conducted in an effort to find communications or information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information, where such communications or information were obtained without a court order, subpoena, or other legal process established by statute;

"(13) the number of criminal proceedings in which the Federal Government or a government of a State or political subdivision thereof entered into evidence or otherwise used or disclosed in a criminal proceeding any information ob-

tained or derived from an acquisition conducted without a court order, subpoena, or other legal process established by statute; and

"(14) a good faith estimate of what percentage of the communications that are subject to the procedures described in section 309(b)(3) of the Intelligence Authorization Act for Fiscal Year 2015 (50 U.S.C. 1813(b)(3))—

"(A) are retained for longer than 5 years; and

"(B) are retained for longer than 5 years in whole in part because they are encrypted.".

(b) REPEAL OF NONAPPLICABILITY TO FEDERAL BUREAU OF INVESTIGATION OF CERTAIN REQUIREMENTS.—Subsection (d) of such section is amended—

(1) by striking paragraph (2); and

(2) by redesignating paragraph (3) as paragraph (2).

(c) CONFORMING AMENDMENT.—Subsection (d)(1) of such section is amended by striking "paragraphs (3), (5), or (6)" and inserting "paragraph (6), (8), or (9)".

SEC. 26. QUARTERLY REPORT .

Section 707 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881f) is amended by adding at the end the following:

"(c) QUARTERLY REPORT.—The Attorney General, in consultation with the Director of National Intelligence, shall submit a report, each quarter, to the congressional intelligence committees and to the Committees on the Judiciary of the Senate and of the House of Representatives, which shall include, for that quarter, the following:

"(1) The total number of warrants issued to conduct a query of information acquired under section 702.

"(2) The total number of times a query was conducted pursuant to an exception under section 702(f)(2)(B) and which exceptions applied.

"(3) The total number of queries of information acquired under section 702 that were conducted using a United States person query term or a query term pertaining to a person reasonably believed to be present in the United States as of the date such query was conducted, disaggregated by the agency that conducted the queries.".

Purpose and Summary

H.R. 6570, introduced by Rep. Andy Biggs (R–AZ), reauthorizes Section 702 of the Foreign Intelligence Surveillance Act (FISA) for three years with significant reforms. It requires the government to obtain an order from the Foreign Intelligence Surveillance Court (FISC) or a warrant prior to conducting U.S. person queries of information collected through Section 702. It provides for greater scrutiny of applications submitted to the FISC, increases transparency in surveillance applications, requires more frequent and detailed reports and audits, and establishes additional penalties for government employees who violate FISA or mislead the FISC.

The bill also closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant. If the agency were to gather this information itself, it would be required to obtain a warrant, subpoena, or other legal order. By closing this loophole, the bill prevents government agencies from conducting an end-run around the protections of the Fourth Amendment.

Background and Need for the Legislation

A. BACKGROUND

i. History and Overview of the Foreign Intelligence Surveillance Act

In 1978, Congress enacted FISA in response to revelations that the federal government had seriously abused warrantless surveillance, resulting in rampant privacy violations.[1] FISA provides a

[1] S. Rep. No. 94–755 (1976) (Book II, Intelligence Activities and the Rights of Americans).

statutory framework for government agencies to conduct surveillance for foreign intelligence purposes through electronic surveillance, physical searches, pen registers and trap and trace devices, or the production of certain business records.[2] FISA also established the FISC to provide judicial oversight of government applications to conduct electronic surveillance, physical searches, and other forms of investigative actions for foreign intelligence purposes.[3]

Subsequent legislation expanded federal statutes involving foreign intelligence gathering. After the September 11, 2001, terrorist attacks, Congress enacted the USA PATRIOT Act to "provid[e] enhanced legislative tools" to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities."[4] The Patriot Act and, later, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[5] further amended FISA. Specifically, section 206 of the Patriot Act permitted roving wiretaps[6] and Section 6001(a) of IRTPA permitted the targeting of non-U.S. persons who are shown to be engaged in international terrorism without requiring evidence connecting those persons to a foreign power or terrorist group (lone-wolf provision).[7]

Section 215 of the Patriot Act enlarged the scope of FISA's business records provision so that the government could request "any tangible thing" about a U.S. person based on a showing that "there are reasonable grounds to believe" that those records are "relevant" to an "authorized investigation" into "international terrorist or clandestine intelligence activities."[8] This section also authorized the bulk collection of telephone metadata. In 2015, however, Congress passed the USA FREEDOM Act to reform intelligence gathering programs in the wake of Edward Snowden's disclosures.[9] The Act prohibited the bulk collection of records under Section 215 of the Patriot Act, thus narrowing Section 215's FISA authorities.[10]

In 2008, Congress enacted FISA Section 702, which allows the government to acquire foreign intelligence by targeting non-U.S. persons who are reasonably believed to be outside of the United States, for the purpose of obtaining foreign intelligence information.[11] More details about Section 702 are below.

In 2018, Congress enacted the FISA Amendments Reauthorization Act of 2017 into law, which extended Section 702 through December 31, 2023.[12] The bill required the FBI to seek a warrant when conducting queries during the "predicative" stage of an investigation but allowed the warrantless queries under Section 702 to

---

[2] *See The Foreign Intelligence Surveillance Act of 1978*, Bureau of Justice Assistance U.S. Department of Justice, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286#:~:text=FISA%20was%20initially%20enacted%20in,collection%20of%20foreign%20intelligence%20information (last visited Apr. 12, 2023).

[3] *See id*.

[4] H.R. REP. NO. 107–236, at 41 (2001).

[5] Pub. L. No. 108–458 (2004).

[6] *See* Pub. L. No. 107–56 (2001).

[7] Pub. L. No. 108–458 (2004).

[8] *See* Pub. L. No. 107–56 (2001).

[9] Pub. L. No. 114–23 (2015).

[10] *See H.R. 2048, the USA Freedom Act*, H. Comm. on the Judiciary, available at https://judiciary.house.gov/usa-freedom-act (last visited Dec. 3, 2023).

[11] 50 U.S.C. § 1881a(a), (b)(3).

[12] Pub. L. No. 115–118, 132 Stat. 3 (2018).

continue in other situations.[13] Prior to 2018, Congress last reauthorized Section 702 in 2012.[14]

In 2020, Section 215 of the Patriot Act, along with the lone wolf provision and the roving wiretap provision, expired.[15] However, some of the provisions remained in effect due to a sunset clause that authorized the continued effect of the amendments regarding investigations that started, or potential offenses that took place, prior to the provisions' sunset date.[16]

a. FISA Title I

Title I of FISA established the procedures for the government to conduct foreign intelligence surveillance and established the FISC.[17] Under Title I, the government may apply to the FISC for an order authorizing the government to conduct electronic surveillance against a particular target.[18] In applying for an order, the government must demonstrate probable cause to believe that the target is a foreign power or an agent of a foreign power.[19]

The FISC sits in Washington, D.C., and is composed of 11 district court judges selected by the Chief Justice of the United States from at least seven of the judicial circuits, and three of the judges must reside within 20 miles of the District of Columbia.[20] Typically, judges sit on the court for one week at a time on a rotational basis.[21] The presiding judge of the FISC is selected by the Chief Justice.[22] These judges are eligible to serve one term of seven years.[23]

The FISC is tasked with authorizing the government's surveillance applications.[24] Proceedings before the court are generally *ex parte*, meaning only the government is represented. In 2015, Congress amended FISA to authorize the FISC to appoint five amici curiae to assist with review of applications or to interpret the law or provide guidance on novel issues.[25] In his review of the FISA program, Department of Justice Inspector General Michael Horowitz highlighted the concerns many have with the FISC:

> FISC proceedings are ex parte, meaning that unlike most court proceedings, the government is present but the government's counterparty is not, and FISA orders generally are not subject to scrutiny through subsequent adversarial proceedings. As a result, the FBI and [DOJ's Na-

---

[13] *See* Martin Matishak and Cory Bennett, *Surveillance bill heads to Trump's desk*, Politico (Jan. 18, 2018), https://www.politico.com/story/2018/01/18/fisa-bill-senate-pass-trump-293130. The "predicative" stage is the last stage before the FBI begins a formal investigation. Prior to this stage, the FBI can query communications without seeking a warrant as they build cases in non-security matters.

[14] P.L. 112–238 (Dec. 2012).

[15] *See* India McKinney, *Section 215 Expired: Year in Review 2020*, Electronic Frontier Foundation (Dec. 29, 2020), https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020.

[16] *Id.*

[17] *The Foreign Intelligence Surveillance Act of 1978 (FISC)*, Bureau of Justice Assistance Department of Justice, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 (last visited Apr. 15, 2023).

[18] 50 U.S.C. § 1804.

[19] *Id.* at § 1805.

[20] Andrew Nolan and Richard M. Thompson II, *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes* at 3, CONG. RESEARCH SERVICE, (Aug. 26, 2014).

[21] *Id.*

[22] *Id.*

[23] United States Foreign Intelligence Surveillance Court, *About the Foreign Intelligence Surveillance Court* (last visited May 30, 2021).

[24] *Id.*

[25] 50 U.S.C. § 1803(i)(2).

> tional Security Division] FISA application process is critical to ensuring that DOJ officials asked to authorize FISA applications, and judges on the FISC asked to approve them, have a complete and accurate set of facts in the FISA application on which they can rely.[26]

Because of the secretive nature of FISC proceedings, it is vital that the intelligence community comply with its own procedures for surveillance and provide the FISC with all necessary information needed to issue orders. However, as evidenced by Inspector General Horowitz's investigation and audit of the FBI's use of its FISA authorities, as well as Special Counsel John Durham's investigation of the FBI's surveillance of Carter Page, it is clear that the FBI has failed to consistently comply with these procedures and that the FISC is in need of reform.

b. FISA Section 702

Congress enacted Section 702 of FISA in 2008 as part of the FISA Amendments Act.[27] Section 702 provides an alternative to the surveillance requirements of Title I of FISA. Title VII of FISA (which includes Section 702) generally addresses electronic surveillance directed at targets outside the United States.[28] Section 702 may only be used to target:

(1) non-U.S. persons;

(2) who are reasonably believed to be outside of the United States;

(3) for the purpose of obtaining foreign intelligence information.[29]

The statute only permits the acquisition of information "from or with the assistance of an electronic communications service provider."[30] The FISC supervises such surveillance by approving certifications submitted jointly by the Attorney General and the Director of National Intelligence (DNI), ensuring that the surveillance complies with the statutory requirements of Section 702.[31] The certification must detail the targeting procedures, minimization procedures, and querying procedures that the government intends to use in its surveillance.[32] But unlike orders under Title I of FISA, the statute does not require the FISC to make probable cause determinations as to individual surveillance targets.[33] Rather, the court reviews and certifies the Attorney General and DNI's targeting procedures to ensure they are properly limited, with such authorizations effective for one year.[34]

1. Communications Collection

Once the FISC approves targeting procedures, the government has various ways to conduct surveillance and collect communica-

---

[26] U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at i (2021).

[27] Pub. L. 110–261 (2008).

[28] *See* EDWARD C. LIU, CONG. RESEARCH SERV., R47477, REAUTHORIZATION OF TITLE VII OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2023).

[29] 50 U.S.C. § 1881a(a), (b)(3).

[30] *Id.* § 1881a(h)(2)(A)(vi).

[31] *Id.* § 1881a(j)(1)(A).

[32] *Id.*

[33] *Id.* § 1881a(j)(2).

[34] *Id.* § 1881a(a), (h)(1)(A).

tions. These methods include downstream collection, upstream collection, and about collection.

In downstream collection, the government may direct a communications service provider (internet service provider, telephone provider, or email provider) to provide all communications to or from a selector, such as an email address, associated with a Section 702 target.[35] In upstream collection, the government directs its requests to telecommunications "backbone" providers, such as companies that operate internet cables.[36]

About, or abouts, collection has been the subject of controversy over the years. About collection involves the government capturing vast amounts of communications in which the selector (e.g., email address) of a target appeared somewhere in communications, even when the target is not a party to the communication.[37] A declassified FISC opinion shed light on this type of collection, noting that it resulted in the collection of "tens of thousands of wholly domestic communications each year" by the National Security Agency (NSA).[38] In 2017, the NSA announced that it was no longer performing "about" collection and in 2018 Congress amended Title VII to prohibit "about" collection unless the Attorney General and DNI notify the House and Senate Judiciary and Intelligence Committees that the NSA plans to resume such collection.[39] While the NSA is not currently performing this type of collection, it is free to resume it at any time, provided it notifies Congress.

2. Minimization Procedures

Under Section 702, the government is required to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning nonconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[40] For example, if the government collects communications discussing or mentioning a U.S. person, but it contains no foreign intelligence information, it must be deleted as soon as practicable but no later than five years from the Section 702 authorization's expiration subject to certain exceptions.[41]

3. Querying Procedures

Much of the controversy surrounding Section 702 involves the government's querying of Section 702-acquired communications already in the government's possession, nearly always without first obtaining a warrant. While the government is required to minimize the sharing and retention of U.S. person information and communications, the NSA "routinely shares raw Section 702 data" with the other intelligence agencies.[42] Each of the intelligence agencies

---

[35] *See* Liu, *supra* note 28 at 10–11.

[36] *Id.* at 11.

[37] *Id.* (citing PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 37 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf).

[38] Redacted, 2011 WL 10945618, at *15 (FISA Ct. Oct. 3, 2011).

[39] *See* Liu, *supra* note 28 at 12 (citing 50 U.S.C. § 1881a(b)(5)).

[40] *Id.* (citing 50 U.S.C. § 1801(h)).

[41] *Id.*

[42] Elizabeth Goitein, *The Year of Section 702 Reform, Part I: Backdoor Searches*, Just Security (Feb. 13, 2023), https://www.justsecurity.org/85068/the-year-of-section-702-reform-part-i-backdoor-searches/ (citing ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE, SEMI-

that have access to Section 702-acquired information—the FBI, CIA, National Counterterrorism Center (NCTC), and the NSA—establish procedures that govern how they may query such information.[43] While these agencies are required to establish procedures to limit the number of Americans affected, the amount of information available to the government is significant. According to the Privacy and Civil Liberties Oversight Board (PCLOB), an independent federal agency established to uphold civil liberties with respect to terrorism-related policies, "[a]part from communications acquired by mistake, U.S. persons" communications are not typically purged or eliminated from agency databases, even when they do not contain foreign intelligence information, until the data is aged off in accordance with retention limits."[44]

Members of Congress and privacy and civil liberties advocates have raised concerns about the querying of Section 702 data for Americans' communications as a "backdoor search." Critics disparage the tactic as an end-run around of the warrant requirement because "backdoor searches" purport to be carried out for foreign intelligence purposes while actually seeking information on Americans without a court order.[45] For example, the FBI is able to query information in most circumstances without a court's approval.[46] In a small subset of cases, the FBI is required to obtain an order from FISC authorizing a query of Section 702 communications if the query is unrelated to national security, known as "evidence of a crime only" queries. Yet in 2022, the FBI only ran such queries 16 times.[47] The FBI may conduct the vast majority of its queries without obtaining an order as long as the query is done to obtain foreign intelligence information or to pursue investigations related to national security.[48]

ii. Justice Department Office of Inspector General Audits of FISA

The Justice Department Office of Inspector General (OIG) has issued numerous reports documenting the FBI's mishandling of surveillance authorities. These reports largely focused on the FBI's misuse of Title I of FISA, whereby the government may apply to the FISC for an order authorizing the government to conduct electronic surveillance against a particular target.[49] In 2001, the FBI adopted the "Woods Procedures," following concerns raised by the FISC about inaccuracies in FISA applications.[50] The Woods Procedures mandate compiling supporting documentation for each fact in the FISA application. This FBI policy requires that a FISA application include a sub-file that contains: (1) supporting documentation for every factual assertion contained in a FISA applications, and (2)

ANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Sep. 2021)).

[43] *See* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 8 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541094125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf.

[44] *See id.* at 8.

[45] *See* Goitein, *supra* note 42.

[46] *See* Liu, *supra* note 28 at 13.

[47] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 27 (2023).

[48] *See Id*.

[49] 50 U.S.C. § 1804.

[50] *See* 2021 DOJ OIG Audit, *supra* note 26 at i.

supporting documentation and the results of required database searches and other verifications.[51]

In December 2019, the OIG issued a 478-page report finding that the FBI had abused its FISA authority to unlawfully surveil former Trump campaign associate Carter Page.[52] The report found 17 significant "errors or omissions'" and 51 wrong or unsupported factual assertions in the applications to surveil Page.[53] The OIG also found that the FBI downplayed the significance of the Democratic National Committee-financed opposition research document prepared by Christopher Steele (the "Steele Dossier") in the applications.[54] Per the report, the FBI cherry-picked facts to support its application, ignored exculpatory evidence, and fabricated evidence presented to a FISC judge to support its surveillance against Page.[55] This led the Justice Department to later admit that "there was insufficient predication to establish probable cause to believe that [Carter] Page was acting as an agent of a foreign power."[56]

During the 116th Congress, on February 5, 2020, FBI Director Christopher Wray testified before the House Committee on the Judiciary. During the hearing, Director Wray indicated that the FBI was taking the FISA abuses seriously and working to address them.[57] At the hearing, Director Wray testified that Americans should not "lose any sleep over" the "vast majority" of FISA applications.[58] This followed testimony from former FBI Director James Comey during a transcribed interview with the Committee in December 2018, when he heralded the FBI's FISA operations as a "labor-intensive and supervision heavy" process with an emphasis on high standards.[59] Comey labeled it a "top tier" FBI program.[60] The OIG's findings undercut the FBI's former and current leaderships' stated confidence in the FISA process.

Shortly after Director Wray's testimony, as a result of the OIG's findings in 2019, the OIG conducted further analysis of the FBI's FISA processes, releasing a management advisory in March 2020.[61] The management advisory detailed the FBI's extensive noncompliance with Woods Procedures. The OIG wrote that it "do[es] not

---

[51] *See* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at 3 (Mar. 30, 2020).

[52] U.S. DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019).

[53] *Id.* at viii & xiii.

[54] *Id.* at vi.

[55] *Id.* at xi.

[56] *In re Carter W. Page*, Nos. 16–1182, 17–52, 17–375, 17–679 (FISC Jan. 7, 2020).

[57] *Oversight of the Federal Bureau of Investigation, hearing before the H. Comm. on Judiciary, 116th Cong.* (Feb. 5, 2020).

[58] *Id.* ("And the thing I would say whenever we talk about anything with FISA, when you use phrases like 'every single time,' is that it's important for the American people to understand, for this committee to understand that the vast majority of the FISAs that we do, both the initial applications and renewals, are the kinds of applications that I am quite confidence—we don't know each other, but I'm quite confident you wouldn't lose any sleep over. And we really wouldn't want to grind things to a halt on that front.").

[59] James Comey Transcribed Interview 145 (Dec. 17, 2018) ("And if you know the FISA process, you know how high the standards are."); *id.* at 147 ("It's one of the things that is the most labor-intensive and supervision heavy that the FBI does. There are some things I can think of that are also very, very carefully scrubbed, but it's one of that top tier.").

[60] *Id.*. The OIG previously found that Comey made one "unauthorized disclosure of sensitive investigative information" involving President Trump, specifically in the hopes of "achiev[ing] a personally desired outcome"—the appointment of Special Counsel Robert Mueller.

[61] *See* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at 3 (Mar. 30, 2020).

have confidence that the FBI has executed its Woods Procedures in compliance with FBI Policy, or that the process is working as it was intended to help achieve the 'scrupulously accurate' standard for FISA applications."[62] Of the 29 surveillance applications on U.S. persons that the OIG sought to examine, the FBI was unable to even locate the Woods Files for four applications.[63] There was unsupported, uncorroborated, or inconsistent information in the Woods Files of all of the remaining 25 applications reviewed.[64] The OIG "identified an average of about 20 issues per application reviewed."[65]

In September 2021, the OIG issued a more detailed report confirming its initial finding of widespread FBI non-compliance with the Woods Procedures.[66] The OIG noted that "certain public statements from the FBI . . . in 2020 failed to recognize the significant risks posed by systemic non-compliance with the Woods Procedures, and during our audit some FBI field personnel minimized the significance of Woods Procedures non-compliance."[67] In conducting an accuracy review of the 29 FISA applications, the OIG found over 400 instances of non-compliance with the Woods Procedures.[68] Of the more than 7,000 FISA applications from January 2015 through March 2020, there were 179 instances of missing, destroyed, or incomplete Woods Files, in addition to the four discovered in the March 2020 review.[69]

iii. Special Counsel John Durham Report

On May 12, 2023, Special Counsel John Durham issued his report investigating the intelligence activities and investigations arising out of the 2016 presidential campaigns, namely, the FBI's Crossfire Hurricane investigation. As did the OIG, Special Counsel Durham reviewed the FBI's use of its FISA authorities to surveil Carter Page. And, like the OIG, the Special Counsel's report identified significant abuses of the FBI's FISA authorities.

The Special Counsel's report found that the FBI's FISA applications to surveil Trump campaign associate Carter Page were based almost entirely on the debunked allegations in the Steele dossier.[70] The information relied largely on subsources, none of whom the FBI interviewed could corroborate any of the information in the Steele dossier.[71] For example, the FBI never interviewed Charles Dolan, likely the source of several of the allegations.[72] Despite the lack of evidence, two days after receiving Steele dossier information, the FBI incorporated the information into its Page FISA application.[73] Some FBI agents even expressed concern over the reli-

---

[62] *Id.* at 8.
[63] *Id.* at 7.
[64] *Id.*
[65] *Id.*
[66] U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS (2021).
[67] *Id.* at ii.
[68] *Id.* at 7.
[69] *Id.*
[70] Office of Special Counsel John H. Durham, *Report on Matters Related to Intelligence Activities and Investigations Arising out of the 2016 Presidential Campaigns,* U.S. Dep't of Justice at 117, 134 [hereinafter: "Special Counsel's Report"].
[71] *Id.* at 228.
[72] *Id.* at 172.
[73] *Id.* at 117.

ability of the information but were pressured by FBI leadership to open a full investigation.[74] As it pressed forward with the investigation, the FBI used confidential human sources to obtain more information, but mischaracterized and misstated intelligence gathered by the sources, errors that were included in all three renewal FISA applications.[75] Ultimately, Carter Page was subjected to unlawful surveillance for eleven months.[76]

iv. Abuses of FISA Section 702

While the Justice Department OIG and Special Counsel Durham have thoroughly detailed abuses and deficiencies in FISA Title I applications, there are separate, significant concerns related to Section 702, particularly with querying procedures. Despite the statute's limitation of surveillance to foreign nationals, "Section 702 has become a rich source of warrantless government access to Americans" phone calls, texts, and emails."[77] That is because rather than minimizing the sharing and retention of Americans' data, "the NSA routinely shares such data with the FBI, CIA, and National Counterterrorism Center, and all agencies retain it for at least five years."[78] While the government may not intentionally acquire communications from senders or recipients that are located in the United States,[79] it frequently "incidentally" acquires this information.[80] Section 702 permits the government to target foreigners abroad in search of "foreign intelligence information," which is interpreted broadly and often has no nexus to national security.[81]

In 2014, the Privacy and Civil Liberties Oversight Board (PCLOB) issued a comprehensive unclassified report of the Section 702 program.[82] The 2014 report issued 12 recommendations and noted the privacy risks inherent in this surveillance program due to the large scope of "incidental" collection of U.S. persons communications, the use of "about" collection, and the use of queries to search the communications of specific U.S. persons.[83]

The FBI, NSA, CIA, and NCTC are all authorized to query Section 702-acquired content for foreign intelligence information.[84] But only the FBI is authorized to conduct queries that are reasonably likely to return evidence of a crime.[85] Because of this, the FBI conducts U.S. person queries at a higher rate than other intelligence agencies.[86] In January 2023, the PCLOB hosted a public forum to discuss the potential reauthorization of FISA Section 702 and high-

---

[74] *Id.* at 102.
[75] *Id.* at 208–09, 212.
[76] U.S. DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION at vi (2019).
[77] *Section 702 of FISA: A "Foreign Intelligence" Law Turned Domestic Spying Tool*, The Brennan Center for Justice (Feb. 2, 2023), https://www.brennancenter.org/our-work/research-reports/coalition-document-proposes-reforms-section-702.
[78] *Id.*
[79] 50 U.S.C. § 1881a(b).
[80] *See Warrantless Surveillance Under Section 702 of FISA,* ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa (last visited Apr. 17, 2023).
[81] *Id.*
[82] *See* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014).
[83] *Id.* at 93, 111, 123, 134.
[84] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2021 at 19 (2022).
[85] *Id.*
[86] *Id.* at 20.

light issues with the program and the need for reform.[87] In her testimony at this forum, Cindy Cohn, Executive Director of the Electronic Frontier Foundation, noted that one of the major concerns with Section 702 is the fact that the "fruits of this surveillance don't just stay with the NSA . . . [they] stretch over to the FBI which means they are available for prosecution and indeed have been used for prosecution."[88] These use cases raise questions about whether a tool designed for foreign intelligence gathering has been transformed into a weapon for the FBI to use in its domestic law enforcement mission capacity.

In October 2023, the PCLOB issued a new report, calling for various legislative and internal changes to the Section 702 program.[89] While stating that "Section 702 remains highly valuable to protect national security," the PCLOB also found that the program "creates serious privacy and civil liberties risks."[90] To address these issues, the PCLOB made 19 legislative and administrative recommendations, most notably a requirement that the FISC review and authorize U.S. person queries.[91] Other recommendations include a prohibition on "abouts" collection, further reporting and transparency measures, additional audits of the Section 702 program, and more robust amici authority in the FISC.[92]

a. Constitutional Concerns with Warrantless Searches

The FBI's use of Section 702 certainly implicates the privacy and civil liberties of Americans, but it also may violate the Fourth Amendment to the Constitution. The FISC has repeatedly held that queries of Section 702-acquired information do not violate the Fourth Amendment, stating that the "targeting, minimization, and querying procedures, as written, are consistent with the requirements of the Fourth Amendment" and "adequately guard against error and abuse."[93]

The FISC's view of the constitutionality of such searches has been challenged in the past, however. Following the enactment of new querying provisions in the FISA Amendments Reauthorization Act of 2017, amici argued that the FISC "should regard queries as distinct Fourth Amendment searches."[94] The FISC declined to do so, stating that although Congress believed that "Fourth Amendment concerns are implicated by Section 702 queries," the FISC determined that the law expanded statutory protections, but not the scope of what constitutes an unlawful search under the Fourth Amendment.[95]

In contrast, in 2019, the U.S. Court of Appeals for the Second Circuit held that Section 702 queries do implicate the Fourth Amendment and found that each query should be regarded as "a separate Fourth Amendment event that, in itself, must be reason-

---

[87] U.S. Privacy and Civil Liberties Oversight Board, *PCLOB Public Forum on FISA Section 702*, YOUTUBE (Jan. 12, 2023), https://www.youtube.com/watch?v=AZvaimMTqio.
[88] *Id.* at min. 1:34:50.
[89] *See* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2023).
[90] *Id.* at 7.
[91] *Id.* at 205–08.
[92] *See generally id.* at 208–25.
[93] *See* Memorandum Opinion and Order, *Document re: Section 702 2021 Certification* at 66 (FISA Ct. Apr. 21, 2022).
[94] *Id.* at 63.
[95] *Id.* (citing Memorandum Opinion and Order at 87 (FISA Ct. Oct. 18, 2018)).

able."[96] The Court raised concerns about the ability to query such a vast trove of communications, stating that permitting:

> that information to be accessed indiscriminately, for domestic law enforcement purposes, without any reason to believe that the individual is involved in any criminal activity and or even that any information about the person is likely to be in the database, just to see if there is anything incriminating in any conversations that might happen to be there, would be at odds with the bedrock Fourth Amendment concept that law enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search.[97]

The Second Circuit's decision takes into account technological changes and the vast amount of information that is collected under Section 702 and raises questions about whether such "backdoor searches" are constitutional.[98] The court explained that "[t]hat concern is compounded by the hundreds of thousands of searches done by the government's aggregate querying of Section 702, representing a massive violation of Americans' privacy."[99] Although the FISC disagreed with the Second Circuit in its 2022 opinion, the FBI's continued violations of its Section 702 authorities raise concerns that it is violating the Fourth Amendment. As Congress considers reforms to Section 702, it cannot rely on the FBI to enact internal changes and police itself. Despite claims of change and improvement, the FBI has consistently violated its Section 702 authorities and Congress must act to protect the constitutional rights of Americans.

b. ODNI Annual Statistical Transparency Report

According to the Office of the Director for National Intelligence (ODNI), the FBI has misused FISA-collected information to surveil Americans without a warrant.[100] In 2021, ODNI data revealed that the FBI conducted an estimated 3,394,053 U.S. person queries[101] and in 2022 the FBI conducted 204,090 searches, or roughly 559 per day.[102]

In its 2022 annual statistical transparency report, ODNI noted that the FBI updated its counting methodology to allow it to identify the number of unique U.S. person query terms, rather than just the total number of queries, as it had done in the past.[103] This methodology eliminates duplicate queries and is more in line with the methods of other intelligence community elements.[104] Based on the "de-duplicated" counting methodology, the FBI reports that it conducted 119,383 U.S. person queries in 2022 compared to a de-

---

[96] *United States v. Hasbajrami*, 945 F.3d 641, 672 (2d Cir. 2019).
[97] *Id.* at 672.
[98] *See* Andrew Crocker, *The Foreign Intelligence Surveillance Court Has Made a Mockery of the Constitutional Right to Privacy,* Electronic Frontier Foundation (June 1, 2023), https://www.eff.org/deeplinks/2023/06/foreign-intelligence-surveillance-court-has-made-mockery-constitutional-right.
[99] *Id.*
[100] *See generally* 2021 ODNI Annual Statistical Transparency Report, *supra* note 84.
[101] *Id.* at 4, 21.
[102] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 24 (2023).
[103] *Id.* at 23.
[104] *Id.*

duplicated number of 2,964,643 in 2021 (as opposed to 204,090 queries and 3,394,053 queries, respectively).[105] Even with an updated counting methodology, such a precipitous drop—over 95% lower—does raise questions as to the efficacy of the program and should garner scrutiny to ensure the method is being applied with integrity. And though this counting method is consistent with those used by the CIA, NSA, and NCTC, it is not perfect. For example, when the FBI uses a U.S. person identifier to query unminimized Section 702-acquired information, that will now be counted as a single query term, regardless how many times the FBI uses that term.[106]

In recent years, Congress and the FISC have sought to impose limits on these backdoor searches. Those proposals include requiring the FBI to show probable cause and obtain an order from the FISC for queries in "predicated criminal investigations that do[ ] not relate to the national security of the United States."[107] However, because the FBI often runs queries before an investigation is predicated, this requirement is rarely triggered.[108] Even when such a requirement is triggered, as it has been approximately 100 times since 2018, the FBI rarely complies.[109] For the vast majority of cases, the only limitation is the requirement that U.S. person queries must be reasonably likely to return foreign intelligence or evidence of a crime—a low bar.[110]

c. ODNI Semiannual Report

Analysis of Section 702 in recent years reveals the extent of the problem of this type of warrantless surveillance. The Justice Department and ODNI released an unclassified copy of their 24th semiannual assessment of FISA Section 702 in December 2022.[111] The report details issues ranging from conducting queries unlikely to return foreign intelligence information, evidence of ordinary criminal activity, and conducting overly broad queries. Recently, Congressman Darin Lahood (R–IL) revealed that he was likely subjected to wrongful FISA queries multiple times.[112] The semiannual report determined this search was improper, as the FBI conducted a query using only the Congressman's name, with no limiters, potentially returning troves of sensitive communications.[113]

Additionally, the FBI is also using Section 702 to search the communications of everyday Americans. The 24th semiannual report also uncovered information about the FBI's queries of individuals who had requested to participate in the FBI's "Citizens Academy," individuals who came to an FBI field office to conduct repairs, and individuals who entered a field office to provide a tip or to report

---

[105] *Id.* at 24.
[106] *Id.* at 25.
[107] *See* 50 U.S.C. § 1881a(f)(2); *see also* Goitein, *supra* note 42.
[108] *See* Goitein, *supra* note 42.
[109] *Id.* (citing OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2021 at 19 (2022)).
[110] *Id.*
[111] DEPARTMENT OF JUSTICE AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (December 2021). This report covers the timeframe of December 1, 2019 through May 31, 2020.
[112] *See* Charlie Savage, *Lawmaker Says He Was Target of F.B.I. Surveillance Material Searches,* THE NEW YORK TIMES (March 9, 2023).
[113] *See* 24th DOJ–ODNI Semiannual Assessment, *supra* note 111 at 58 fn. 92.

that they were the victim of a crime.[114] The FBI also queried the names of a local political party to determine if it had any connections to foreign intelligence; the report found that this query "was not reasonably likely to achieve foreign intelligence information." [115] The FBI has also searched for the communications of journalists, college students participating in a "Collegiate Academy," police officer candidates, and colleagues and relatives of the FBI agent performing the search, among others.[116]

In 2023, the Justice Department and ODNI released unclassified copies of their 25th and 26th semiannual assessments, covering June 1, 2020, through November 30, 2020, and December 1, 2020, through May 31, 2021, respectively. While the number of querying incidents declined from the previous reporting periods, the reports still showed querying violations. For example, the 25th semiannual assessment identified querying violations as a result of FBI personnel conducting overly broad queries, queries unlikely to return foreign intelligence information, or being unaware that a query would be run against FISA-acquired information.[117] FBI personnel also conducted U.S. person queries to research prospective law enforcement personnel.[118] Similarly, while the 26th semiannual assessment showed a decrease in querying compliance incidents, FBI personnel violated the querying standards on various occasions, such as by failing to properly document the justification for a query or improperly conducting batch queries.[119]

d. FISC Opinions

On May 19, 2023, the ODNI released two unclassified FISC opinions, including the 2021 FISA Section 702 Certifications and Targeting, Minimization, and Querying Procedures opinion, initially issued in April 2022.[120] This opinion included results from the Justice Department's National Security Division (NSD) audit and the FBI's Office of Internal Auditing audit of query compliance generally between 2020 and 2021. While the Justice Department and FBI have continually told Congress and the FISC that it is making changes to its querying procedures, the FISC opinion demonstrates continued querying violations.

For example, according to the opinion, FBI agents ran a batch query of unminimized FISA information in June 2020, using identifiers of over 100 individuals in connections with the George Floyd protests without "any specific potential connections to terrorist related activity" known to the FBI.[121] The Justice Department's NSD assessed that those searches were unlikely to return foreign intelligence information or evidence of a crime.[122] Additionally, multiple

---

[114] *Id.* at 58.
[115] *Id.*
[116] *See Section 702 of FISA: A "Foreign Intelligence" Law Turned Domestic Spying Tool,* The Brennan Center for Justice (Feb. 2, 2023), https://www.brennancenter.org/our-work/research-reports/coalition-document-proposes-reforms-section-702.
[117] DEPARTMENT OF JUSTICE AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT at 55–56 (April 2022).
[118] *Id.* at 56.
[119] DEPARTMENT OF JUSTICE AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT at 55–57 (August 2022).
[120] *See* Memorandum Opinion and Order, *Document re: Section 702 2021 Certification* (FISA Ct. Apr. 21, 2022).
[121] *Id.* at 27 (internal quotations omitted).
[122] *Id.*

FBI agents ran queries against unminimized information of individuals suspected of involvement in the events that occurred at the Capitol on January 6, 2021.[123] This included a query of "thousands of names within FBI systems in relation to the Capitol breach investigation," including running thirteen names against unminimized data in order to determine if any individuals had foreign ties.[124] Another agent conducted 360 queries in connection with drug investigations, domestic terrorism investigations, and January 6, 2021, without providing any information to support a reasonable belief that the query would return foreign intelligence information or evidence of a crime.[125]

Reports also revealed the FBI conducted a batch query for over 19,000 donors to a congressional campaign in an attempt to determine if it was a target of foreign influence, and the NSD determined that only eight of the identifiers used had a sufficient connection to foreign influence activities to justify such a search.[126] In total, the FBI conducted more than 278,000 improper searches of U.S. persons' communications, including information acquired pursuant to Section 702.[127]

Despite the FBI's claims that its internal remedial measures have resulted in increased compliance, the FISC's 2023 FISA Section 702 Certifications and Targeting, Minimization, and Querying Procedures opinion identified further violations. For example, the FBI conducted various queries without receiving Deputy Director approval before using a "sensitive query term," a violation of the FBI's recently-adopted procedures.[128] In June 2022, an analyst conducted four queries of Section 702 information using the last names of a United States Senator and a state senator based on information that a foreign intelligence service was targeting those individuals.[129] The analyst not only failed to receive requisite approval, but the NSD also determined the querying standard of "reasonably likely to retrieve" foreign intelligence information was not met.[130] Another agent ran a query using the social security number of a state judge who "had complained to the FBI." [131]

e. Use of Section 702 in Court

A significant concern arises when Section 702-acquired information is used against a defendant in court.[132] While the law generally requires the government to notify defendants when information "derived from" FISA Section 702 electronic surveillance is used to investigate them,[133] there are several loopholes the government exploits to avoid this requirement.[134] For example, the Justice Department reportedly relies on a "secret interpretation" of the

---

[123] *Id.* at 28.
[124] *Id.*
[125] *Id.* at 29.
[126] *Id.*
[127] *Id.* at 31.
[128] *See* Memorandum Opinion and Order, *Document re: Section 702 2023 Certification* at 86 (FISA Ct. Jul. 21, 2023).
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *See* Jake Laperruque, *CDT Issue Brief: FISA Section 702 Key Reforms*, Center for Democracy & Technology (Jan. 30, 2023), https://cdt.org/insights/cdt-issue-brief-fisa-section-702-key-reforms/.
[133] 50 U.S.C. § 1806(c), (d).
[134] *See* Laperruque, *supra* note 132.

phrase "derived from," leading it often to determine no notification is required.[135] The government also uses "parallel construction" whereby "government officials are alerted to unlawful activity, but instead of divulging the fact that they received this information from a secret database, they tip off local officials" allowing them to discover information from a different source.[136]

In a 2020 opinion, the FISC sounded the alarm about the FBI's actions in using FISA-acquired data for domestic criminal and other non-intelligence purposes. The court noted the discovery of 40 queries in which the FBI accessed information for investigations involving "health-care fraud, transnational organized crime, violent gangs, domestic terrorism involving racially motivated violent extremists, as well as investigations relating to public corruption and bribery," none of which were "related to national security, and they returned numerous Section 702-acquired products in response."[137]

f. The Need for a Warrant Requirement

Such consistent violations of FISA demonstrate the need to include a warrant requirement for U.S. person queries in any reauthorization of the Act. On July 14, 2023, the Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary held its second hearing of the 118th Congress on the need to reform FISA.[138] There, each witness highlighted the merits of such a warrant requirement.[139] According to one witness, Professor Jonathan Turley, the warrantless searches that have so often occurred under Section 702 "threaten a host of rights including free speech, the free press, freedom of religion, and free association."[140]

Additionally, Elizabeth Goitein, Senior Director of the Liberty and National Security Program at the Brennan Center for Justice at NYU School of Law, testified that "[w]arrantless access to Americans" communications has become a core feature of a surveillance program that purports to be solely foreign-focused."[141] Goitein noted that government officials have defended these back door searches as merely searches of lawfully acquired information, so the agencies "may use the information for any government purpose."[142] In countering this argument, she highlighted that, in the law enforcement context outside of FISA, a warrant is normally required to search the contents of communications and the Supreme Court has held that officers must obtain a warrant to search cell phone data even when the cell phone was lawfully seized without a warrant incident to arrest.[143]

---

[135] *Id*.

[136] *How Rand Paul plans to overhaul FISA surveillance program*, FOXBusiness (Jan. 10, 2018), https://www.foxbusiness.com/politics/how-rand-paul-plans-to-overhaul-fisa-surveillance-program.

[137] Memorandum Opinion and Order, *Document re Section 702 Certification* at 42 (FISA Ct. Nov. 18, 2020).

[138] *Fixing FISA, Part II, Hearing Before the Subcomm. on Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).

[139] *Id*.

[140] *Id*. (Testimony of Professor Jonathan Turley at 1).

[141] *Id*. (Testimony of Elizabeth Goitein at 9).

[142] *Id*.

[143] Id. (Testimony of Elizabeth Goitein at 10 n. 48) (citing *Riley v. California*, 573 U.S. 373 (2014)); *see also id*. at n. 48 (quoting *United States v. Odoni*, 782 F.3d 1226, 1237–38 (11th Cir. 2015) ("We . . . must analyze the search and the seizure separately, keeping in mind that the fact that police have lawfully come into possession of an item does not necessarily mean they are entitled to search that item without a warrant.")).

Goitein's testimony demonstrated that it logically follows that the search of communications acquired under FISA Section 702 should be subject to those same limitations, stating that "[t]he starting point for any reauthorization of Section 702 must be an end to warrantless searches of Americans' 'incidentally' obtained communications."[144] In the same hearing, attorney Gene Schaerr similarly stated that as a condition to reauthorizing Section 702, Congress should require that "government access to Americans' communications or other private data be allowed *only* pursuant to a judicial order, issued under the Fourth Amendment probable cause standard."[145] Such a requirement would "prevent the government from invading Americans' privacy when there is no good reason to do so."[146]

While opponents of a warrant requirement often state that requiring a warrant would prevent the intelligence officials from protecting victims, cybersecurity and civil liberties experts have consistently supported a warrant requirement, noting that such a requirement "is not just feasible, it is also essential to preventing misconduct."[147] Some of the worst surveillance abuses were conducted under the guise of protecting victims, such as the surveillance of Martin Luther King and the recent querying violation of Congressman LaHood.[148] A warrant requirement can coexist with the need to protect victims by, for example, allowing the intelligence community to conduct searches with the consent of the victim.[149] A warrant requirement will help to prevent misconduct by the intelligence community and ensure that the government only conducts a search when it has probable cause "to believe that any harm is being or is about to be inflicted on the Nation or one of its citizens."[150]

g. The Executive Branch's Push for a Clean Reauthorization of Section 702

Despite the clear evidence of abuse, the intelligence community is pushing for a clean reauthorization of Section 702. At the PCLOB public forum in January 2023, General Paul M. Nakasone of U.S. Cyber Command gave the keynote address, urging the reauthorization of FISA Section 702. In this address, he described Section 702 as "one of the most important intelligence legal authorities for addressing U.S. threats" and called the Act "irreplaceable."[151] General Nakasone described Section 702 as an "agile" and "technology-neutral" legal authority in the fight against cybersecurity attacks.[152] He dismissed concerns over privacy violations by citing preventative measures already in place to protect civil liberties, including through annual training, policy controls on when and how

[144] *Id*. (Testimony of Elizabeth Goitein at 23).
[145] *Id*. (Testimony of Gene Schaerr at 2).
[146] *Id*. (Testimony of Gene Schaerr at 3).
[147] Jake Lapperuque and Greg Nojeim, *CDT FISA Issue Brief: A Warrant Rule for US Person Queries Would Not Prevent Victim-Focused Queries*, Center for Democracy & Technology (Oct. 17, 2023), https://cdt.org/insights/cdt-fisa-issue-brief-a-warrant-rule-for-us-person-queries-would-not-prevent-victim-focused-queries/.
[148] *Id*.
[149] *Id*.
[150] *Fixing FISA, Part II, Hearing Before the Subcomm. on Crime and Fed. Gov't Surveillance*, 117th Cong. (2023) (Testimony of Gene Schaerr at 3).
[151] U.S. Privacy and Civil Liberties Oversight Board, *PCLOB Public Forum on FISA Section 702*, YOUTUBE at min. 8:30 (Jan. 12, 2023), https://www.youtube.com/watch?v=AZvaimMTqio.
[152] *Id*. at min. 11:30.

queries are performed, technical controls on access to the data, the self-reporting by agencies, and oversight by all three branches of government.[153]

On February 28, 2023, President Biden's National Security Advisor Jake Sullivan similarly issued a statement calling Section 702 "a cornerstone of U.S. national security," an "invaluable tool that continues to protect Americans every day," and called its reauthorization a "top priority for the Administration."[154] That same day, Attorney General Merrick Garland and Director of National Intelligence Avril Haines sent a letter to congressional leadership urging the reauthorization of Section 702.[155]

On March 1, 2023, Attorney General Garland testified before the United States Senate Committee on the Judiciary, expressing support for the reauthorization of Section 702, noting that the Act "is subject to robust targeting, minimization, and querying procedures to protect the privacy and civil liberties of U.S. persons."[156] On July 12, 2023, FBI Director Christopher Wray testified before the House Committee on the Judiciary, similarly expressing support for Section 702.[157] Specifically, Director Wray expressed concerns about the proposal that the FBI obtain a warrant before conducting queries of U.S. person communications, stating, "A warrant requirement would amount to a *de facto* ban, because query applications either would not meet the legal standard to win court approval" or would cause the FBI to expend vast resources and time that "in the world of rapidly evolving threats, the government often doesn't have."[158] He testified that the FBI's internal measures have improved the FBI's query compliance rate.[159]

The FBI has stated that beginning in the second half of 2021, it has made changes relating to queries of Section 702-acquired information designed to prevent the abuses of recent years.[160] Changes include requiring attorney approval for batch queries of over 100 or more queries, requiring FBI users to affirmatively opt-in to query Section 702-acquired information, updated guidance and training, and enhanced approval requirements for sensitive queries, such as those involving public officials.[161]

These statements and claims of reform ignore the clear abuse that has occurred for years. Whether the result of a misunderstanding of the querying procedures or something more nefarious, queries that involve U.S. persons should raise oversight sensitivi-

---

[153] *Id*. at min. 17:13.

[154] *Statement by National Security Advisor Jake Sullivan on the Biden-Harris Administration's Support for the Reauthorization of Vital Intelligence Collection Authorities*, The White House (Feb. 28, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/28/statement-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-support-for-the-reauthorization-of-vital-intelligence-collection-authorities/.

[155] *See* Letter from Merrick Garland, Attorney General, and Avril Haines, Dir. of Nat. Intelligence, to Charles Schumer, Majority Leader, U.S. Senate, Kevin McCarthy, Speaker, U.S. House of Representatives, Mitch McConnell, Minority Leader, U.S. Senate, and Hakeem Jeffries, Minority Leader, U.S. House of Representatives Minority Leader (Feb. 28, 2023), *available at* https://s3.documentcloud.org/documents/23692331/garland-haines-fisa702-letter.pdf.

[156] *See Oversight of the United States Department of Justice: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. (Mar. 1, 2023) (Testimony of Hon. Merrick Garland, Att'y Gen., U.S. Dep't of Justice, at 8).

[157] *See Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 118th Cong. (Jul. 12, 2023) (Testimony of Hon. Christopher Wray, Dir., Fed. Bureau of Investigation).

[158] *Id.* (Testimony of Hon. Christopher Wray, Dir., Fed. Bureau of Investigation at 13).

[159] *Id.*

[160] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 23 (2023).

[161] *Id.* at 23.

ties. For years, the FBI has claimed to have made improvements to limit the warrantless surveillance of Americans, but abuses continue to be exposed. The intelligence community, and the FBI in particular, is failing to protect the civil rights and liberties of the American people it is entrusted to protect.

v. Electronic Communications Privacy Act

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to limit the government's ability to access digital communications.[162] Under ECPA, the government must seek a warrant or other court order before compelling certain electronic communications services providers to disclose the contents and records of electronic communications. These warrant and order requirements, however, only apply to certain communications services providers.

ECPA prevents a Remote Computing Service (RCS) and an Electronic Communications Service (ECS) provider from knowingly disclosing communications contents to third parties under certain circumstances. An RCS means the "provision to the public of computer storage or processing services by means of an electronic communications system."[163] An ECS means "any service which provides to users thereof the ability to send or receive wire or electronic communications."[164] These include phone companies like AT&T and Verizon, and tech companies like Google, Microsoft, and Facebook.

An ECS provider is prohibited from disclosing to third parties "the contents of a communication while in electronic storage by that service,"[165] while an RCS provider cannot disclose "the contents of any communication which is carried or maintained on that service."[166] Both providers are prohibited from knowingly divulging non-content information to the government absent an exception.[167] The government may obtain subscriber information, like names, addresses, and phone numbers, from an RCS or ECS by issuing a subpoena.[168] It may obtain more sensitive non-content information like traffic or transactional information by obtaining a separate order after demonstrating "specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material to an ongoing criminal investigation."[169] When the government seeks to obtain the content of electronic communications, it must obtain a probable cause warrant.[170]

However, ECPA does not restrict the ability of these electronic services providers from voluntarily providing non-content information to non-government third parties.[171] As long as those third parties are not RCS or ECS providers, then ECPA does not apply to them and does not prohibit their selling the information to the gov-

---

[162] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Center for Democracy & Technology at 15 (2021).
[163] 18 U.S.C. § 2711(2).
[164] 18 U.S.C. § 2510(15).
[165] 18 U.S.C. § 2702(a)(1).
[166] 18 U.S.C. § 2702(a)(2).
[167] *See* 18 U.S.C. § 2702(a)(3), (b).
[168] *See* 18 U.S.C. § 2703(c)(2).
[169] Shenkman, et al. *supra* note 162 at 16; See also 18 U.S.C. § 2703(d).
[170] Shenkman, et al. *supra* note 162 at 16.
[171] *Id.*

ernment.[172] This has led to a loophole whereby RCS and ECS providers can transfer data to private third parties and the government is able to purchase the data from those third parties without obtaining the otherwise required court order, subpoena, or warrant.

At a July 14, 2023, hearing of the Subcommittee on Crime and Federal Government Surveillance, witnesses addressed this data broker loophole.[173] One testified that "the law is woefully outdated. It does not cover digital data brokers or many app developers, for the simple reason that they did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections."[174] Data brokers serve as a "middleman" and allow the government to sidestep the requirements of the Fourth Amendment.[175]

vi. Supreme Court Precedent on Location Data

Over 40 years ago, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[176] The Court has relied on this "third-party doctrine" over the years to find that the Fourth Amendment does not protect records or information voluntarily shared with someone else.[177] In 2018, in *Carpenter v. United States*, however, the Court held "that the Government must generally obtain a warrant supported by probable cause before acquiring" cell-site location information for a seven-day period.[178] Writing for the Court, Chief Justice Roberts highlighted the "seismic shifts in digital technology" that makes tracking a person's location possible.[179] The Court recognized that location information "provides an intimate window into a person's life, revealing not only his particular movements, but through them, his 'familial, political, professional, religious, and sexual associations'."[180]

While the Court's decision in *Carpenter* dealt with cell-site location information, rather than commercially available geolocation data, "the Court's reasoning surrounding the privacy concerns of location data strongly suggest that collection of a multitude of sensitive digital information . . . is also covered by the Fourth Amendment's warrant requirement."[181] However, the government has construed *Carpenter*'s holding as limited to the facts of the case. Indeed, the Court "expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party."[182]

---

[172] *Id.*

[173] *See Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).

[174] *Id.* (Testimony of Elizabeth Goitein at 39).

[175] *Id.*

[176] *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (citing *United States v. Miller*, 425 U.S. 435, 442–44 (1976)).

[177] *See* Amy Howe, *Opinion analysis: Court holds that police will generally need a warrant for sustained cellphone location information*, SCOTUSblog (Jun. 22, 2018), https://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/.

[178] *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).

[179] *Id.* at 2219.

[180] *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415 (Sotomayor, J., concurring)).

[181] Shenkman, et al. *supra* note 162 at 18.

[182] *See Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023) (Testimony of Elizabeth Goitein at 41).

vii. Data Collection, Retention, and Sale

Today, data is often referred to as the world's most valuable resource, even surpassing oil.[183] It can include information from public sources, such as "demographic information, property records, court filings, criminal convictions, professional licenses, census data, birth certificates, marriage licenses, divorce records," bankruptcy records, and voter registration information, among others.[184] Commercially-sourced data may include "purchase history, warranty registration, credit information, employment registration, loyalty card data, membership data, subscriptions, etc." And still yet, even more intimate data can be procured through the collection of information originating from "social media profiles, web browsing activity, mobile apps, media reports, websites, mail-in rebate forms, forum posts, web browser cookies, plugins, addons, device data, IP fingerprints, network data, metadata" and so on.[185]

Data brokers aggregate, package, and sell the data acquired from a variety of sources, including those described above. Often, data brokers have thousands of different data points reflecting information about a person that, when combined, reveal valuable and intimate insights about an individual that would otherwise be unavailable.[186] In other words, for data brokers, consumers and their information are the product. For example, data brokers can receive geolocation data, sometimes accurate to just a few yards, from a mobile device up to 14,000 times per day.[187] This data allows a purchaser to identify patterns that can reveal where a person lives, where they work, and where they spend their free time.[188] This information can be useful in commercial applications, such as advertising.[189] However, it can also be exploited to learn about a person's daily life and to track their historic movements.[190]

As a result of the nature of this information, it is extremely attractive to government agencies, and recent reporting indicates that data-based policing is becoming increasingly prevalent. For example, the Internal Revenue Service (IRS), Drug Enforcement Administration (DEA), FBI, Department of Homeland Security (DHS), and Department of Defense (DOD) have all purchased geolocation information from data brokers.[191] And other experts have found that the practice of law enforcement and intelligence agencies buying sensitive data—ranging from geolocation to personal communications—is increasing, with some agencies spending "tens of millions of dollars on multi-year contracts."[192]

In recent years, the government has turned to data brokers like Venntel to purchase location data from Americans' smartphones.

---

[183] Kiran Bhageshpur, *Data Is The New Oil—And That's A Good Thing*, FORBES (Nov. 15, 2019).

[184] Henrik Twetman, *Gundars Bergmanis-Korats, Data Brokers and Security: Risks and vulnerabilities related to commercially available data*, NATO STRATEGIC COMMC'NS CTRE. OF EXCELLENCE (Jan. 20, 2020).

[185] *Id.*

[186] *What Are Data Brokers—And What Is Your Data Worth?*, WEBFX (Mar. 16, 2020).

[187] Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018).

[188] *See Id.*

[189] *Id.*

[190] *Id.*

[191] Elizabeth Goitein, *The government can't seize your digital data. Except by buying it.*, WASH. POST (Apr. 26, 2021).

[192] Sharon Bradford Franklin, Greg Nojeim & Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021).

The IRS purchased access to a commercial database that "records the locations of millions of American cellphones" to attempt to "identify and track potential criminal suspects."[193] Another data broker, Clearview AI, developed a facial recognition software to create a database of photos from sites like Facebook, LinkedIn, and Twitter and marketed to law enforcement.[194] Because ECPA does not protect consumers from data brokers that collect their information, the government purchases data as a way to avoid seeking a warrant as would otherwise be required by the Fourth Amendment.[195]

This year, the FBI admitted to buying "precise geolocation data derived from mobile-phone advertising."[196] At a hearing before the Senate Select Committee on Intelligence, Director Wray stated that the FBI now seeks court orders when obtaining phone data from commercial vendors, but the data broker loophole in ECPA would permit the FBI to resume purchasing such data in the future.[197] Leaked documents also revealed that Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) purchased cell phone location data, and ICE also purchased utility data and information from private license plate reader databases.[198] Defense contractors reportedly purchased location data from Muslim prayer apps and dating apps.[199] The Secret Service and DOD have also purchased smart phone location data.[200]

As part of the House Committee on the Judiciary's investigation into the IRS's troubling visit to the home of journalist Matt Taibbi on the day he testified before the Select Subcommittee on the Weaponization of the Federal Government, the Committee discovered that the IRS collected personal data from data brokers to use in its investigation of Taibbi.[201] For example, the IRS collected data from the data broker Anywho, a People Search Website.[202] It is concerning enough that the IRS would take the extreme step of visiting someone's home on the day he testified before Congress. But the IRS compiled its information from a data broker, potentially accessing vast amounts of Taibbi's private information.

These actions allow government agencies and law enforcement to evade the Fourth Amendment and collect limitless information of Americans. The Fourth Amendment Is Not For Sale Act closes this legal loophole and stops data brokers from buying and selling Americans' personal information to the government by requiring

---

[193] *See* Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL STREET JOURNAL (Jun. 19, 2020), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.

[194] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[195] *See* Alex Deise, *Bill of the Month: The Fourth Amendment is Not for Sale Act*, FREEDOMWORKS (Jul. 29, 2022), https://www.freedomworks.org/bill-of-the-month-july-2022-the-fourth-amendment-is-not-for-sale-act/.

[196] *See* Byron Tau, *FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do.*, WALL STREET JOURNAL.

[197] *Id.*

[198] *See* Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CENTER FOR JUSTICE (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.

[199] *Id.*

[200] *Id.*

[201] *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Daniel Werfel, Commissioner, Internal Revenue Service (May 24, 2023).

[202] *See* Yael Grauer, *Here's a Long List of Data Broker Sites and How to Opt-Out of Them*, VICE (Mar. 27, 2018).

the government to obtain a court order before acquiring customer or subscriber information from a third party.

As technology continues to advance and Americans incidentally share more data through the devices we use every day, it is important for Congress to protect privacy interests and ensure that government agencies and law enforcement abide by the Fourth Amendment. Congress has the opportunity to codify the Supreme Court's decision in *Carpenter* and address "additional categories of highly sensitive information that merit the protection of a warrant regardless of whether they are held by third parties."[203]

B. NEED FOR LEGISLATION

On April 27, 2023, the House Judiciary Subcommittee on Crime and Federal Government Surveillance held a hearing entitled "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them."[204] On July 14, 2023, the Subcommittee held a second hearing entitled "Fixing FISA, Part II."[205] Both of those hearings explored the utilities of FISA and the ways in which FISA is in need of reform to better protect Americans' civil liberties from government surveillance and abuse. In considering necessary FISA reforms, several witnesses and lawmakers expressed concerns regarding recent revelations exposing the misuse of FISA authorities by government actors.[206]

On July 19, 2023, the House Judiciary Committee unanimously passed H.R. 4639, the Fourth Amendment Is Not For Sale Act.[207] During the markup of H.R. 4639, lawmakers expressed a similar concern regarding warrantless government surveillance of Americans' data.[208] Specifically, Members expressed concern about the developing practice wherein government agencies are able to exploit a legal loophole to purchase massive amounts of Americans' information from data brokers, even though that same information would ordinarily require the agency to obtain a court order if gathering the information themselves.[209]

The pervasive surveillance and misuse of FISA authorities are well-documented. For example, in 2019 and 2020, Department of Justice Inspector General Michael Horowitz exposed how the FBI violated its authorities under FISA by improperly spying on Trump campaign associates.[210] The government also conducts "backdoor searches" of Americans' communications, most of the time without obtaining a warrant. Illustratively, in 2021, the FBI queried the communications of U.S. persons over 3.3 million times.[211] In 2022,

---

[203] *Id.*

[204] *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).

[205] *Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).

[206] *See id.*

[207] *Markup of H.R. 1531, H.R. 4250, and H.R. 4639 Before the H. Comm. On the Judiciary*, 118th Cong. (2023).

[208] *See generally id.*

[209] *Id.*

[210] *See, e.g.*, U.S. DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019); *see also* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS AT 3 (2020).

[211] *See generally* 2021 ODNI Annual Statistical Transparency Report, *supra* note 84.

the FBI similarly conducted hundreds of U.S. person queries per day.[212] These queries included Members of Congress, state senators, judges, campaign donors, protestors, and others.[213] With respect to the practice of data purchasing, several law enforcement agencies and reports have revealed the purchase of Americans' information in bulk, including the FBI, CBP, ICE, Secret Service, and DOD.[214]

H.R. 6570, the Protect Liberty and End Warrantless Surveillance Act, would put important guardrails in place to limit government surveillance and protect Americans' civil liberties. The bill requires a court order from the FISC or a warrant before any member of the intelligence community is able to query U.S. persons' information held in the Section 702 database, subject to limited exceptions. In addition, the bill drastically reduces the number of FBI officials authorized to conduct such queries. Moreover, its provisions limit the use of information obtained pursuant to Section 702, repeals the ability of the intelligence community to resume "abouts" collection, and makes important reforms to the FISC that ensure the court, and the proceedings before it, are carried out with greater transparency, integrity, and accountability. The bill also provides Congress with greater oversight of the FISC and FISCR, as well as more visibility into the intelligence community's compliance with FISA. It also eliminates the legal loophole that federal agencies use to purchase data on Americans by requiring the government to obtain a court order before acquiring such information from a third party.

Hearings

For the purposes of clause 3(c)(6)(A) of House rule XIII, the following hearings were used to develop H.R. 6570: "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them" a hearing held on April 27, 2023, before the Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary. The Committee heard testimony from the following witnesses:

- Mr. Michael Horowitz, Inspector General, U.S. Department of Justice Office of the Inspector General;
- Ms. Sharon Bradford Franklin, Chair, Privacy and Civil Liberties Oversight Board; and
- Ms. Beth A. Williams, Board Member, Privacy and Civil Liberties Oversight Board.

The hearing addressed the use of FISA authorities and non-compliance with established statutory and administrative procedures intended to safeguard Americans' civil liberties.

The Subcommittee on Crime and Federal Government Surveillance also held a hearing on July 14, 2023, titled "Fixing FISA, Part II." The Committee heard testimony from the following witnesses:

---

[212] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 24.

[213] *See, e.g.*, Memorandum Opinion and Order, *Document re: Section 702 2021 Certification* at 29 (FISA Ct. Apr. 21, 2022).

[214] *See* Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data, Brennan Center for Justice* (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data; Byron Tau, *FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do.*, Wall Street Journal.

- Professor Jonathan Turley, George Washington University Law School;
- Mr. Phil Kiko, Principal, Williams & Jensen;
- Mr. Gene Schaerr, General Counsel, Project for Privacy and Surveillance Accountability; and
- Ms. Elizabeth Goitein, Senior Director, Liberty & National Security Program, Brennan Center for Justice.

The hearing further addressed the deficient safeguards in FISA, and contemplated the necessity of imposing a warrant requirement for Section 702 queries.

Committee Consideration

On December 6, 2023, the Committee met in open session and ordered the bill, H.R. 6570, favorably reported with an amendment in the nature of a substitute, by a roll call vote of 35 to 2, a quorum being present.

Committee Votes

In compliance with clause 3(b) of House rule XIII, the following roll call votes occurred during the Committee's consideration of H.R. 6570:

1. Vote on Amendment #3 to H.R. 6570 ANS, offered by Mr. Swalwell, failed 9–20
2. Vote on Amendment #4 to H.R. 6570 ANS, offered by Mr. Buck, failed 4–22
3. Vote on Favorably Reporting H.R. 6570, as amended, passed 35–2

Date: 3/16/2022

COMMITTEE ON EDUCATION AND LABOR RECORD OF COMMITTEE VOTE

Roll Call:1 Bill: 5428 Amendment Number:2

Disposition: Defeated by a roll call vote of 21-28

Sponsor/Amendment: Owens / RANS_001

Name & State	Aye	No	Not Voting	Name & State	Aye	No	Not Voting
Mr. SCOTT (VA) (Chairman)		X		Mrs. FOXX (NC) (Ranking)	X		
Mr. GRIJALVA (AZ)		X		Mr. WILSON (SC)	X		
Mr. COURNTEY (CT)		X		Mr. THOMPSON (PA)	X		
Mr. SABLAN (MP)			X	Mr. WALBERG (MI)	X		
Ms. WILSON (FL)		X		Mr. GROTHMAN (WI)	X		
Ms. BONAMICI (OR)		X		Ms. STEFANIK (NY)	X		
Mr. TAKANO (CA)		X		Mr. ALLEN (GA)	X		
Ms. ADAMS (NC)		X		Mr. BANKS (IN)	X		
Mr. DESAULNIER (CA)		X		Mr. COMER (KY)	X		
Mr. NORCROSS (NJ)		X		Mr. FULCHER (ID)	X		
Ms. JAYAPAL (WA)		X		Mr. KELLER (PA)	X		
Mr. MORELLE (NY)		X		Ms. MILLER-MEEKS (IA)	X		
Ms. WILD (PA)		X		Mr. OWENS (UT)	X		
Mrs. MCBATH (GA)		X		Mr. GOOD (VA)		X	
Mrs. HAYES (CT)		X		Mrs. MCCLAIN (MI)	X		
Mr. LEVIN (MI)		X		Mrs. HARSHBARGER (TN)	X		
Ms. OMAR (MN)		X		Mrs. MILLER (IL)	X		
Ms. STEVENS (MI)		X		Mrs. SPARTZ (IN)			X
Ms. LEGER FERNÁNDEZ (NM)		X		Mr. FITZGERALD (WI)	X		
Mr. JONES (NY)		X		Mr. CAWTHORN (NC)	X		
Ms. MANNING (NC)		X		Mrs. STEEL (CA)	X		
Mr. MRVAN (IN)		X		Ms. LETLOW (LA)	X		
Mr. BOWMAN (NY)		X		Mr. JACOBS (NY)	X		
Mrs. CHERFILUS-MCCORMICK (FL)		X		*Vacancy*			
Mr. POCAN (WI)		X					
Mr. CASTRO (TX)		X					
Ms. SHERRILL (NJ)		X					
Mr. ESPAILLAT (NY)		X					
Mr. KWEISI MFUME (MD)			X				

TOTALS: Ayes: 21 Nos:28 Not Voting: 3

Total: 53 / Quorum: / Report:

(29 D - 24 R)

^Although not present for the recorded vote, Member expressed he/she would have voted AYE if present at time of vote.

*Although not present for the recorded vote, Member expressed he/she would have voted NO if present at time of vote.

Date: 3/16/2022

COMMITTEE ON EDUCATION AND LABOR RECORD OF COMMITTEE VOTE

Roll Call:2 Bill: 5428 Amendment Number: 3

Disposition: Defeated by a roll call vote of 22-27

Sponsor/Amendment: Stefanik / RAMD_002

Name & State	Aye	No	Not Voting	Name & State	Aye	No	Not Voting
Mr. SCOTT (VA) (Chairman)		X		Mrs. FOXX (NC) (Ranking)	X		
Mr. GRIJALVA (AZ)		X		Mr. WILSON (SC)	X		
Mr. COURNTEY (CT)		X		Mr. THOMPSON (PA)	X		
Mr. SABLAN (MP)			X	Mr. WALBERG (MI)	X		
Ms. WILSON (FL)		X		Mr. GROTHMAN (WI)	X		
Ms. BONAMICI (OR)		X		Ms. STEFANIK (NY)	X		
Mr. TAKANO (CA)		X		Mr. ALLEN (GA)	X		
Ms. ADAMS (NC)		X		Mr. BANKS (IN)	X		
Mr. DESAULNIER (CA)		X		Mr. COMER (KY)	X		
Mr. NORCROSS (NJ)		X		Mr. FULCHER (ID)	X		
Ms. JAYAPAL (WA)		X		Mr. KELLER (PA)	X		
Mr. MORELLE (NY)		X		Ms. MILLER-MEEKS (IA)	X		
Ms. WILD (PA)		X		Mr. OWENS (UT)	X		
Mrs. MCBATH (GA)		X		Mr. GOOD (VA)	X		
Mrs. HAYES (CT)		X		Mrs. MCCLAIN (MI)	X		
Mr. LEVIN (MI)		X		Mrs. HARSHBARGER (TN)	X		
Ms. OMAR (MN)		X		Mrs. MILLER (IL)	X		
Ms. STEVENS (MI)		X		Mrs. SPARTZ (IN)			X
Ms. LEGER FERNÁNDEZ (NM)		X		Mr. FITZGERALD (WI)	X		
Mr. JONES (NY)		X		Mr. CAWTHORN (NC)	X		
Ms. MANNING (NC)		X		Mrs. STEEL (CA)	X		
Mr. MRVAN (IN)		X		Ms. LETLOW (LA)	X		
Mr. BOWMAN (NY)		X		Mr. JACOBS (NY)	X		
Mrs. CHERFILUS-MCCORMICK (FL)		X		*Vacancy*			
Mr. POCAN (WI)		X					
Mr. CASTRO (TX)		X					
Ms. SHERRILL (NJ)		X					
Mr. ESPAILLAT (NY)		X					
Mr. KWEISI MFUME (MD)			X				

TOTALS: Ayes: 22 Nos: 27 Not Voting: 3

Total: 53 / Quorum: / Report:

(29 D - 24 R)

^Although not present for the recorded vote, Member expressed he/she would have voted AYE if present at time of vote.

*Although not present for the recorded vote, Member expressed he/she would have voted NO if present at time of vote.

Date: 3/16/2022

COMMITTEE ON EDUCATION AND LABOR RECORD OF COMMITTEE VOTE

Roll Call:3 Bill: 5428 Amendment Number: 4

Disposition: Defeated by a roll call vote of 22-27

Sponsor/Amendment: Allen / RAMD_001

Name & State	Aye	No	Not Voting	Name & State	Aye	No	Not Voting
Mr. SCOTT (VA) (Chairman)		X		Mrs. FOXX (NC) (Ranking)	X		
Mr. GRIJALVA (AZ)		X		Mr. WILSON (SC)	X		
Mr. COURNTEY (CT)		X		Mr. THOMPSON (PA)	X		
Mr. SABLAN (MP)			X	Mr. WALBERG (MI)	X		
Ms. WILSON (FL)		X		Mr. GROTHMAN (WI)	X		
Ms. BONAMICI (OR)		X		Ms. STEFANIK (NY)	X		
Mr. TAKANO (CA)		X		Mr. ALLEN (GA)	X		
Ms. ADAMS (NC)		X		Mr. BANKS (IN)	X		
Mr. DESAULNIER (CA)		X		Mr. COMER (KY)	X		
Mr. NORCROSS (NJ)		X		Mr. FULCHER (ID)	X		
Ms. JAYAPAL (WA)		X		Mr. KELLER (PA)	X		
Mr. MORELLE (NY)		X		Ms. MILLER-MEEKS (IA)	X		
Ms. WILD (PA)		X		Mr. OWENS (UT)	X		
Mrs. MCBATH (GA)		X		Mr. GOOD (VA)	X		
Mrs. HAYES (CT)		X		Mrs. MCCLAIN (MI)	X		
Mr. LEVIN (MI)		X		Mrs. HARSHBARGER (TN)	X		
Ms. OMAR (MN)		X		Mrs. MILLER (IL)	X		
Ms. STEVENS (MI)		X		Mrs. SPARTZ (IN)			X
Ms. LEGER FERNÁNDEZ (NM)		X		Mr. FITZGERALD (WI)	X		
Mr. JONES (NY)		X		Mr. CAWTHORN (NC)	X		
Ms. MANNING (NC)		X		Mrs. STEEL (CA)	X		
Mr. MRVAN (IN)		X		Ms. LETLOW (LA)	X		
Mr. BOWMAN (NY)		X		Mr. JACOBS (NY)	X		
Mrs. CHERFILUS-MCCORMICK (FL)		X		*Vacancy*			
Mr. POCAN (WI)		X					
Mr. CASTRO (TX)		X					
Ms. SHERRILL (NJ)		X					
Mr. ESPAILLAT (NY)		X					
Mr. KWEISI MFUME (MD)			X				

TOTALS: Ayes: 22 Nos: 27 Not Voting: 3

Total: 53 / Quorum: / Report:

(29 D - 24 R)

^Although not present for the recorded vote, Member expressed he/she would have voted AYE if present at time of vote.

*Although not present for the recorded vote, Member expressed he/she would have voted NO if present at time of vote.

Committee Oversight Findings

In compliance with clause 3(c)(1) of House rule XIII, 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

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the *Congressional Budget Act of 1974* and with respect to the requirements of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the *Congressional Budget Act of 1974*, the Committee has requested but not received a cost estimate for this bill from the Director of the Congressional Budget Office. The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures. The Chairman of the Committee shall cause such estimate and statement to be printed in the *Congressional Record* upon its receipt by the Committee.

Congressional Budget Office Cost Estimate

With respect to the requirement of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974* was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

Committee Estimate of Budgetary Effects

With respect to the requirements of clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974*.

Duplication of Federal Programs

Pursuant to clause 3(c)(5) of House rule XIII, no provision of H.R. 6570 establishes or reauthorizes a program of the federal government known to be duplicative of another federal program.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of House rule XIII, H.R. 6570 reauthorizes Section 702 of the Foreign Intelligence Surveillance Act (FISA) for three years with significant reforms. It requires the government to obtain an order from the Foreign Intelligence Surveillance Court (FISC) or a warrant prior to conducting U.S. person queries of information collected through Section 702. It provides for greater scrutiny of applications sub-

mitted to the FISC, increases transparency in surveillance applications, requires more frequent and detailed reports and audits, and establishes additional penalties for government employees who violate FISA or mislead the FISC.

The bill also closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant. If the agency were to gather this information itself, it would be required to obtain a warrant, subpoena, or other legal order. By closing this loophole, the bill prevents government agencies from conducting an end-run around the protections of the Fourth Amendment.

Advisory on Earmarks

In accordance with clause 9 of House rule XXI, H.R. 6570 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clauses 9(d), 9(e), or 9(f) of House rule XXI.

Federal Mandates Statement

An estimate of federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the *Unfunded Mandates Reform Act* was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the *Federal Advisory Committee Act* were created by this legislation.

Applicability to Legislative Branch

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the *Congressional Accountability Act* (Pub. L. 104–1).

Section-by-Section Analysis

Sec. 1. Short title

- The Act is the "Protect Liberty and End Warrantless Surveillance Act."

Sec. 2. Query procedure reform

- Limits the number of FBI employees who may perform United States person queries to 5 employees per field office.
- Limits the number of FBI employees at FBI headquarters who may perform U.S. person queries to 5.
- Prohibits U.S. person queries of Section 702-acquired information if the compelled production of that information would require a probable cause warrant if sought for law enforcement purposes in the United States.

- Provides an exception when the subject of a query is subject to an order or emergency authorization under Title I or Title III of FISA, or a criminal warrant.
- Provides an exception when there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm and the information is sought for the purpose of preventing or mitigating the threats. Requires a description of the query to be sent to FISC, House and Senate Judiciary Committees, and House and Senate Intelligence Committees.
- Provides an exception where the U.S. person gives consent to the query.
- Provides an exception where the query uses a known cybersecurity threat signature as a query term, and query is conducted for sole purpose of mitigating or preventing such a threat. Requires these queries to be reported to the Foreign Intelligence Surveillance Court (FISC).

• Permits queries for communications metadata but prohibits use of results of a metadata query as a basis for access to communications and other protected information.

• Requires that queries must be reasonably likely to retrieve foreign intelligence information.

• For all U.S. person queries, requires documentation of the query term, date of query, identifier for person conducting query, and statement of facts showing that query was reasonably likely to retrieve foreign intelligence information or in furtherance of the exceptions.

Sec. 3. Limitation on use of information obtained under section 702 of the Foreign Intelligence Surveillance Act of 1978 relating to United States persons and persons located in the United States in criminal, civil, and administrative actions

• Prohibits the use in criminal, civil, and administrative proceedings and investigations, of information acquired under section 702, except with prior approval of the Attorney General and provided that the proceeding or investigation involves terrorism, actions necessitating counterintelligence, the proliferation or use of a weapon of mass destruction, a cybersecurity breach or attack from a foreign country, incapacitation or destruction of critical infrastructure, an attack against the armed forces of the United States or an ally of the United States or to other personnel of the United States Government or a government ally of the United States, or international narcotics trafficking.

Sec. 4. Repeal of authority for the resumption of abouts collection

• Repeals the authority to resume "abouts" collection under Section 702. Existing law permits the resumption of "abouts" collection with notice to Congress.

Sec. 5. Foreign Intelligence Surveillance Court (FISC) reform

• Requires the same FISC judge to hear FISA renewal applications unless that judge is no longer serving on the FISC.

• Allows the FISC to appoint one or more amicus curiae in a case and expands the types of cases where the FISC shall appoint an amicus curiae, unless the court issues a finding that such ap-

pointment is not appropriate. Such cases would include: A case that presents a novel or significant interpretation of the law (current law only provides for amicus participation in these such cases); a case that presents significant concerns with respect to the activities of a U.S. person that are protected by the First Amendment of the Constitution; a case that presents or involves a Sensitive Investigative Matter; a case that presents a request for approval of a new program, a new technology, or a new use of existing technology; a case that presents a request for reauthorization of programmatic surveillance; a case that otherwise presents novel or significant civil liberties issues; and a case that involves the activities of a U.S. person.

- Defines Sensitive Investigative Matter (SIM) to be an investigative matter involving the activities of: a domestic public official or political candidate, or a staff member of such an official or candidate; a domestic religious or political organization, or a U.S. person prominent in such an organization; or the domestic news media.
    - SIM also includes "any other investigative matter involving a domestic entity or a known or suspected U.S. person that," in the judgment of the applicable court, is as sensitive as a Sensitive Investigative Matter.
- Grants amici the authority to seek review of FISC decisions to the United States Foreign Intelligence Surveillance Court of Review (FISCR) and of FISCR decisions to the United States Supreme Court, and requires the FISC to provide a written statement of reasons for a denial of a petition for review by an amicus.
- Provides amici with access to certain documents in connection with the matter, including classified information.

Sec. 6. Application for an order approving electronic surveillance

- Requires the application to include a statement describing the normal investigative techniques taken before submitting the application and an explanation as to why those techniques are insufficient.
- Applications for electronic surveillance must include all information material to an application, including exculpatory information.
- Each federal employee who contributes to the drafting of a FISA application must sign an affidavit attesting to the accuracy of the application.
- Prohibits the use of opposition research and news media in FISA applications unless that information disclosed in the application and provided that it is not the sole source of the information justifying the allegations in the application.

Sec. 7. Public disclosure and declassification of certain documents

- Currently, 50 U.S.C. 1871(c) requires the Attorney General to share with the House and Senate Intelligence and Judiciary Committees certain FISC decisions, orders, and opinions within 45 days of issuance. This provision would require that the Attorney General also share copies of those documents that have undergone declassification review at that same time.

• Amends 50 U.S.C. 1872(a) to require the Director of National Intelligence and Attorney General to conclude their declassification review not later than 45 days after commencement of such review.

Sec. 8. Transcriptions of proceedings; attendance of certain Congressional Officials at certain proceedings

• Allows the Chair and Ranking Member of the House and Senate Judiciary Committees and the House and Senate Intelligence Committees, or their designated staff, to attend all FISC and FISCR proceedings. Allows the Chairs and Ranking Members to designate 2 Members of Congress to attend proceedings on their behalf.

• Requires transcripts of FISC proceedings to be maintained and available for review by those permitted to attend proceedings not later than 45 days after any such proceedings.

Sec. 9. Annual Audit of FISA Compliance by Inspector General

• Requires the DOJ IG to complete an annual report of alleged violations and failures to comply with the requirements of FISA and to submit that report to the congressional intelligence committees and House and Senate Judiciary Committees by June 30 of each year.

Sec. 10. Reporting on accuracy and completeness of applications

• Requires an existing annual report by the Director of the Administrative Office of the United States Courts to include an additional analysis of the accuracy and completeness of applications and certifications.

Sec. 11. Annual report of the Federal Bureau of Investigation

• Requires the FBI to annually report to Congress a comprehensive account of ongoing disciplinary investigations, adjudication of concluded investigations, and subsequent disciplinary actions resulting from violations of the requirements of FISA.

• Requires the FBI to annually report to Congress on the number of U.S. person queries conducted, what terms were used, the number of warrants issued and denied, and the number of times exceptions from the warrant requirement were alleged.

Sec. 12. Extension of Title VII of FISA; expiration of FISA authorities; effective dates

• Extends Title VII (including Section 702 of FISA) for 3 years, until December 31, 2026.

Sec. 13. Criminal penalties for violations of FISA

• Increases the maximum penalty for a person who intentionally engages in electronic surveillance under color of law or intentionally discloses or uses information obtained under color of law by electronic surveillance not authorized by law. Makes these offenses punishable by a fine of not more than $10,000 or imprisonment of not more than 8 years, or both.

• Adds criminal penalty for knowingly making a false material declaration or material omission in any document submitted to or statement made before the FISC or FISCR. Makes this offense

punishable by a fine of not more than $10,000 or imprisonment for not more than 8 years, or both.

• Adds criminal penalty for intentionally disclosing a FISA application or classified information contained in the application to any person not entitled to receive such information. Makes this offense punishable by a fine of not more than $10,000 or imprisonment for not more than 8 years, or both.

Sec. 14. Contempt power of FISC and FISCR

• Provides FISC and FISCR with the authority to prosecute a person for contempt and requires the FISC and FISCR to jointly submit an annual report to Congress on the use of this authority.

Sec. 15. Increased penalties for civil actions

• Increases civil damages for a U.S. person harmed by a violation of FISA to $10,000 (current statute is $1,000 for an aggrieved person).

• If a court finds a person violated the Act, the head of the agency that employs that person shall submit a report to Congress on the administrative action taken against that person and report their name to the FISC.

Sec. 16. Accountability procedures for incidents relating to queries conducted by the FBI

• Requires the Director of the FBI to establish procedures to hold FBI employees accountable for violations of law, guidance, and procedures governing queries of Section 702-acquired information.

• The accountability procedures shall include centralized tracking of incidents, minimum consequences for initial and subsequent incidents. Includes a clarification for requirements for referring intentional misconduct and reckless conduct to the FBI's Inspection Division for investigation and disciplinary action by the FBI's Office of Professional Responsibility.

• Requires a report to Congress detailing the accountability procedures and an annual report describing disciplinary actions taken and a description of the circumstances surrounding each such disciplinary action.

Sec. 17. Agency procedures to ensure compliance

• Requires each agency that acquires foreign intelligence information under FISA to establish clear rules on what constitutes a violation of the Act, and procedures for taking appropriate adverse personnel actions against any officer or employee who engages in such a violation, including more severe adverse actions for any subsequent violation. Requires the head of each federal department or agency to report to Congress on such procedures not later than 3 months after the date of enactment.

Sec. 18. Protection of records held by data brokers

• Defines various terms and prevents law enforcement and intelligence agencies from buying data about a United States person, located anywhere in the world, or data about any person located in the United States that:

- Is data about a person's device, from their online account, or created or shared by a technology and telecommunications company providing a service to that person;
- Was obtained from a technology or communications company providing service to the target in a manner that violated a contract, or the company's terms of service or privacy policy;
- Was obtained by deceiving the person whose information was obtained; or
- Was obtained by accessing the person's device or online account without authorization.

• Also prohibits the use or sharing by the government of any information obtained in violation of this section, including as evidence in court or before a grand jury, regulatory body, or in another similar proceeding. This section further requires the Attorney General to adopt specific procedures to minimize the acquisition and retention of this information, and to prohibit its dissemination.

Sec. 19. Required disclosure

• Prohibits the use or sharing by the government of any information obtained in violation of this section, including as evidence in court or before a grand jury, regulatory body, or in another similar proceeding. This section further requires the Attorney General to adopt specific procedures to minimize the acquisition and retention of this information, and to prohibit its dissemination.

Sec. 20. Intermediary service providers

• Extends the protections in the Electronic Communications Privacy Act to data held by intermediary service providers, which are entities that directly or indirectly deliver, store, or process communications for or on behalf of technology or communications firms.

Sec. 21. Limits on surveillance conducted for foreign intelligence purposes other than under the Foreign Intelligence Surveillance Act of 1978

• Narrows a legal carveout in FISA permitting the intelligence community, without an order issued by a court, to buy or obtain through other methods, metadata about calls, texts, emails, and web browsing, where at least one end of the communication is located abroad. This section limits the carveout such that it only applies to the acquisition of foreign intelligence information of non-Americans located outside the United States.

• Specifies that FISA authorities shall be the exclusive means by which the government obtains information inside the U.S. or from U.S. technology or communications companies electronic communications transactions records, call detail records, or other metadata about the communications of United States persons, located anywhere in the world, or any person located in the United States.

• Specifies that Title I and sections 303, 304, 703, 704, and 705 of FISA shall be the exclusive means by which the government obtains inside the location information of U.S. persons or persons inside the United States, web browsing history, Internet search history, or any other data that would require a court order to compel, about United States persons, located anywhere in the world, or any person located in the United States.

Sec. 22. Limit on civil immunity for providing information, facilities, or technical assistance to the government absent a court order

Removes the Attorney General's authority to grant civil immunity to those that provide unlawful assistance for government surveillance not required or permitted by federal law. Immunity remains for any surveillance assistance ordered by a court.

Sec. 23. Prohibition on reverse targeting of United States persons and persons located in the United States

Prohibits the acquisition of communications if a significant purpose is to acquire the information of one or more United States person or persons believed to be located in the United States.

Sec. 24. Required disclosure of relevant information in Foreign Intelligence Surveillance Act of 1978 applications

Requires the Attorney General to establish a set of accuracy procedures to ensure that an application for a court order under FISA includes all information that might reasonably call into question the accuracy of the information or reasonableness of any assessment in the application. Requires the application to include a description of the accuracy procedures and a certification that the federal officer making the application has reviewed it for accuracy and completeness.

Sec. 25. Enhanced annual reports by Director of National Intelligence

Requires enhanced reports on statistics regarding persons targeted for surveillance under Section 702, and other reports including the number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of U.S. persons, the number of disseminated intelligence reports derived from collection not authorized by FISA containing the identities of U.S. persons, the number of queries conducted to find communications or information of or about U.S. persons, the number of criminal proceedings in which the government entered into evidence or otherwise used or disclosed in a criminal proceeding any information obtained or derived from an acquisition conducted without a court order, subpoena, or other legal process established by statute.

Sec. 26. Quarterly report

Requires the Attorney General, in consultation with the Director of National Intelligence, to submit quarterly reports to the congressional intelligence committees and Committees on the Judiciary of the Senate and of the House of Representatives that include the total number of warrants issued to conduct a query of information acquired under section 702, the total number of times a query was conducted pursuant to an exception, the total number of queries that were conducted using a United States person query term.

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 omit-

ted is enclosed in black brackets, new matter is printed in italics, and 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 I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

DESIGNATION OF JUDGES

SEC. 103. (a)(1) The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b). *To the extent practicable, no judge designated under this subsection shall hear a renewal application for electronic surveillance under this Act, which application was previously granted by another judge designated under this subsection, unless the term of the judge who granted the application has expired, or that judge is otherwise no longer serving on the court.*

(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) or paragraph (4) or (5) of section 702(i), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

(ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) [Proceedings under this Act] *(1) Proceedings under this Act* shall be conducted as expeditiously as possible. The record of proceedings under this Act, [including applications made and orders granted] *including applications made, orders granted, and transcriptions of proceedings,*, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.

(2) The chair and ranking minority member of each of the congressional intelligence committees and of the Committees on the Judiciary of the House of Representatives and of the Senate shall be entitled to attend any proceeding of the Foreign Intelligence Surveillance Court or any proceeding of the Foreign Intelligence Surveillance Court of Review. Each person entitled to attend a proceeding pursuant to this paragraph may designate not more than 2 Members of Congress and not more than 2 staff members of such committee to attend on their behalf, pursuant to such procedures as the Attorney General, in consultation with the Director of National Intelligence may establish. Not later than 45 days after any such proceeding, a copy of any application made, order granted, or transcription of the proceeding shall be made available for review to each person who is entitled to attend a proceeding pursuant to this paragraph or who is designated under this paragraph. Terms used in this paragraph have the meanings given such terms in section 701(b).

(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall

be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

(e)(1) Three judges designated under subsection (a) who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section 501(f)(1) or 702(h)(4).

(2) Not later than 60 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the court established under subsection (a) shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 501(f)(1) or 702(h)(4) by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.

(g)(1) The courts established pursuant to subsections (a) and (b) may establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this Act.

(2) The rules and procedures established under paragraph (1), and any modifications of such rules and procedures, shall be recorded, and shall be transmitted to the following:

(A) All of the judges on the court established pursuant to subsection (a).

(B) All of the judges on the court of review established pursuant to subsection (b).

(C) The Chief Justice of the United States.

(D) The Committee on the Judiciary of the Senate.

(E) The Select Committee on Intelligence of the Senate.

(F) The Committee on the Judiciary of the House of Representatives.

(G) The Permanent Select Committee on Intelligence of the House of Representatives.

(3) The transmissions required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(h) Nothing in this Act shall be construed to reduce or contravene the inherent authority of a court established under this section to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court.

(i) AMICUS CURIAE.—

(1) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after the enactment of this subsection, jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall serve pursuant to rules the presiding judges may establish. In designating such individuals, the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate.

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

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

(A) shall, unless the court issues a finding that appointment is not appropriate, appoint 1 or more individuals who have been designated under paragraph (1), not fewer than 1 of whom possesses privacy and civil liberties expertise, unless the court finds that such a qualification is inappropriate, to serve as amicus curiae to assist the court in the consideration of any application or motion for an order or review that, in the opinion of the court—

(i) presents a novel or significant interpretation of the law;

(ii) presents significant concerns with respect to the activities of a United States person that are protected by the first amendment to the Constitution of the United States;

(iii) presents or involves a sensitive investigative matter;

(iv) presents a request for approval of a new program, a new technology, or a new use of existing technology;

(v) presents a request for reauthorization of programmatic surveillance;

(vi) otherwise presents novel or significant civil liberties issues; or

(vii) otherwise involves the activities of a United States person; and

(B) may appoint [an individual or organization] *1 or more individuals or organizations* to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion,

permit [an individual or organization] *1 or more individuals or organizations* leave to file an amicus curiae brief.

(3) QUALIFICATIONS OF AMICUS CURIAE.—

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

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

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

[(A)] *(i)* legal arguments that advance the protection of individual privacy and civil liberties*, including legal arguments regarding any privacy or civil liberties interest of any United States person that would be significantly impacted by the application or motion*;

[(B)] *(ii)* information related to intelligence collection or communications technology; or

[(C)] *(iii)* legal arguments or information regarding any other area relevant to the issue presented to the court[.]*; and*

(B) may seek leave to raise any novel or significant privacy or civil liberties issue relevant to the application or motion or other issue directly impacting the legality of the proposed electronic surveillance with the court, regardless of whether the court has requested assistance on that issue.

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

(6) ACCESS TO INFORMATION.—

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

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

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

(A) IN GENERAL.—

(i) RIGHT OF AMICUS.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

(I) shall have access, to the extent such information is available to the Government, to—

(aa) the application, certification, petition, motion, and other information and supporting materials, including any information described in section 901, submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed, including access to any relevant legal precedent (including any such precedent that is cited by the Government, including in such an application);

(bb) an unredacted copy of each relevant decision made by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review in which the court decides a question of law, without regard to whether the decision is classified; and

(cc) any other information or materials that the court determines are relevant to the duties of the amicus curiae; and

(II) may make a submission to the court requesting access to any other particular materials or information (or category of materials or information) that the amicus curiae believes to be relevant to the duties of the amicus curiae.

(ii) SUPPORTING DOCUMENTATION REGARDING ACCURACY.—The Foreign Intelligence Surveillance Court, upon the motion of an amicus curiae appointed under paragraph (2) or upon its own motion, may require the Government to make available the supporting documentation described in section 902.

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

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

(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court shall have access, to the extent such information is available to the Government, to unredacted copies of each opinion, order, transcript, pleading, or other document of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review, including, if the individual is eligible for access

to classified information, any classified documents, information, and other materials or proceedings.

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

(7) AUTHORITY TO SEEK REVIEW OF DECISIONS.—

(A) FISA COURT DECISIONS.—

(i) PETITION.—Following issuance of an order under this Act by the Foreign Intelligence Surveillance Court, an amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court to certify for review to the Foreign Intelligence Surveillance Court of Review a question of law pursuant to subsection (j).

(ii) WRITTEN STATEMENT OF REASONS.—If the Foreign Intelligence Surveillance Court denies a petition under this subparagraph, the Foreign Intelligence Surveillance Court shall provide for the record a written statement of the reasons for the denial.

(iii) APPOINTMENT.—Upon certification of any question of law pursuant to this subparagraph, the Court of Review shall appoint the amicus curiae to assist the Court of Review in its consideration of the certified question, unless the Court of Review issues a finding that such appointment is not appropriate.

(B) FISA COURT OF REVIEW DECISIONS.—An amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court of Review to certify for review to the Supreme Court of the United States any question of law pursuant to section 1254(2) of title 28, United States Code.

(C) DECLASSIFICATION OF REFERRALS.—For purposes of section 602, a petition filed under subparagraph (A) or (B) of this paragraph and all of its content shall be considered a decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review described in paragraph (2) of section 602(a).

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

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

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

[(10)**]** *(11)* RECEIPT OF INFORMATION.—Nothing in this subsection shall limit the ability of a court established under sub-

section (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.

[(11)**]** *(12)* COMPENSATION.—Notwithstanding any other provision of law, a court established under subsection (a) or (b) may compensate an amicus curiae appointed under paragraph (2) for assistance provided under such paragraph as the court considers appropriate and at such rate as the court considers appropriate.

(13) DEFINITION.—In this subsection, the term "sensitive investigative matter" means—

(A) an investigative matter involving the activities of—

(i) a domestic public official or political candidate, or an individual serving on the staff of such an official or candidate;

(ii) a domestic religious or political organization, or a known or suspected United States person prominent in such an organization; or

(iii) the domestic news media; or

(B) any other investigative matter involving a domestic entity or a known or suspected United States person that, in the judgment of the applicable court established under subsection (a) or (b), is as sensitive as an investigative matter described in subparagraph (A).

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

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

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

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

APPLICATION FOR AN ORDER

SEC. 104. (a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title. It shall include—

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques *(and a description of such techniques)*;

(7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(8) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; **[**and**]**

(9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter**[**.**]***; and*

(10) all information material to the application, including any information that tends to rebut—

(A) any allegation set forth in the application; or

(B) the existence of probable cause to believe that—

(i) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(ii) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.

(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

(d)(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) an application under that subsection for a target described in section 101(b)(2).

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such offi-

cial may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

(e) The statement of facts and circumstances under subsection (a)(3) may only include information obtained from the content of a media source or information gathered by a political campaign if—

(1) such information is disclosed in the application as having been so obtained or gathered; and

(2) such information is not the sole source of the information used to justify the applicant's belief described in subsection (a)(3).

ISSUANCE OF AN ORDER

SEC. 105. (a) Upon an application made pursuant to section 104, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 101(h)**[**; and**]***;*

(4) the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d)**[**.**]***; and*

(5) the statement of facts and circumstances under subsection (a)(3) may only include information obtained from the content of a media source or information gathered by a political campaign if—

(A) such information is disclosed in the application as having been so obtained or gathered; and

(B) such information is not the sole source of the information used to justify the applicant's belief described in subsection (a)(3).

(b) In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c)(1) SPECIFICATIONS.—An order approving an electronic surveillance under this section shall specify—

(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3);

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(3) SPECIAL DIRECTIONS FOR CERTAIN ORDERS.—An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of—

(A) the nature and location of each new facility or place at which the electronic surveillance is directed;

(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

(d)(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a), (1), (2), or (3), for the period specified in the application or for one year, whichever is less, and (B) an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this Act for a surveillance targeted against a foreign power, a defined in paragraph (5), (6), or (7) of section 101(a), or against a foreign power as defined in section 101(a)(4) that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(4) A denial of the application made under section 104 may be reviewed as provided in section 103.

(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—

(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

(D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such electronic surveillance, the surveillance 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 of authorization by the Attorney General, whichever is earliest.

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

(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance 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 surveillance 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).

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

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

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

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

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

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

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

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

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

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

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

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

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

(g) Notwithstanding any other provision of this title, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine to capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and

(D) *Provided,* That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 705 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(h) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained for a period of at least ten years from the date of the certification or application.

(i) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

(j) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2).

* * * * * * *

PENALTIES

SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he **[**intentionally**]**—

(1) *intentionally* engages in electronic surveillance under color of law except as authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112; **[**or**]**

(2) *intentionally* disclose or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112**[**.**]***;*

(3) knowingly submits any document to or makes any false statement before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, knowing such document or statement to contain—

(A) a false material declaration; or

(B) a material omission; or

(4) knowingly discloses the existence of an application for an order authorizing surveillance under this title, or any information contained therein, to any person not authorized to receive such information.

(b) DEFENSE.—It is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic

surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

[(c) PENALTY.—An offense in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.]

(c) PENALTIES.—In the case of an offense under any of paragraphs (1) through (4) of subsection (a), the offense is punishable by a fine of not more than $10,000 or imprisonment for not more than 8 years, or both.

(d) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

* * * * * * *

SEC. 110. CIVIL ACTION.—An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101 (a) or (b)(1)(A), respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 109 shall have a cause of action against any person who committed such violation and shall be entitled to recover—

[(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;]

(a) actual damages, but not less than liquidated damages equal to the greater of—

(1) if the aggrieved person is a United States person, $10,000 or $1,000 per day for each day of violation; or

(2) for any other aggrieved person, $1,000 or $100 per day for each day of violation;

(b) punitive damages; and

(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

SEC. 110A. REPORTING REQUIREMENTS FOR CIVIL ACTIONS.

(a) REPORT TO CONGRESS.—If a court finds that a person has violated this Act in a civil action under section 110, the head of the agency that employs that person shall report to Congress on the administrative action taken against that person pursuant to section 607 or any other provision of law.

(b) FISC.—If a court finds that a person has violated this Act in a civil action under section 110, the head of the agency that employs that person shall report the name of such person to the Foreign Intelligence Surveillance Court. The Foreign Intelligence Surveillance Court shall maintain a list of each person about whom it received a report under this subsection.

* * * * * * *

TITLE VI—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) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for—

(A) electronic surveillance under section 105;

(B) physical searches under section 304;

(C) pen registers under section 402;

(D) access to records under section 501;

(E) acquisitions under section 703; and

(F) acquisitions under section 704;

(2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C);

(3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;

(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.

(b) FREQUENCY.—The first report under this section shall be submitted not later than 6 months after the date of enactment of this section. Subsequent reports under this section shall be submitted semi-annually thereafter.

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

(1) not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues a decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act, a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion*, including declassified copies that have undergone review under section 602*; and

(2) a copy of each such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on the date of the enactment of the FISA Amendments Act of 2008 and not previously submitted in a report under subsection (a).

(d) PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets.

(e) DEFINITIONS.—In this section:

(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term "Foreign Intelligence Surveillance Court" means the court established under section 103(a).

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The term "Foreign Intelligence Surveillance Court of Review" means the court established under section 103(b).

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

(a) DECLASSIFICATION REQUIRED.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review*, to be concluded not later than 45 days after the commencement of such 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 law *or results in a change of application of any provision of this Act or a novel application of any provision of this Act*, including any novel or significant construction or interpretation of the term "specific selection term", and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

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

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

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

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

(A) summarizing the significant construction or interpretation of any provision of law, which shall include, to the extent consistent with national security, a description of the context in which the matter arises and any significant construction or interpretation of any statute, constitutional

provision, or other legal authority relied on by the decision; and

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

SEC. 603. ANNUAL REPORTS.

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

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

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

(B) an analysis of the accuracy and completeness of such applications and certifications submitted;

[(B)] *(C)* the number of such orders granted under each of those sections;

[(C)] *(D)* the number of orders modified under each of those sections;

[(D)] *(E)* the number of applications or certifications denied under each of those sections;

[(E)] *(F)* 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; and

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

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

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

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

(A) the number of targets of such orders;

(B) the number of targets of such orders who are known to not be United States persons; and

(C) the number of targets of such orders who are known to be United States persons;

(2) the total number of orders issued pursuant to section 702, including pursuant to subsection (f)(2) of such section, and a good faith estimate of—

(A) the number of targets of such orders;

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

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

(D) the number of instances in which the Federal Bureau of Investigation opened, under the Criminal Investigative Division or any successor division, an investigation of a United States person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under such section;

(3) a description of the subject matter of each of the certifications provided under section 702(h);

(4) statistics revealing the number of persons and identifiers targeted under section 702(a), disaggregated by certification under which the person or identifier was targeted;

(5) the total number of directives issued pursuant to section 702(i)(1), disaggregated by each type of electronic communication service provider described in subparagraphs (A) through (E) of section 701(b)(4);

[(3)] *(6)* the total number of orders issued pursuant to title IV and a good faith estimate of—

(A) the number of targets of such orders, including—

(i) the number of targets of such orders who are known to not be United States persons; and

(ii) the number of targets of such orders who are known to be United States persons; and

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

[(4)] *(7)* the number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to subsection (c) or (d) of section 106 (including with respect to information acquired from an acquisition conducted under section 702) or subsection (d) or (e) of section 305 of the intent of the government to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or an acquisition conducted pursuant to this Act;

[(5)] *(8)* the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

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

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

[(6)] *(9)* the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

(A) the number of targets of such orders;

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

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

[(7)] *(10)* the total number of national security letters issued and the number of requests for information contained within such national security letters[.]*;*

(11)(A) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons regardless of whether the identities of the United States persons were openly included or masked;

(B) the total number of disseminated intelligence reports derived from collection not authorized by this Act containing the identities of United States persons regardless of whether the identities of the United States persons were openly included or masked;

(C) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were masked;

(D) the total number of disseminated intelligence reports derived from collection not authorized by this Act containing the identities of United States persons in which the identities of the United States persons were masked;

(E) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were openly included; and

(F) the total number of disseminated intelligence reports derived from collection not authorized by this Act containing the identities of United States persons in which the identities of the United States persons were openly included;

(12) the number of queries conducted in an effort to find communications or information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information, where such communications or information were obtained without a court order, subpoena, or other legal process established by statute;

(13) the number of criminal proceedings in which the Federal Government or a government of a State or political subdivision thereof entered into evidence or otherwise used or disclosed in a criminal proceeding any information obtained or derived from an acquisition conducted without a court order, subpoena, or other legal process established by statute; and

(14) a good faith estimate of what percentage of the communications that are subject to the procedures described in section

309(b)(3) of the Intelligence Authorization Act for Fiscal Year 2015 (50 U.S.C. 1813(b)(3))—

(A) are retained for longer than 5 years; and

(B) are retained for longer than 5 years in whole in part because they are encrypted.

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

(d) EXCEPTIONS.—

(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of ⟦paragraphs (3), (5), or (6)⟧ *paragraph (6), (8), or (9)* of subsection (b) is fewer than 500, it shall be expressed as a numerical range of "fewer than 500" and shall not be expressed as an individual number.

⟦(2) NONAPPLICABILITY TO CERTAIN INFORMATION.—

⟦(A) FEDERAL BUREAU OF INVESTIGATION.—Paragraphs (2)(B), (2)(C), and (6)(C) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation, except with respect to information required under paragraph (2) relating to orders issued under section 702(f)(2).

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

⟦(3)⟧ *(2)* CERTIFICATION.—

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

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

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

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

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

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

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

(e) DEFINITIONS.—In this section:

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

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

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

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

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

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

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

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

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

* * * * * * *

SEC. 605. ANNUAL AUDIT OF FISA COMPLIANCE BY INSPECTOR GENERAL.

Beginning with the first calendar year that begins after the effective date of this section, by not later than June 30th of that year and each year thereafter, the Inspector General of the Department of Justice shall conduct an audit on alleged violations and failures to comply with the requirements of this Act and any procedures established pursuant to this Act, and submit a report thereon to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and of the Senate.

SEC. 606. ANNUAL REPORT OF THE FEDERAL BUREAU OF INVESTIGATION.

Not later than 1 year after the date of enactment of this section, and annually thereafter, the Director of the Federal Bureau of Investigation shall submit to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and of the Senate—

(1) a report on disciplinary activities taken by the Director to address violations of the requirements of law or the procedures established under this Act, including a comprehensive account of disciplinary investigations, including—

(A) all such investigations ongoing as of the date the report is submitted;

(B) the adjudications of such investigations when concluded; and

(C) disciplinary actions taken as a result of such adjudications; and

(2) a report on the conduct of queries conducted under section 702 for the preceding year using a United States person query term, including—

(A) the number of such queries conducted;

(B) what terms were used;

(C) the number of warrants issued and denied under section 702(f)(1); and

(D) the number of times exceptions were alleged under 702(f)(2).

SEC. 607. AGENCY PROCEDURES TO ENSURE COMPLIANCE.

The head of each Federal department or agency authorized to acquire foreign intelligence information under this Act shall establish procedures—

(1) setting forth clear rules on what constitutes a violation of this Act by an officer or employee of that department or agency; and

(2) for taking appropriate adverse personnel action against any officer or employee of the department or agency who engages in such a violation, including more severe adverse actions for any subsequent violation.

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) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (j)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

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

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) [may not intentionally] *may not—*

(A) 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 in the United States;] *if a significant purpose of such acquisition is to acquire the information of 1 or more United States persons or persons reasonably believed to be located in the United States at the time of acquisition or communication, unless—*

(i)(I) there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm to such United States person or person reasonably believed to be located in the United States at the time of the query or the time of acquisition or communication;

(II) the information is sought for the purpose of assisting that person; and

(III) a description of the targeting is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress in a timely manner; or

(ii) the United States person or persons reasonably believed to be located in the United States at the time of acquisition or communication has provided consent to the targeting, or if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person has provided consent; and

(B) in the case of information acquired pursuant to subparagraph (A)(i) or evidence derived from such targeting, be used, received in evidence, or otherwise disseminated in any investigation, 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, except in proceedings or investigations that arise from the threat that prompted the targeting;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a)**[**, except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017**]**; and

(6) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) CONDUCT OF ACQUISITION.—

(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (h), such certification.

(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), 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 pursuant to subsection (j)(3) prior to the implementation of such authorization.

(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

(A) before the submission of a certification in accordance with subsection (h); or

(B) by amending a certification pursuant to subsection (j)(1)(C) at any time during which judicial review under subsection (j) of such certification is pending.

(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) TARGETING PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

[(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and]

(A) ensure that—

(i) any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

(ii) except as provided in subsection (b)(2), a significant purpose of an acquisition is not to acquire the information of 1 or more United States persons or persons reasonably believed to be in the United States at the time of acquisition or communication; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (j).

(e) MINIMIZATION PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (j).

(3) PUBLICATION.—The Director of National Intelligence, in consultation with the Attorney General, shall—

(A) conduct a declassification review of any minimization procedures adopted or amended in accordance with paragraph (1); and

(B) consistent with such review, and not later than 180 days after conducting such review, make such minimization procedures publicly available to the greatest extent practicable, which may be in redacted form.

(f) QUERIES.—

(1) PROCEDURES REQUIRED.—

(A) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt querying procedures consistent with the requirements of the fourth amendment to the Constitution of the United States *and the limitations and requirements in*

paragraph (2) for information collected pursuant to an authorization under subsection (a).

(B) RECORD OF UNITED STATES PERSON QUERY TERMS.—The Attorney General, in consultation with the Director of National Intelligence, shall ensure that the procedures adopted under subparagraph (A) include a technical procedure whereby a record is kept of each ⟦United States person query term used for a query⟧ *term for a United States person or person reasonably believed to be in the United States used for a query as required by paragraph (3)*.

(C) JUDICIAL REVIEW.—The procedures adopted in accordance with subparagraph (A) shall be subject to judicial review pursuant to subsection (j).

(D) LIMITATION ON ELIGIBILITY OF FBI PERSONNEL TO CONDUCT UNITED STATES PERSON QUERIES.—The Attorney General shall ensure that the procedures adopted under subparagraph (A) limit the authority to conduct queries such that—

(i) for each field office of the Federal Bureau of Investigation, the most senior official whose primary duty station is that field office is authorized to designate not more than five individuals whose primary duty station is that field office who are eligible to conduct a query using a United States person query term; and

(ii) for the headquarters of the Federal Bureau of Investigation, the Director of the Federal Bureau of Investigation is authorized to designate not more than five individuals whose primary duty station is the Headquarters of the Federal Bureau of Investigation who are eligible to conduct a query using a United States person query term.

⟦(2) ACCESS TO RESULTS OF CERTAIN QUERIES CONDUCTED BY FBI.—

⟦(A) COURT ORDER REQUIRED FOR FBI REVIEW OF CERTAIN QUERY RESULTS IN CRIMINAL INVESTIGATIONS UNRELATED TO NATIONAL SECURITY.—Except as provided by subparagraph (E), in connection with a predicated criminal investigation opened by the Federal Bureau of Investigation that does not relate to the national security of the United States, the Federal Bureau of Investigation may not access the contents of communications acquired under subsection (a) that were retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information unless—

⟦(i) the Federal Bureau of Investigation applies for an order of the Court under subparagraph (C); and

⟦(ii) the Court enters an order under subparagraph (D) approving such application.

⟦(B) JURISDICTION.—The Court shall have jurisdiction to review an application and to enter an order approving the access described in subparagraph (A).

⟦(C) APPLICATION.—Each application for an order under this paragraph shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subparagraph (B). Each application shall require

the approval of the Attorney General based upon the finding of the Attorney General that the application satisfies the criteria and requirements of such application, as set forth in this paragraph, and shall include—

[(i) the identity of the Federal officer making the application; and

[(ii) an affidavit or other information containing a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant that the contents of communications described in subparagraph (A) covered by the application would provide evidence of—

[(I) criminal activity;

[(II) contraband, fruits of a crime, or other items illegally possessed by a third party; or

[(III) property designed for use, intended for use, or used in committing a crime.

[(D) ORDER.—Upon an application made pursuant to subparagraph (C), the Court shall enter an order approving the accessing of the contents of communications described in subparagraph (A) covered by the application if the Court finds probable cause to believe that such contents would provide any of the evidence described in subparagraph (C)(ii).

[(E) EXCEPTION.—The requirement for an order of the Court under subparagraph (A) to access the contents of communications described in such subparagraph shall not apply with respect to a query if the Federal Bureau of Investigation determines there is a reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm.

[(F) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed as—

[(i) limiting the authority of the Federal Bureau of Investigation to conduct lawful queries of information acquired under subsection (a);

[(ii) limiting the authority of the Federal Bureau of Investigation to review, without a court order, the results of any query of information acquired under subsection (a) that was reasonably designed to find and extract foreign intelligence information, regardless of whether such foreign intelligence information could also be considered evidence of a crime; or

[(iii) prohibiting or otherwise limiting the ability of the Federal Bureau of Investigation to access the results of queries conducted when evaluating whether to open an assessment or predicated investigation relating to the national security of the United States.]

(2) PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS AND OTHER INFORMATION OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.—

(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C), no officer or employee of the United States may conduct a query of information acquired under this section in an effort to find communications or information the com-

pelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States, of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information.

(B) EXCEPTIONS FOR CONCURRENT AUTHORIZATION, CONSENT, EMERGENCY SITUATIONS, AND CERTAIN DEFENSIVE CYBERSECURITY QUERIES.—

(i) IN GENERAL.—Subparagraph (A) shall not apply to a query related to a United States person or person reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information if—

(I) such person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105 or 304 of this Act, or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction authorizing the conduct of the query;

(II)(aa) the officer or employee carrying out the query has a reasonable belief that—

(AA) an emergency exists involving an imminent threat of death or serious bodily harm; and

(BB) in order to prevent or mitigate this threat, the query must be conducted before authorization pursuant to subparagraph (I) can, with due diligence, be obtained; and

(bb) a description of the query is provided to the Foreign Intelligence Surveillance Court and the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and of the Senate in a timely manner;

(III) such person or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person, has provided consent to the query on a case-by-case basis; or

(IV)(aa) the query uses a known cybersecurity threat signature as a query term;

(bb) the query is conducted, and the results of the query are used, for the sole purpose of identifying targeted recipients of malicious software and preventing or mitigating harm from such malicious software;

(cc) no additional contents of communications retrieved as a result of the query are accessed or reviewed; and

(dd) all such queries are reported to the Foreign Intelligence Surveillance Court.

(ii) LIMITATIONS.—

(I) USE IN SUBSEQUENT PROCEEDINGS AND INVESTIGATIONS.—No information retrieved pursuant to a query authorized by clause (i)(II) or informa-

tion derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, 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, except in proceedings or investigations that arise from the threat that prompted the query.

(II) ASSESSMENT OF COMPLIANCE.—The Attorney General shall not less frequently than annually assess compliance with the requirements under subclause (I).

(C) MATTERS RELATING TO EMERGENCY QUERIES.—

(i) TREATMENT OF DENIALS.—In the event that a query for communications or information, the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States, of or about 1 more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information is conducted pursuant to an emergency authorization described in subparagraph (B)(i)(I) and the application for such emergency authorization is denied, or in any other case in which the query has been conducted and no order is issued approving the query—

(I) no information obtained or evidence derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, 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

(II) no information concerning any United States person or person reasonably believed to be located in the United States at the time of the query or the time of the communication or the creation of the information acquired from such query may subsequently be used or disclosed in any other manner 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.

(ii) ASSESSMENT OF COMPLIANCE.—The Attorney General shall not less frequently than annually assess compliance with the requirements under clause (i).

(D) FOREIGN INTELLIGENCE PURPOSE.—Except as provided in subparagraph (B)(i), no officer or employee of the United States may conduct a query of information acquired under this section in an effort to find information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation

of the information unless the query is reasonably likely to retrieve foreign intelligence information.

(3) DOCUMENTATION.—No officer or employee of the United States may conduct a query of information acquired under this section in an effort to find information of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of query or the time of the communication or the creation of the information, unless first an electronic record is created, and a system, mechanism, or business practice is in place to maintain such record, that includes the following:

(A) Each term used for the conduct of the query.

(B) The date of the query.

(C) The identifier of the officer or employee.

(D) A statement of facts showing that the use of each query term included under subparagraph (A) is—

(i) reasonably likely to retrieve foreign intelligence information; or

(ii) in furtherance of the exceptions described in paragraph (2)(B)(i).

(4) PROHIBITION ON RESULTS OF METADATA QUERY AS A BASIS FOR ACCESS TO COMMUNICATIONS AND OTHER PROTECTED INFORMATION.—If a query of information acquired under this section is conducted in an effort to find communications metadata of 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or communication and the query returns such metadata, the results of the query shall not be used as a basis for reviewing communications or information a query for which is otherwise prohibited under this section.

(5) FEDERATED DATASETS.—The prohibitions and requirements in this section shall apply to queries of federated and mixed datasets that include information acquired under this section, unless a mechanism exists to limit the query to information not acquired under this section.

[(3)**]** *(6)* DEFINITIONS.—In this subsection:

(A) The term "contents" has the meaning given that term in section 2510(8) of title 18, United States Code.

(B) The term "query" means the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under subsection (a).

(g) GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

(A) compliance with the limitations in subsection (b); and

(B) that an application for a court order is filed as required by this Act.

(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

(A) the congressional intelligence committees;

(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

(C) the Foreign Intelligence Surveillance Court.

(h) CERTIFICATION.—

(1) IN GENERAL.—

(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) REQUIREMENTS.—A certification made under this subsection shall—

(A) attest that—

(i) there are targeting procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

[(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and]

(I) ensure that—

(aa) an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United States persons located outside the United States; and

(bb) except as provided in subsection (b)(2), a significant purpose of an acquisition is not to acquire the information of 1 or more United States persons or persons reasonably believed to be in the United States at the time of acquisition or communication; and

(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(ii) the minimization procedures to be used with respect to such acquisition—

(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(II) have been approved, have been submitted for approval, or will be submitted with the certifi-

cation for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (g) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;

(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);

(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

(i) appointed by the President, by and with the advice and consent of the Senate; or

(ii) the head of an element of the intelligence community;

(D) include—

(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (j)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (j).

(i) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) CHALLENGING OF DIRECTIVES.—

(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) ENFORCEMENT OF DIRECTIVES.—

(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) APPEAL.—

(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(j) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

(1) IN GENERAL.—

(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1), and amendments to such certification or such procedures.

(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

(2) REVIEW.—The Court shall review the following:

(A) CERTIFICATION.—A certification submitted in accordance with subsection (h) to determine whether the certification contains all the required elements.

(B) TARGETING PROCEDURES.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—

[(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and**]**

(i) ensure that—

(I) an acquisition authorized under subsection (a) is limited to targeting persons reasonably be-

lieved to be non-United States persons located outside the United States; and

(II) except as provided in subsection (b)(2), a significant purpose of an acquisition is not to acquire the information of 1 or more United States persons or persons reasonably believed to be in the United States at the time of acquisition or communication; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) MINIMIZATION PROCEDURES.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.

(D) QUERYING PROCEDURES.—The querying procedures adopted in accordance with subsection (f)(1) to assess whether such procedures comply with the requirements of such subsection.

(3) ORDERS.—

(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (h) contains all the required elements and that the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification submitted in accordance with subsection (h) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d), (e), and (f)(1) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(D) LIMITATION ON USE OF INFORMATION.—

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

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

(4) APPEAL.—

(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue—

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted

under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) SCHEDULE.—

(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (h) and the procedures adopted in accordance with subsections (d), (e), and (f)(1) at least 30 days prior to the expiration of such authorization.

(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(k) JUDICIAL PROCEEDINGS.—

(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(l) MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(m) ASSESSMENTS [REVIEWS, AND REPORTING] *AND REVIEWS*.—

(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting, mini-

mization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and the guidelines adopted in accordance with subsection (g) and shall submit each assessment to—

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

(A) are authorized to review compliance with the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and the guidelines adopted in accordance with subsection (g);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to—

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) ANNUAL REVIEW.—

(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

[(4) REPORTING OF MATERIAL BREACH.—

[(A) IN GENERAL.—The head of each element of the intelligence community involved in the acquisition of abouts communications shall fully and currently inform the Committees on the Judiciary of the House of Representatives and the Senate and the congressional intelligence committees of a material breach.

[(B) DEFINITIONS.—In this paragraph:

[(i) The term "abouts communication" means a communication that contains a reference to, but is not to or from, a target of an acquisition authorized under subsection (a).

[(ii) The term "material breach" means significant noncompliance with applicable law or an order of the Foreign Intelligence Surveillance Court concerning any acquisition of abouts communications.]

* * * * * * *

SEC. 706. USE OF INFORMATION ACQUIRED UNDER TITLE VII.

(a) INFORMATION ACQUIRED UNDER SECTION 702.—

(1) IN GENERAL.—Information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106, except for the purposes of subsection (j) of such section.

[(2) UNITED STATES PERSONS.—

[(A) IN GENERAL.—Any information concerning a United States person acquired under section 702 shall not be used in evidence against that United States person pursuant to paragraph (1) in any criminal proceeding unless—

[(i) the Federal Bureau of Investigation obtained an order of the Foreign Intelligence Surveillance Court to access such information pursuant to section 702(f)(2); or

[(ii) the Attorney General determines that—

[(I) the criminal proceeding affects, involves, or is related to the national security of the United States; or

[(II) the criminal proceeding involves—

[(aa) death;

[(bb) kidnapping;

[(cc) serious bodily injury, as defined in section 1365 of title 18, United States Code;

[(dd) conduct that constitutes a criminal offense that is a specified offense against a minor, as defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006 (34 U.S.C. 20911);

[(ee) incapacitation or destruction of critical infrastructure, as defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e));

[(ff) cybersecurity, including conduct described in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)) or section 1029, 1030, or 2511 of title 18, United States Code;

[(gg) transnational crime, including transnational narcotics trafficking and transnational organized crime; or

[(hh) human trafficking.

[(B) NO JUDICIAL REVIEW.—A determination by the Attorney General under subparagraph (A)(ii) is not subject to judicial review.]

(2) LIMITATION ON USE IN CRIMINAL, CIVIL, AND ADMINISTRATIVE PROCEEDINGS AND INVESTIGATIONS.—No information acquired pursuant to section 702(f) of or about a United States person or person reasonably believed to be located in the United

States at the time of acquisition or communication may be introduced as evidence against such person in any criminal, civil, or administrative proceeding or used as part of any criminal, civil, or administrative investigation, except—

(A) with the prior approval of the Attorney General; and

(B) in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat of—

(i) the commission of a Federal crime of terrorism under any of clauses (i) through (iii) of section 2332b(g)(5)(B) of title 18, United States Code;

(ii) actions necessitating counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003));

(iii) the proliferation or the use of a weapon of mass destruction (as defined in section 2332a(c) of title 18, United States Code);

(iv) a cybersecurity breach or attack from a foreign country;

(v) incapacitation or destruction of critical infrastructure (as defined in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)));

(vi) an attack against the armed forces of the United States or an ally of the United States or to other personnel of the United States Government or a government of an ally of the United States; or

(vii) international narcotics trafficking.

(b) INFORMATION ACQUIRED UNDER SECTION 703.—Information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106.

SEC. 707. CONGRESSIONAL OVERSIGHT.

(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, concerning the implementation of this title.

(b) CONTENT.—Each report under subsection (a) shall include—

(1) with respect to section 702—

(A) any certifications submitted in accordance with section 702(h) during the reporting period;

(B) with respect to each determination under section 702(c)(2), the reasons for exercising the authority under such section;

(C) any directives issued under section 702(i) during the reporting period;

(D) a description of the judicial review during the reporting period of such certifications and targeting and minimization procedures adopted in accordance with sub-

sections (d) and (e) of section 702 and utilized with respect to an acquisition under such section, including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of section 702;

(E) any actions taken to challenge or enforce a directive under paragraph (4) or (5) of section 702(i);

(F) any compliance reviews conducted by the Attorney General or the Director of National Intelligence of acquisitions authorized under section 702(a);

(G) a description of any incidents of noncompliance—

(i) with a directive issued by the Attorney General and the Director of National Intelligence under section 702(i), including incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under section 702(i); and

(ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with subsections (d), (e), (f)(1), and (g) of section 702; and

(H) any procedures implementing section 702;

(2) with respect to section 703—

(A) the total number of applications made for orders under section 703(b);

(B) the total number of such orders—

(i) granted;

(ii) modified; and

(iii) denied; and

(C) the total number of emergency acquisitions authorized by the Attorney General under section 703(d) and the total number of subsequent orders approving or denying such acquisitions; and

(3) with respect to section 704—

(A) the total number of applications made for orders under section 704(b);

(B) the total number of such orders—

(i) granted;

(ii) modified; and

(iii) denied; and

(C) the total number of emergency acquisitions authorized by the Attorney General under section 704(d) and the total number of subsequent orders approving or denying such applications.

(c) QUARTERLY REPORT.—The Attorney General, in consultation with the Director of National Intelligence, shall submit a report, each quarter, to the congressional intelligence committees and to the Committees on the Judiciary of the Senate and of the House of Representatives, which shall include, for that quarter, the following:

(1) The total number of warrants issued to conduct a query of information acquired under section 702.

(2) The total number of times a query was conducted pursuant to an exception under section 702(f)(2)(B) and which exceptions applied.

(3) The total number of queries of information acquired under section 702 that were conducted using a United States person query term or a query term pertaining to a person reasonably believed to be present in the United States as of the date such query was conducted, disaggregated by the agency that conducted the queries.

* * * * * * *

SEC. 709. ACCOUNTABILITY PROCEDURES FOR INCIDENTS RELATING TO QUERIES CONDUCTED BY THE FEDERAL BUREAU OF INVESTIGATION.

(a) IN GENERAL.—The Director of the Federal Bureau of Investigation shall establish procedures to hold employees of the Federal Bureau of Investigation accountable for violations of law, guidance, and procedure governing queries of information acquired pursuant to section 702.

(b) ELEMENTS.—The procedures established under subsection (a) shall include the following:

(1) Centralized tracking of individual employee performance incidents involving negligent violations of law, guidance, and procedure described in subsection (a), over time.

(2) Escalating consequences for such incidents, including—

(A) consequences for initial incidents, including, at a minimum—

(i) suspension of access to information acquired under this Act; and

(ii) documentation of the incident in the personnel file of each employee responsible for the violation; and

(B) consequences for subsequent incidents, including, at a minimum—

(i) possible indefinite suspension of access to information acquired under this Act;

(ii) reassignment of each employee responsible for the violation; and

(iii) referral of the incident to the Inspection Division of the Federal Bureau of Investigation for review of potentially reckless conduct.

(3) Clarification of requirements for referring intentional misconduct and reckless conduct to the Inspection Division of the Federal Bureau of Investigation for investigation and disciplinary action by the Office of Professional Responsibility of the Federal Bureau of Investigation.

* * * * * * *

TITLE IX—CERTIFICATION REGARDING ACCURACY PROCEDURES

SEC. 901. CERTIFICATION REGARDING ACCURACY PROCEDURES.

(a) DEFINITION OF ACCURACY PROCEDURES.—In this section, the term "accuracy procedures" means specific procedures, adopted by the Attorney General, to ensure that an application for a court order under this Act, including any application for renewal of an existing order, is accurate and complete, including procedures that ensure, at a minimum, that—

(1) the application reflects all information that might reasonably call into question the accuracy of the information or the reasonableness of any assessment in the application, or otherwise raises doubts about the requested findings;

(2) the application reflects all material information that might reasonably call into question the reliability and reporting of any information from a confidential human source that is used in the application;

(3) a complete file documenting each factual assertion in an application is maintained;

(4) the applicant coordinates with the appropriate elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), concerning any prior or existing relationship with the target of any surveillance, search, or other means of investigation, and discloses any such relationship in the application;

(5) before any application targeting a United States person is made, the applicant Federal officer shall document that the officer has collected and reviewed for accuracy and completeness supporting documentation for each factual assertion in the application; and

(6) the applicant Federal agency establish compliance and auditing mechanisms on an annual basis to assess the efficacy of the accuracy procedures that have been adopted and report such findings to the Attorney General.

(b) STATEMENT AND CERTIFICATION OF ACCURACY PROCEDURES.—Any Federal officer making an application for a court order under this Act shall include with the application—

(1) a description of the accuracy procedures employed by the officer or the officer's designee; and

(2) a certification that the officer or the officer's designee has collected and reviewed for accuracy and completeness—

(A) supporting documentation for each factual assertion contained in the application;

(B) all information that might reasonably call into question the accuracy of the information or the reasonableness of any assessment in the application, or otherwise raises doubts about the requested findings; and

(C) all material information that might reasonably call into question the reliability and reporting of any information from any confidential human source that is used in the application.

(c) NECESSARY FINDING FOR COURT ORDERS.—A judge may not enter an order under this Act unless the judge finds, in addition to any other findings required under this Act, that the accuracy procedures described in the application for the order, as required under subsection (b)(1), are actually accuracy procedures as defined in this section.

FISA AMENDMENTS REAUTHORIZATION ACT OF 2017

* * * * * * *

TITLE I—ENHANCEMENTS TO FOREIGN INTELLIGENCE COLLECTION AND SAFEGUARDS, ACCOUNTABILITY, AND OVERSIGHT

* * * * * * *

SEC. 103. CONGRESSIONAL REVIEW AND OVERSIGHT OF ABOUTS COLLECTION.

[(a) IN GENERAL.—]Section 702(b) (50 U.S.C. 1881a(b)) is amended—

(1) in paragraph (4), by striking "and" at the end;

(2) by redesignating paragraph (5) as paragraph (6); and

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

"(5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and".

[(b) CONGRESSIONAL REVIEW AND OVERSIGHT OF ABOUTS COLLECTION.—

[(1) DEFINITIONS.—In this subsection:

[(A) The term "abouts communication" means a communication that contains a reference to, but is not to or from, a target of an acquisition authorized under section 702(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(a)).

[(B) The term "material breach" means significant noncompliance with applicable law or an order of the Foreign Intelligence Surveillance Court concerning any acquisition of abouts communications.

[(2) SUBMISSION TO CONGRESS.—

[(A) REQUIREMENT.—Notwithstanding any other provision of law, and except as provided in paragraph (4), if the Attorney General and the Director of National Intelligence intend to implement the authorization of the intentional acquisition of abouts communications, before the first such implementation after the date of enactment of this Act, the Attorney General and the Director of National Intelligence 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 written notice of the intent to implement the authorization of such an acquisition, and any supporting materials in accordance with this subsection.

[(B) CONGRESSIONAL REVIEW PERIOD.—During the 30-day period beginning on the date written notice is submitted under subparagraph (A), 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 shall, as appropriate, hold hearings and

briefings and otherwise obtain information in order to fully review the written notice.

[(C) LIMITATION ON ACTION DURING CONGRESSIONAL REVIEW PERIOD.—Notwithstanding any other provision of law, and subject to paragraph (4), unless the Attorney General and the Director of National Intelligence make a determination pursuant to section 702(c)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(c)(2)), the Attorney General and the Director of National Intelligence may not implement the authorization of the intentional acquisition of abouts communications before the end of the period described in subparagraph (B).

[(3) WRITTEN NOTICE.—Written notice under paragraph (2)(A) shall include the following:

[(A) A copy of any certification submitted to the Foreign Intelligence Surveillance Court pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a), or amendment thereto, authorizing the intentional acquisition of abouts communications, including all affidavits, procedures, exhibits, and attachments submitted therewith.

[(B) The decision, order, or opinion of the Foreign Intelligence Surveillance Court approving such certification, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion.

[(C) A summary of the protections in place to detect any material breach.

[(D) Data or other results of modeling, simulation, or auditing of sample data demonstrating that any acquisition method involving the intentional acquisition of abouts communications shall be conducted in accordance with title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.), if such data or other results exist at the time the written notice is submitted and were provided to the Foreign Intelligence Surveillance Court.

[(E) Except as provided under paragraph (4), a statement that no acquisition authorized under subsection (a) of such section 702 shall include the intentional acquisition of an abouts communication until after the end of the 30-day period described in paragraph (2)(B).

[(4) EXCEPTION FOR EMERGENCY ACQUISITION.—

[(A) NOTICE OF DETERMINATION.—If the Attorney General and the Director of National Intelligence make a determination pursuant to section 702(c)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(c)(2)) with respect to the intentional acquisition of abouts communications, the Attorney General and the Director of National Intelligence shall notify 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 as soon as practicable, but not later than 7 days after the determination is made.

[(B) IMPLEMENTATION OR CONTINUATION.—

[(i) IN GENERAL.—If the Foreign Intelligence Surveillance Court approves a certification that authorizes the intentional acquisition of abouts communications before the end of the 30-day period described in paragraph (2)(B), the Attorney General and the Director of National Intelligence may authorize the immediate implementation or continuation of that certification if the Attorney General and the Director of National Intelligence jointly determine that exigent circumstances exist such that without such immediate implementation or continuation intelligence important to the national security of the United States may be lost or not timely acquired.

[(ii) NOTICE.—The Attorney General and the Director of National Intelligence 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 notification of a determination pursuant to clause (i) as soon as practicable, but not later than 3 days after the determination is made.

[(5) REPORTING OF MATERIAL BREACH.—Subsection (m) of section 702 (50 U.S.C. 1881a), as redesignated by section 101, is amended—

[(A) in the heading by striking "and Reviews" and inserting "Reviews, and Reporting"; and

[(B) by adding at the end the following new paragraph:

["(4) REPORTING OF MATERIAL BREACH.—

["(A) IN GENERAL.—The head of each element of the intelligence community involved in the acquisition of abouts communications shall fully and currently inform the Committees on the Judiciary of the House of Representatives and the Senate and the congressional intelligence committees of a material breach.

["(B) DEFINITIONS.—In this paragraph:

["(i) The term 'abouts communication' means a communication that contains a reference to, but is not to or from, a target of an acquisition authorized under subsection (a).

["(ii) The term 'material breach' means significant noncompliance with applicable law or an order of the Foreign Intelligence Surveillance Court concerning any acquisition of abouts communications.".

[(6) APPOINTMENT OF AMICI CURIAE BY FOREIGN INTELLIGENCE SURVEILLANCE COURT.—For purposes of section 103(i)(2)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)(A)), the Foreign Intelligence Surveillance Court shall treat the first certification under section 702(h) of such Act (50 U.S.C. 1881a(h)) or amendment thereto that authorizes the acquisition of abouts communications as presenting a novel or significant interpretation of the law, unless the court determines otherwise.]

* * * * * * *

FISA AMENDMENTS ACT OF 2008

* * * * * * *

TITLE IV—OTHER PROVISIONS

* * * * * * *

SEC. 403. REPEALS.

(a) REPEAL OF PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) AMENDMENTS TO FISA.—

(A) IN GENERAL.—Except as provided in section 404, sections 105A, 105B, and 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805a, 1805b, and 1805c) are repealed.

(B) TECHNICAL AND CONFORMING AMENDMENTS.—

(i) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to sections 105A, 105B, and 105C.

(ii) CONFORMING AMENDMENTS.—Except as provided in section 404, section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(I) in paragraph (1), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)"; and

(II) in paragraph (2), by striking "105B(h) or 501(f)(1)" and inserting "501(f)(1) or 702(h)(4)".

(2) REPORTING REQUIREMENTS.—Except as provided in section 404, section 4 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 555) is repealed.

(3) TRANSITION PROCEDURES.—Except as provided in section 404, subsection (b) of section 6 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556) is repealed.

(b) FISA AMENDMENTS ACT OF 2008.—

(1) IN GENERAL.—Except as provided in section 404, effective [December 31, 2023] *December 31, 2026*, title VII of the Foreign Intelligence Surveillance Act of 1978[, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017,], *as most recently amended,* is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Effective [December 31, 2023] *December 31, 2026*—

(A) the table of contents in the first section of such Act (50 U.S.C. 1801 et seq.) is amended by striking the items related to title VII;

(B) except as provided in section 404, section 601(a)(1) of such Act (50 U.S.C. 1871(a)(1)) is amended to read as such section read on the day before the date of the enactment of this Act; and

(C) except as provided in section 404, section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by striking "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978".

SEC. 404. TRANSITION PROCEDURES.

(a) TRANSITION PROCEDURES FOR PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and

(B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—

(i) the expiration of such order, authorization, or directive; or

(ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(4) PROTECTION FROM LIABILITY.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.

(5) JURISDICTION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—

(A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(6) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act, any amendment made by this Act, the Protect America Act of 2007 (Public Law 110-55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;

(iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, after the date of such certification; and

(iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been included in a semi-annual report required by such section 4.

(7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

(A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.

(B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expira-

tion provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification under section 702(j)(3) of such Act (as so added) at which time the provisions of that section and of section 702(j)(4) of such Act (as so added) shall apply.

(8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.

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

(1) ORDERS IN EFFECT ON [DECEMBER 31, 2023] *DECEMBER 31, 2026*.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978[, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017,] *as most recently amended,* shall continue in effect until the date of the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or directive referred to in paragraph (1), title VII of such Act[, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017,] *as most recently amended,* shall continue to apply until the later of—

(A) the expiration of such order, authorization, or directive; or

(B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant to section 702(i) of such Act, as added by section 101(a);

(B) section 702(i)(3) of such Act (as so added) shall continue to apply with respect to any directive issued pursuant to section 702(i) of such Act (as so added);

(C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;

(D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and

(E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to

apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).

(4) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by section 101(c)(2), and sections 702(m) and 707 of such Act[, as added by section 101(a) and amended by the FISA Amendments Reauthorization Act of 2017,] *, as added by section 101(a) and as most recently amended,* shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;

(iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978[, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017,] *, as most recently amended,* after the date of such certification; and

(iv) that states that the information required to be included in a review, assessment, or report under section 601 of such Act, as amended by section 101(c), or section 702(m) or 707 of such Act[, as added by section 101(a) and amended by the FISA Amendments Reauthorization Act of 2017,] *, as added by section 101(a) and as most recently amended,* relating to any acquisition conducted under title VII of such Act[, as amended by section 101(a) and by the FISA Amendments Reauthorization Act of 2017,] *, as most recently amended,* has been included in a review, assessment, or report under such section 601, 702(l), or 707.

(5) TRANSITION PROCEDURES CONCERNING THE TARGETING OF UNITED STATES PERSONS OVERSEAS.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

TITLE 18, UNITED STATES CODE

PART I—CRIMES

* * * * * * *

CHAPTER 21—CONTEMPTS

§ 402. Contempts constituting crimes

Any person, corporation or association willfully disobeying any lawful writ, process, order, rule, decree, or command of any district court of the United States*, the Foreign Intelligence Surveillance Court, the Foreign Intelligence Surveillance Court of Review,* or any court of the District of Columbia, by doing any act or thing therein, or thereby forbidden, if the act or thing so done be of such character as to constitute also a criminal offense under any statute of the United States or under the laws of any State in which the act was committed, shall be prosecuted for such contempt as provided in section 3691 of this title and shall be punished by a fine under this title or imprisonment, or both.

Such fine shall be paid to the United States or to the complainant or other party injured by the act constituting the contempt, or may, where more than one is so damaged, be divided or apportioned among them as the court may direct, but in no case shall the fine to be paid to the United States exceed, in case the accused is a natural person, the sum of $1,000, nor shall such imprisonment exceed the term of six months.

This section shall not be construed to relate to contempts committed in the presence of the court, or so near thereto as to obstruct the administration of justice, nor to contempts committed in disobedience of any lawful writ, process, order, rule, decree, or command entered in any suit or action brought or prosecuted in the name of, or on behalf of, the United States, but the same, and all other cases of contempt not specifically embraced in this section may be punished in conformity to the prevailing usages at law.

For purposes of this section, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

* * * * * * *

§ 404. Definitions

For purposes of this chapter—

(1) the term "court of the United States" includes the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review; and

(2) the terms "Foreign Intelligence Surveillance Court" and "Foreign Intelligence Surveillance Court of Review" have the

meanings given such terms in section 601(e) of the Foreign Intelligence Surveillance Act of 1978.

* * * * * * *

CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

* * * * * * *

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or elec-

tronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

[(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,]

(B) a certification in writing—

(I) by a person specified in section 2518(7) or the Attorney General of the United States;

(II) that the requirements for an emergency authorization to intercept a wire, oral, or electronic communication under section 2518(7) have been met; and

(III) that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, of-

ficer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

[(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.]

(iii) For assistance provided pursuant to a certification under subparagraph (ii)(B), the limitation on causes of action under the last sentence of the matter following subparagraph (ii)(B) shall only apply to the extent that the assistance ceased at the earliest of the time the application for a court order was denied, the time the communication sought was obtained, or 48 hours after the interception began.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

[(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.]

(f)(i)(A) Nothing contained in this chapter, chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934 (47 U.S.C. 151 et seq.) shall be deemed to affect an acquisition or activity described in clause (B) that is carried out utilizing a means other than electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(B) An acquisition or activity described in this clause is—

(I) an acquisition by the United States Government of foreign intelligence information from international or foreign communications that—

(aa) is acquired pursuant to express statutory authority; or

(bb) only includes information of persons who are not United States persons and are located outside the United States; or

(II) a foreign intelligence activity involving a foreign electronic communications system that—

(aa) is conducted pursuant to express statutory authority; or

(bb) only involves the acquisition by the United States Government of information of persons who are not United States persons and are located outside the United States.

(ii) The procedures in this chapter, chapter 121, and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote

computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a) (i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules

of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

* * * * * * *

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

* * * * * * *

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; **[**and**]**

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; **[**and**]**

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or

customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity**[**.**]***; and*

(4) an intermediary service provider shall not knowingly divulge—

(A) to any person or entity the contents of a communication while in electronic storage by that provider; or

(B) to any governmental entity a record or other information pertaining to a subscriber to or customer of, a recipient of a communication from a subscriber to or customer of, or the sender of a communication to a subscriber to or customer of, the provider of electronic communication service to the public or the provider of remote computing service for, or on behalf of, which the intermediary service provider directly or indirectly delivers, transmits, stores, or processes communications.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(6) to any person other than a governmental entity; or

(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

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

(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR ANYTHING OF VALUE CERTAIN RECORDS AND INFORMATION BY LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.—

(1) DEFINITIONS.—In this subsection—

(A) the term "covered customer or subscriber record" means a covered record that is—

(i) disclosed to a third party by—

(I) a provider of an electronic communication service to the public or a provider of a remote computing service of which the covered person with respect to the covered record is a subscriber or customer; or

(II) an intermediary service provider that delivers, stores, or processes communications of such covered person;

(ii) collected by a third party from an online account of a covered person; or

(iii) collected by a third party from or about an electronic device of a covered person;

(B) the term "covered person" means—

(i) a person who is located inside the United States; or

(ii) a person—

(I) who is located outside the United States or whose location cannot be determined; and

(II) who is a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(C) the term "covered record" means a record or other information that—

(i) pertains to a covered person; and

(ii) is—

(I) a record or other information described in the matter preceding paragraph (1) of subsection (c);

(II) the contents of a communication; or

(III) location information;

(D) the term "electronic device" has the meaning given the term "computer" in section 1030(e);

(E) the term "illegitimately obtained information" means a covered record that—

(i) was obtained—

(I) from a provider of an electronic communication service to the public or a provider of a remote computing service in a manner that—

(aa) violates the service agreement between the provider and customers or subscribers of the provider; or

(bb) is inconsistent with the privacy policy of the provider;

(II) by deceiving the covered person whose covered record was obtained; or

(III) through the unauthorized accessing of an electronic device or online account; or

(ii) was—

(I) obtained from a provider of an electronic communication service to the public, a provider of a remote computing service, or an intermediary service provider; and

(II) collected, processed, or shared in violation of a contract relating to the covered record;

(F) 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);

(G) the term "location information" means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, or device;

(H) the term "obtain in exchange for anything of value" means to obtain by purchasing, to receive in connection with services being provided for consideration, or to otherwise obtain in exchange for consideration, including an access fee, service fee, maintenance fee, or licensing fee;

(I) the term "online account" means an online account with an electronic communication service to the public or remote computing service;

(J) the term "pertain", with respect to a person, means—

(i) information that is linked to the identity of a person; or

(ii) information—

(I) that has been anonymized to remove links to the identity of a person; and

(II) that, if combined with other information, could be used to identify a person; and

(K) the term "third party" means a person who—

(i) is not a governmental entity; and

(ii) in connection with the collection, disclosure, obtaining, processing, or sharing of the covered record at issue, was not acting as—

(I) a provider of an electronic communication service to the public; or

(II) a provider of a remote computing service.

(2) LIMITATION.—

(A) IN GENERAL.—A law enforcement agency of a governmental entity and an element of the intelligence community may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information.

(B) INDIRECTLY ACQUIRED RECORDS AND INFORMATION.—The limitation under subparagraph (A) shall apply without regard to whether the third party possessing the covered customer or subscriber record or illegitimately obtained information is the third party that initially obtained or collected, or is the third party that initially received the disclosure of, the covered customer or subscriber record or illegitimately obtained information.

(3) LIMIT ON SHARING BETWEEN AGENCIES.—An agency of a governmental entity that is not a law enforcement agency or an element of the intelligence community may not provide to a law enforcement agency of a governmental entity or an element of the intelligence community a covered customer or subscriber record or illegitimately obtained information that was obtained from a third party in exchange for anything of value.

(4) PROHIBITION ON USE AS EVIDENCE.—A covered customer or subscriber record or illegitimately obtained information obtained by or provided to a law enforcement agency of a governmental entity or an element of the intelligence community in violation of paragraph (2) or (3), and any evidence derived therefrom, may not be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

(5) MINIMIZATION PROCEDURES.—

(A) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of information pertaining to a covered person that is acquired in violation of paragraph (2) or (3).

(B) USE BY AGENCIES.—If a law enforcement agency of a governmental entity or element of the intelligence community acquires information pertaining to a covered person in

violation of paragraph (2) or (3), the law enforcement agency of a governmental entity or element of the intelligence community shall minimize the acquisition and retention, and prohibit the dissemination, of the information in accordance with the procedures adopted under subparagraph (A).

§ 2703. Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission

from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that

is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

(1) DEFINITIONS.—In this subsection—

(A) the term "qualifying foreign government" means a foreign government—

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) MOTIONS TO QUASH OR MODIFY.—(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication

service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

(iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) COMITY ANALYSIS.—For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

(E) the nature and extent of the provider's ties to and presence in the United States;

(F) the importance to the investigation of the information required to be disclosed;

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) DISCLOSURE OBLIGATIONS DURING PENDENCY OF CHALLENGE.—A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) DISCLOSURE TO QUALIFYING FOREIGN GOVERNMENT.—(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.

(i) COVERED CUSTOMER OR SUBSCRIBER RECORDS AND ILLEGITIMATELY OBTAINED INFORMATION.—

(1) DEFINITIONS.—In this subsection, the terms "covered customer or subscriber record", "illegitimately obtained information", and "third party" have the meanings given such terms in section 2702(e).

(2) LIMITATION.—Unless a governmental entity obtains an order in accordance with paragraph (3), the governmental entity may not require a third party to disclose a covered customer or subscriber record or any illegitimately obtained information if a court order would be required for the governmental entity to require a provider of remote computing service or a provider of electronic communication service to the public to disclose such a covered customer or subscriber record or illegitimately obtained information that is a record of a customer or subscriber of the provider.

(3) ORDERS.—

(A) IN GENERAL.—A court may only issue an order requiring a third party to disclose a covered customer or subscriber record or any illegitimately obtained information on the same basis and subject to the same limitations as would apply to a court order to require disclosure by a provider of remote computing service or a provider of electronic communication service to the public of a record of a customer or subscriber of the provider.

(B) STANDARD.—For purposes of subparagraph (A), a court shall apply the most stringent standard under Federal statute or the Constitution of the United States that would be applicable to a request for a court order to require

a comparable disclosure by a provider of remote computing service or a provider of electronic communication service to the public of a record of a customer or subscriber of the provider.

* * * * * * *

§ 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title;

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; or

(C) a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice) to which a military judge has been detailed; **[**and**]**

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof**[**.**]***; and*

(5) the term "intermediary service provider" means an entity or facilities owner or operator that directly or indirectly delivers, stores, or processes communications for or on behalf of a provider of electronic communication service to the public or a provider of remote computing service.

* * * * * * *

○