IN THE HOUSE OF REPRESENTATIVES

DECEMBER 4, 2023

Mr. Biggs (for himself, Mr. Nadler, Mr. Jordan, Ms. Jayapal, Mr. Davidson, Ms. Jacobs, and Mr. Fry) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Permanent Select Committee on Intelligence, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

DECEMBER 11, 2023

Additional sponsors: Mr. Lieu, Mr. Crane, Ms. Norton, Ms. Hoyle of Oregon, Ms. Lofgren, Mr. Tiffany, Ms. Schakowsky, Mr. Gooden of Texas, Ms. Lee of California, Mr. McClintock, Mr. Roy, Mr. Duncan, Mr. Doggett, Mr. Collins, Ms. Tlaib, Ms. Mace, Mr. Casar, Mr. Burlison, Mr. Good of Virginia, Mr. Bishop of North Carolina, Mr. Van Drew, Mr. Weber of Texas, Ms. Hageman, Mr. Blumenauer, Mr. Mooney, Ms. Chu, and Ms. Porter.

DECEMBER 11, 2023

Reported from the Committee on the Judiciary with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

DECEMBER 11, 2023

Permanent Select Committee on Intelligence discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed.

To amend the Foreign Intelligence Surveillance Act of 1978 to reform certain authorities and to provide greater transparency and oversight.
To amend the Foreign Intelligence Surveillance Act of 1978 to reform certain authorities and to provide greater transparency and oversight.
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

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

VerDate Sep 11 2014 00:50 Dec 12, 2023 Jkt 049200 PO 00000 Frm 00003 Fmt 6652 Sfmt 6203 E:\BILLS\H6570.RH H6570kjohnson on DSK7ZCZBW3PROD with $$_JOB
“(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 SITUATION—
TIONS, 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 other-
wise disseminated in any investiga-
tion, trial, hearing, or other proceeding
in or before any court, grand jury, de-
partment, 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 ac-
quired from such query may subse-
quently be used or disclosed in any
other manner without the consent of
such person, except with the approval
of the Attorney General if the informa-
tion indicates a threat of death or seri-
ous bodily harm to any person.

“(ii) Assessment of Compliance.—
The Attorney General shall not less fre-
quently 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 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 in-
formation 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 Re-
authorization 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 per-
son 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 rel-

tant 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.”;

(B) by redesignating paragraphs (7)
through (12) as paragraphs (8) through (13), re-
spectively; and

(C) by inserting after paragraph (6) the fol-
lowing:

“(7) AUTHORITY TO SEEK REVIEW OF DECI-
SIONS.—

“(A) FISA COURT DECISIONS.—

“(i) PETITION.—Following issuance of
an order under this Act by the Foreign In-
telligence Surveillance Court, an amicus cu-
riae 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 deter-
mines 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 informa-
tion) that the amicus curiae believes to
be relevant to the duties of the amicus
curiae.

“(ii) Supporting documentation
regarding accuracy.—The Foreign Intel-
ligence Surveillance Court, upon the motion
of an amicus curiae appointed under para-
graph (2) or upon its own motion, may re-
quire the Government to make available the
supporting documentation described in sec-
tion 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”.

•HR 6570 RH
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 applicatio-
tion 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
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 Reauthor-
ization 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 dis-

trait 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’ in-

cludes 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 insert-
ing after section 110 the following:

“SEC. 110A. REPORTING REQUIREMENTS FOR CIVIL AC-
TIONS.

“(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 respon-
sible 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 re-
 sponsible for the violation; and
“(iii) referral of the incident to the In-
spection Division of the Federal Bureau of
Investigation for review of potentially reck-
less conduct.
“(3) Clarification of requirements for referring
intentional misconduct and reckless conduct to the In-
spection Division of the Federal Bureau of Investiga-
tion 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.”.

HR 6570 RH
(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.”.


(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 subpara-
graph (A) to read as follows:

“(A) ensure that—

“(i) any acquisition authorized under
subsection (a) is limited to targeting per-
sons 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 acquisi-
tion 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 commu-
ication; and”;

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

“(I) ensure that—

“(aa) an acquisition author-
ized under subsection (a) is lim-
ited to targeting persons reason-
ably 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”;

(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 semi-colon 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 subparagraphe (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 regardless of whether the identities of the United States persons were openly included or masked;
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.”.

(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.”.
To amend the Foreign Intelligence Surveillance Act of 1978 to reform certain authorities and to provide greater transparency and oversight.

A BILL

[Report No. 118-307, Part I]

H. R. 6570

118TH CONGRESS

Union Calendar No. 248