118TH CONGRESS
2D SESSION

S. 3961

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

IN THE SENATE OF THE UNITED STATES

MARCH 14, 2024

Mr. DURBIN (for himself, Mr. LEE, Ms. HIRONO, Mr. DAINES, Mr. WYDEN, Ms. LUMMIS, Ms. BALDWIN, Mr. HEINRICH, Ms. WARREN, Mr. MARKEY, Mr. TESTER, Mr. SANDERS, and Mr. WELCH) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Security And Freedom Enhancement Act of 2024'' or the ''SAFE Act''.

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

TITLE I—PROTECTIONS FOR UNITED STATES PERSONS WHOSE COMMUNICATIONS ARE COLLECTED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

SEC. 101. QUERY PROCEDURE REFORM.

(a) MANDATORY AUDITS OF UNITED STATES PERSON QUERIES CONDUCTED BY FEDERAL BUREAU OF INVESTIGATION.—

(1) IN GENERAL.—The Department of Justice shall conduct an audit of a significant representative sample of covered queries, as defined in paragraph (6) of section 702(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)), as redesignated and amended by subsection (b) of this section, conducted during the 180-day period beginning on the date of enactment of this Act, and during each 180-day period thereafter.

(2) COMPLETION OF AUDIT.—Not later than 90 days after the end of each 180-day period described in paragraph (1), the Department of Justice shall

complete the audit described in such paragraph with respect to such 180-day period.

(b) RESTRICTIONS RELATING TO CONDUCT OF CERTAIN QUERIES BY FEDERAL BUREAU OF INVESTIGATION.—Section 702(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)) is amended—

(1) by redesignating paragraph (3) as paragraph (6);

(2) by inserting before paragraph (6) the following:

''(5) QUERYING PROCEDURES APPLICABLE TO FEDERAL BUREAU OF INVESTIGATION.—For any procedures adopted under paragraph (1) applicable to the Federal Bureau of Investigation, the Attorney General, in consultation with the Director of National Intelligence, shall include the following requirements:

''(A) TRAINING.—A requirement that, prior to conducting any query, and on an annual basis thereafter as a prerequisite for continuing to conduct queries, personnel of the Federal Bureau of Investigation successfully complete training on the querying procedures.

''(B) ADDITIONAL PRIOR APPROVALS FOR SENSITIVE QUERIES.—A requirement that, ab-

sent exigent circumstances, prior to conducting certain queries, personnel of the Federal Bureau of Investigation receive approval, at minimum, as follows:

''(i) Approval from the Deputy Director of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States elected official, an appointee of the President or the governor of a State, a United States political candidate, a United States political organization or a United States person prominent in such organization, or a United States media organization or a United States person who is a member of such organization.

''(ii) Approval from an attorney of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States religious organization or a United States person who is prominent in such organization.

''(iii) Approval from an attorney of the Federal Bureau of Investigation for 2

or more queries conducted together as a batch job.

''(C) PRIOR WRITTEN JUSTIFICATION.—A requirement that—

''(i) prior to conducting a covered query, personnel of the Federal Bureau of Investigation generate a written statement of the specific factual basis to support the reasonable belief that such query meets the standards required by the procedures adopted under paragraph (1); and

''(ii) for each covered query, the Federal Bureau of Investigation shall keep a record of the query term, the date of the conduct of the query, the identifier of the personnel conducting the query, and such written statement.

''(D) AFFIRMATIVE ELECTION TO INCLUDE SECTION 702 INFORMATION IN QUERIES.—Any system of the Federal Bureau of Investigation that stores unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) together with contents or noncontents obtained through other lawful means shall be configured in a manner that—

''(i) requires personnel of the Federal Bureau of Investigation to affirmatively elect to include such unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) when running a query; or

''(ii) includes other controls reasonably expected to prevent inadvertent queries of such unminimized contents or noncontents.''; and

(3) in paragraph (6), as so redesignated—

(A) by redesignating subparagraph (B) as subparagraph (C); and

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

''(B) The term 'covered query' means a query conducted—

''(i) using a term associated with a United States person or a 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; or

''(ii) for the purpose of finding the information of a United States person or a

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.''.

(c) PROHIBITION ON WARRANTLESS ACCESS TO THE COMMUNICATIONS AND OTHER INFORMATION 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)) is amended—

(1) in paragraph (1)(A) by inserting ''and the limitations and requirements in paragraph (2)'' after ''Constitution of the United States'';

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

''(2) PROHIBITION ON WARRANTLESS ACCESS TO 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 access communications content, or information the compelled disclosure of which would require a probable cause warrant if sought for law enforcement

purposes inside the United States, acquired under subsection (a) and returned in response to a covered query.

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

''(i) IN GENERAL.—Subparagraph (A) shall not apply if—

''(I) the person to whom the query relates is the subject of an order or emergency authorization authorizing electronic surveillance, a physical search, or an acquisition under this section or section 105, section 304, section 703, or section 704 of this Act or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction;

''(II)(aa) the officer or employee accessing the communications content or information 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 the threat described in subitem (AA), the communications content or information must be accessed before authorization described in subclause (I) can, with due diligence, be obtained; and

"(bb) not later than 14 days after the communications content or information is accessed, a description of the circumstances justifying the accessing of the query results is provided to the Foreign Intelligence Surveillance Court, the congressional intelligence committees, the Committee on the Judiciary of the House of Representatives, and the Committee on the Judiciary of the Senate;

"(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 for the access on a case-by-case basis; or

''(IV)(aa) the communications content or information is accessed and used for the sole purpose of identifying targeted recipients of malicious software and preventing or mitigating harm from such malicious software;

''(bb) other than malicious software and cybersecurity threat signatures, no communications content or other information are accessed or reviewed; and

''(cc) the accessing of query results is reported to the Foreign Intelligence Surveillance Court.

''(ii) LIMITATIONS.—

''(I) USE IN SUBSEQUENT PROCEEDINGS.—No communications content or information accessed under clause (i)(II) or information derived from such access may be used, received in evidence, or otherwise disseminated 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, except in a proceeding that arises from the threat that prompted the query.

''(II) ASSESSMENT OF COMPLIANCE.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under subclause (I).

''(C) MATTERS RELATING TO EMERGENCY QUERIES.—

''(i) TREATMENT OF DENIALS.—In the event that communications content or information returned in response to a covered query are accessed pursuant to an emergency authorization described in subparagraph (B)(i)(I) and the subsequent application to authorize electronic surveillance, a physical search, or an acquisition pursuant to section 105(e), section 304(e), section 703(d), or section 704(d) of this

Act is denied, or in any other case in which communications content or information returned in response to a covered query are accessed in violation of this paragraph—

''(I) no communications content or information acquired or evidence derived from such access may be used, received in evidence, or otherwise disseminated in any investigation by or 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

''(II) no communications content or information acquired or derived from such access may subsequently be used or disclosed in any other manner without the consent of the person to whom the covered query relates, except in the case that the Attorney General approves the use or disclosure of such information in order to pre-

vent the death of or serious bodily harm to any person.

''(ii) ASSESSMENT OF COMPLIANCE.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under clause (i).

''(D) FOREIGN INTELLIGENCE PURPOSE.—

''(i) IN GENERAL.—Except as provided in clause (ii) of this subparagraph, no officer or employee of the United States may conduct a covered query of information acquired under subsection (a) unless the query is reasonably likely to retrieve foreign intelligence information.

''(ii) EXCEPTIONS.—An officer or employee of the United States may conduct a covered query of information acquired under this section if—

''(I)(aa) the officer or employee conducting the query has a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm; and

''(bb) not later than 14 days after the query is conducted, a de-

scription of the query is provided to the Foreign Intelligence Surveillance Court, the congressional intelligence committees, the Committee on the Judiciary of the House of Representatives, and the Committee on the Judiciary of the Senate;

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

''(III)(aa) 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;

''(bb) other than malicious software and cybersecurity threat signatures, no additional contents of communications acquired as a result of

the query are accessed or reviewed; and

''(cc) the query is reported to the Foreign Intelligence Surveillance Court; or

''(IV) the query is necessary to identify information that must be produced or preserved in connection with a litigation matter or to fulfill discovery obligations in a criminal matter under the laws of the United States or any State thereof.

''(3) DOCUMENTATION.—No officer or employee of the United States may access communications content, or information the compelled disclosure of which would require a probable cause warrant if sought for law enforcement purposes inside the United States, returned in response to a covered query unless an electronic record is created that includes a statement of facts showing that the access is authorized pursuant to an exception specified in paragraph (2)(B)(i).

''(4) QUERY RECORD SYSTEM.—The head of each agency that conducts queries shall ensure that a system, mechanism, or business practice is in place

to maintain the record described in paragraph (3). Not later than 90 days after the date of enactment of the SAFE Act, the head of each agency that conducts queries shall report to Congress on its compliance with this procedure.''.

(d) CONFORMING AMENDMENTS.—

(1) Section 603(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873(b)(2)) is amended, in the matter preceding subparagraph (A), by striking '', including pursuant to subsection (f)(2) of such section,''.

(2) Section 706(a)(2)(A)(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881e(a)(2)(A)(i)) is amended by striking ''obtained an order of the Foreign Intelligence Surveillance Court to access such information pursuant to section 702(f)(2)'' and inserting ''accessed such information in accordance with section 702(b)(2)''.

SEC. 102. QUARTERLY REPORTS.

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 REPORTS.—The Attorney General, in consultation with the Director of National Intelligence, shall submit to the congressional intelligence committees,

the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives a quarterly report, which shall include, for that quarter, disaggregated by each agency that conducts queries of information acquired under section 702, the following information:

''(1) The total number of covered queries (as defined in section 702(f)(6)) conducted of information acquired under section 702.

''(2) The number of times an officer or employee of the United States accessed communications contents (as defined in section 2510(8) of title 18, United States Code) or information the compelled disclosure of which would require a probable cause warrant if sought for law enforcement purposes in the United States, returned in response to such queries.

''(3) The number of applications for orders relating to an emergency authorization described in subclause (I) of section 702(f)(2)(B)(i) with respect to a person for which communications contents or information relating to such person were accessed under such subclause and the number of such orders granted.

''(4) The number of times an exception subclause (II), (III), or (IV) of section 702(f)(2)(B)(i) was asserted, disaggregated by the subclause under which an exception was asserted.''.

SEC. 103. 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 the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after the item relating to section 708 the following:

''Sec. 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 enactment of this Act, the Director of the Federal Bureau of Investigation shall submit to the Committee on the Judiciary of the House of Representatives, the Committee on the Judiciary of the Senate, and 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 Committee on the Judiciary of the House of Representatives, the Committee on the Ju-

diciary of the Senate, and 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. 104. 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 target 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;

''(II) the information is necessary to mitigate that threat;

''(III) a description of the targeting is provided to the Foreign Intelligence Surveillance Court, the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives in a timely manner; and

''(IV) any information acquired from such targeting is used, received in evidence, or otherwise disseminated solely in an investigation by or in a trial, hearing, or other proceeding in or before a court,

grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, that arises from the threat that prompted the targeting; 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;'';

(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), targeting 1 or more United States persons or persons reasonably believed to

be in the United States at the time of acquisition or communication is not a significant purpose of an acquisition; 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 target 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 tar-

geting 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 target 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. 105. FISA COURT REVIEW OF TARGETING DECISIONS.

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

(1) in subsection (h)(2)—

(A) in subparagraph (D)(ii), by striking ''and'' at the end;

(B) in subparagraph (E), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(F) include a random sample of targeting decisions and supporting written justifications from the prior year, using a sample size and methodology that has been approved by the Foreign Intelligence Surveillance Court.''; and

(2) in subsection (j)(1)—

(A) by striking ''subsection (g)'' each place it appears and inserting ''subsection (h)''; and

(B) in subparagraph (A), as amended by subparagraph (A) of this paragraph, by inserting '', including reviewing the random sample of targeting decisions and written justifications submitted under subsection (h)(2)(F),'' after ''subsection (h)''.

SEC. 106. 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; 132 Stat. 10) is amended—

(A) by striking subsection (b) (50 U.S.C. 1881a note); and

(B) by striking ''(a) IN GENERAL.—''.

SEC. 107. 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) (50 U.S.C. 1881 note)—

(A) by striking ''April 19, 2024'' and inserting ''December 31, 2027''; 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) (18 U.S.C. 2511 note), in the matter preceding subparagraph (A), by striking ''April 19, 2024'' and inserting ''December 31, 2027''.

(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 ''APRIL 19, 2024'' and inserting ''DECEMBER 31, 2027''; 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,'' both places it appears and inserting '', as most recently amended,''.

TITLE II—ADDITIONAL REFORMS RELATING TO ACTIVITIES UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

SEC. 201. APPLICATION FOR AN ORDER UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) REQUIREMENT FOR SWORN STATEMENTS FOR FACTUAL ASSERTIONS.—

(1) TITLE I.—Subsection (a)(3) of section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended by striking ''a statement of'' and inserting ''a sworn statement of''.

(2) TITLE III.—Subsection (a)(3) of section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended by striking ''a statement of'' and inserting ''a sworn statement of''.

(3) SECTION 703.—Subsection (b)(1)(C) of section 703 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881b) is amended by striking ''a statement of'' and inserting ''a sworn statement of''.

(4) SECTION 704.—Subsection (b)(3) of section 704 of the Foreign Intelligence Surveillance Act of

1978 (50 U.S.C. 1881c) is amended by striking ''a statement of'' and inserting ''a sworn statement of''.

(5) APPLICABILITY.—The amendments made by this subsection shall apply with respect to applications made on or after the date that is 120 days after the date of enactment of this Act.

(b) DESCRIPTION OF TECHNIQUES CARRIED OUT BEFORE APPLICATION.—

(1) TITLE I.—Subsection (a) of section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended—

(A) in paragraph (8), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (9), by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following:

''(10) with respect to a target who is a United States person, a statement summarizing the investigative techniques carried out before making the application;''.

(2) APPLICABILITY.—The amendments made by this subsection shall apply with respect to applications made on or after the date that is 120 days after the date of enactment of this Act.

(c) REQUIREMENT FOR CERTAIN JUSTIFICATION PRIOR TO EXTENSION OF ORDERS.—

(1) APPLICATIONS FOR EXTENSION OF ORDERS UNDER TITLE I.—Subsection (a) of section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804), as amended by this Act, is further amended by adding at the end the following:

''(11) in the case of an application for an extension of an order under this title for a surveillance targeted against a United States person, a summary statement of the foreign intelligence information obtained pursuant to the original order (and any preceding extension thereof) as of the date of the application for the extension, or a reasonable explanation of the failure to obtain such information;''.

(2) APPLICATIONS FOR EXTENSION OF ORDERS UNDER TITLE III.—Subsection (a) of section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—

(A) in paragraph (7), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (8), by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following:

''(9) in the case of an application for an extension of an order under this title in which the target of the physical search is a United States person, a summary statement of the foreign intelligence information obtained pursuant to the original order (and any preceding extension thereof) as of the date of the application for the extension, or a reasonable explanation of the failure to obtain such information;''.

(3) APPLICABILITY.—The amendments made by this subsection shall apply with respect to applications made on or after the date that is 120 days after the date of enactment of this Act.

(d) REQUIREMENT FOR JUSTIFICATION OF UNDERLYING CRIMINAL OFFENSE IN CERTAIN APPLICATIONS.—

(1) TITLE I.—Subsection (a)(3)(A) of section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended by inserting before the semicolon at the end the following: '', and, in the case of a target that is a United States person alleged to be acting as an agent of a foreign power (as described in section 101(b)(2)(B)), that a violation of the criminal statutes of the United States as referred to in section 101(b)(2)(B) has occurred or will occur''.

(2) TITLE III.—Subsection (a)(3)(A) of section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended by inserting before the semicolon at the end the following: ", and, in the case of a target that is a United States person alleged to be acting as an agent of a foreign power (as described in section 101(b)(2)(B)), that a violation of the criminal statutes of the United States as referred to in section 101(b)(2)(B) has occurred or will occur".

(3) APPLICABILITY.—The amendments made by this subsection shall apply with respect to applications made on or after the date that is 120 days after the date of enactment of this Act.

(e) REQUIRED DISCLOSURE OF RELEVANT INFORMATION IN FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 APPLICATIONS.—

(1) 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—REQUIRED DISCLOSURE OF RELEVANT INFORMATION

"SEC. 901. DISCLOSURE OF RELEVANT INFORMATION.

''The Attorney General or any other Federal officer or employee making an application for a court order under this Act shall provide the court with—

''(1) all information in the possession of the Government that is material to determining whether the application satisfies the applicable requirements under this Act, including any exculpatory information; and

''(2) all information in the possession of the Government that might reasonably—

''(A) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made; or

''(B) otherwise raise doubts with respect to the findings that are required to be made under the applicable provision of this Act in order for the court order to be issued.''.

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

"TITLE IX—REQUIRED DISCLOSURE OF RELEVANT INFORMATION

"Sec. 901. Disclosure of relevant information.".

(f) CERTIFICATION REGARDING ACCURACY PROCEDURES.—

(1) CERTIFICATION REGARDING ACCURACY PROCEDURES.—Title IX of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (e) of this section, is amended by adding at the end the following:

"SEC. 902. 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 assess-

ment 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 (as defined in section 101) 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 to address, on an annual basis, the efficacy of the accuracy proce-

dures 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.''.

(2) TECHNICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978, as amended by subsection (e) of this section, is amended by adding at the end the following:

''Sec. 902. Certification regarding accuracy procedures.''.

(g) 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;

''(2) with regard to information gathered from the content of a media source, the application includes an explanation of the investigative techniques used to corroborate the information; and

''(3) with regard to information gathered by a political campaign, such information is not the sole source of the information used to justify the applicant's belief described in subsection (a)(3).''.

(h) 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) for an application that is based, in whole or in part, on information obtained from the content of a media source or information gathered by a political campaign—

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

''(B) with regard to information gathered from the content of a media source, the application includes an explanation of the investigative techniques used to corroborate the information; and

''(C) with regard to information gathered by a political campaign, such information is not the sole source of the information used to justify the applicant's belief described in section 104(a)(3).''.

SEC. 202. 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—

(1) in subsection (a)—

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

(B) in paragraph (1)—

(i) by inserting ''intentionally'' before ''engages''; and

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

(C) in paragraph (2)—

(i) by inserting ''intentionally'' before ''disclose''; 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 court established under section 103(a) or the court established

under section 103(b), 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, except insofar as such disclosure is authorized by statute or executive order setting forth permissible disclosures by whistleblowers.''; and

(2) in subsection (c), by striking ''five'' and inserting ''8''.

(b) RULE OF CONSTRUCTION.—This section and the amendments made by this section 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. 203. INCREASED PENALTIES FOR CIVIL ACTIONS.

(a) INCREASED PENALTIES.—Section 110 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1810) is amended by striking subsection (a) and inserting the following:

''(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 court established under section 103(a). Such court shall maintain a list of each person about whom it received a report under this subsection.''.

SEC. 204. 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.) is amended by adding at the end the following:

"SEC. 605. 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 a violation described in paragraph (1), including more severe adverse personnel actions for any subsequent violation by such officer or employee.''.

(b) CLERICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978 is amended by inserting after the item relating to section 604 the following:

''Sec. 605. Agency procedures to ensure compliance.''.

(c) REPORT.—Not later than 90 days after the date of enactment of this Act, the head of each Federal department or agency that is required to establish procedures under section 605 of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (a) of this section,

shall report to Congress on the implementation of such procedures.

SEC. 205. 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 that subparagraph 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.''.

TITLE III—REFORMS RELATING TO PROCEEDINGS BEFORE THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND OTHER COURTS

SEC. 301. 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; or

''(vi) otherwise presents novel or significant civil liberties issues; 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 paragraph (1) of this subsection, 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 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), 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 court established under subsection (a), an amicus curiae appointed under paragraph (2) may petition the court to certify for review to the court established under subsection (b) a question of law pursuant to subsection (j).

''(ii) WRITTEN STATEMENT OF REASONS.—If the court established under subsection (a) denies a petition under this subparagraph, the 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 established

under subsection (b) shall appoint the amicus curiae to assist the court in its consideration of the certified question, unless the court 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 court established under subsection (b) 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 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 court established under subsection (a) 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 court established under subsection (a) or the court established under subsection (b) 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 court established under subsection (a), 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 court established under subsection (a) and the court established under subsection (b), including, if the individual is eligible for access to classified information, any classified documents, information, and other materials or proceedings.''.

(C) CONSULTATION AMONG AMICI CURIAE.—Section 103(i)(6) of the Foreign Intel-

ligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(6)) is amended—

(i) by redesignating subparagraph (D) as subparagraph (E); and

(ii) by inserting after subparagraph (C) the following:

''(D) CONSULTATION AMONG AMICI CURIAE.—An amicus curiae appointed under paragraph (2) by the court established under subsection (a) or the court established under subsection (b) may consult with 1 or more of the other individuals designated by the court to serve as amicus curiae pursuant to paragraph (1) of this subsection regarding any of the information relevant to any assigned proceeding.''.

(4) EFFECTIVE DATE.—The amendments made by this subsection 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. 302. 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 ", to be concluded not later than 180 days after the issuance of such decision, order, or opinion," after "(as defined in section 601(e))"; and

(2) by inserting "or results in a change of application of any provision of this Act or a novel application of any provision of this Act" after "law".

SEC. 303. SUBMISSION OF COURT TRANSCRIPTS TO CONGRESS.

Section 601(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(c)), as amended by section 302 of this Act, is amended—

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

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

(3) by adding at the end the following:

''(3) for any matter at which a court reporter is present and creates a transcript of a hearing or oral argument before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, a copy of each such transcript not later than 45 days after the government's receipt of the transcript or the date on which the matter concerning such hearing or oral argument is resolved, whichever is later.''.

SEC. 304. CONTEMPT POWER OF FISC AND FISCR.

(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 those terms in section 601(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(e)).''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 21 of title 18, United States Code, is amended by adding at the end the following:

''404. Definitions.''.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review (as those terms are defined in section 601(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(e))) shall jointly submit to Congress a report on the exercise of authority under chapter 21 of title 18, United States Code, by those courts during the 1-year period ending on the date that is 60 days before the date of submission of the report.

TITLE IV—INDEPENDENT EXECUTIVE BRANCH OVERSIGHT

SEC. 401. PERIODIC 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.), as amended by section 204 of this Act, is amended by adding at the end the following:

''SEC. 606. PERIODIC AUDIT OF FISA COMPLIANCE BY INSPECTOR GENERAL.

''Not later than June 30 of the first calendar year that begins after the date of enactment of this section, and every 5 years thereafter, the Inspector General of the Department of Justice shall—

''(1) conduct an audit of alleged or potential violations and failures to comply with the requirements of this Act, and any procedures established pursuant to this Act, which shall include an analysis of the accuracy and completeness of applications and certifications for orders submitted under each of sections 105, 303, 402, 502, 702, 703, and 704; and

''(2) submit to the Select Committee on Intelligence of the Senate, the Committee on the Judiciary of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the House of Representatives a report on the audit required under paragraph (1).''.

(b) CLERICAL AMENDMENT.—The table of contents for the Foreign Intelligence Surveillance Act of 1978, as

amended by section 204 of this Act, is amended by inserting after the item relating to section 605 the following:

''Sec. 606. Periodic audit of FISA compliance by Inspector General.''.

SEC. 402. INTELLIGENCE COMMUNITY PARITY AND COMMUNICATIONS WITH PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.

(a) WHISTLEBLOWER PROTECTIONS FOR MEMBERS OF INTELLIGENCE COMMUNITY FOR COMMUNICATIONS WITH PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (b)(1), in the matter before subparagraph (A), by inserting ''the Privacy and Civil Liberties Oversight Board,'' after ''Inspector General of the Intelligence Community,''; and

(2) in subsection (c)(1)(A), in the matter before clause (i), by inserting ''the Privacy and Civil Liberties Oversight Board,'' after ''Inspector General of the Intelligence Community,''.

(b) PARITY IN PAY FOR PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD STAFF AND THE INTELLIGENCE COMMUNITY.—Section 1061(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(j)(1)) is amended by striking ''except that'' and all that follows through the period at the end and inserting ''except that no rate of pay fixed under this sub-

section may exceed the highest amount paid by any element of the intelligence community for a comparable position, based on salary information provided to the chairman of the Board by the Director of National Intelligence.''.

TITLE V—PROTECTIONS FOR UNITED STATES PERSONS WHOSE SENSITIVE INFORMATION IS PURCHASED BY INTELLIGENCE AND LAW ENFORCEMENT AGENCIES

SEC. 501. LIMITATION ON INTELLIGENCE ACQUISITION OF UNITED STATES PERSON DATA.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003));

(B) the Committee on the Judiciary of the Senate; and

(C) the Committee on the Judiciary of the House of Representatives.

(2) COVERED DATA.—The term ''covered data'' means data, derived data, or any unique identifier that—

(A) is linked to or is reasonably linkable to a covered person; and

(B) does not include data that—

(i) is lawfully available to the public through Federal, State, or local government records or through widely distributed media;

(ii) is reasonably believed to have been voluntarily made available to the general public by the covered person; or

(iii) is a specific communication or transaction with a targeted individual who is not a covered person.

(3) COVERED PERSON.—The term ''covered person'' means an individual who—

(A) is reasonably believed to be located in the United States at the time of the creation or acquisition of the covered data; or

(B) is a United States person.

(4) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given

such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(5) STATE, UNITED STATES, UNITED STATES PERSON.—The terms ''State'', ''United States'', and ''United States person'' have the meanings given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) LIMITATION.—

(1) IN GENERAL.—Subject to paragraphs (2) through (7), an element of the intelligence community may not acquire a dataset that includes covered data.

(2) AUTHORIZATION PURSUANT TO COURT ORDER.—An element of the intelligence community may acquire covered data if the collection has been authorized by an order or emergency authorization issued pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or title 18, United States Code, by a court of competent jurisdiction covering the period of the acquisition, subject to the use, dissemination, querying, retention, and other minimization limitations required by such authorization.

(3) AUTHORIZATION FOR EMPLOYMENT-RELATED USE.—An element of the intelligence commu-

nity may acquire covered data about an employee of, or applicant for employment by, an element of the intelligence community for employment-related purposes, provided that—

(A) access to and use of the covered data is limited to such purposes; and

(B) the covered data is destroyed at such time as it is no longer necessary for such purposes.

(4) EXCEPTION FOR COMPLIANCE PURPOSES.—An element of the intelligence community may acquire covered data for the purpose of supporting compliance with collection limitations and minimization requirements imposed by statute, guidelines, procedures, or the Constitution of the United States, provided that—

(A) access to and use of the covered data is limited to such purpose; and

(B) the covered data is destroyed at such time as it is no longer necessary for such purpose.

(5) EXCEPTION FOR LIFE OR SAFETY.—An element of the intelligence community may acquire covered data if there is a reasonable belief than an emergency exists involving an imminent threat of

death or serious bodily harm and the covered data is necessary to mitigate that threat, provided that—

(A) access to and use of the covered data is limited to addressing the threat; and

(B) the covered data is destroyed at such time as it is no longer necessary for such purpose.

(6) EXCEPTION FOR CONSENT.—An element of the intelligence community may acquire covered data if—

(A) each covered person linked or reasonably linkable to the covered data, or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of the person, has provided consent to the acquisition and use of the data on a case-by-case basis;

(B) access to and use of the covered data is limited to the purposes for which the consent was provided; and

(C) the covered data is destroyed at such time as it is no longer necessary for such purposes.

(7) EXCEPTION FOR NONSEGREGABLE DATA.—An element of the intelligence community may ac-

quire a dataset that includes covered data if the covered data is not reasonably segregable prior to acquisition, provided that the element of the intelligence community complies with the minimization procedures in subsection (c).

(c) MINIMIZATION PROCEDURES.—

(1) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and to restrict the querying, of covered data that is not subject to 1 or more of the exceptions set forth in subsection (b).

(2) ACQUISITION AND RETENTION.—The procedures adopted under paragraph (1) shall require elements of the intelligence community to exhaust all reasonable means—

(A) to exclude covered data not subject to 1 or more exceptions set forth in subsection (b) from datasets prior to acquisition; and

(B) to remove and delete covered data not subject to 1 or more exceptions set forth in subsection (b) prior to the operational use of the acquired dataset or the inclusion of the dataset in a database intended for operational use.

(3) DESTRUCTION.—The procedures adopted under paragraph (1) shall require that if an element of the intelligence community identifies covered data not subject to 1 or more exceptions set forth in paragraphs (2) through (6) of subsection (b), such covered data shall be promptly destroyed.

(4) QUERYING.—

(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C), no officer or employee of an element of the intelligence community may conduct a query of covered data, including covered data already subjected to minimization, in an effort to find records of or about a particular covered person.

(B) EXCEPTIONS.—Subparagraph (A) shall not apply to a query related to a particular covered person if—

(i) such covered person is the subject of a court order or emergency authorization issued under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or title 18, United States Code, that would authorize the element of the intelligence community to compel the produc-

tion of the covered data, during the effective period of that order;

(ii) the purpose of the query is to retrieve information about an employee of, or applicant for employment by, an element of the intelligence community, provided that any covered data accessed through such query is used only for such purpose;

(iii) the query is conducted for the purpose of supporting compliance with collection limitations and minimization requirements imposed by statute, guidelines, procedures, or the Constitution of the United States, provided that any covered data accessed through such query is used only for such purpose;

(iv) the officer or employee of an element of the intelligence community carrying out the query has a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm, and that in order to prevent or mitigate such threat, the query must be conducted before a court order can, with due diligence, be obtained, provided that any

covered data accessed through such query is used only for such purpose; or

(v) such covered person or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of the person has consented to the query, provided that any use of covered data accessed through such query is limited to the purposes for which the consent was provided.

(C) SPECIAL RULE FOR NONSEGREGABLE DATASETS.—For a query of a dataset acquired under subsection (b)(7)—

(i) each query shall be reasonably designed to exclude personal data of covered persons, unless the query is subject to an exception set forth in paragraph (4); and

(ii) any personal data of covered persons returned pursuant to a query that is not subject to an exception set forth in paragraphs (2) through (7) of subsection (b) shall not be reviewed and shall immediately be destroyed.

(d) PROHIBITION ON USE OF DATA OBTAINED IN VIOLATION OF THIS SECTION.—Covered data acquired by

an element of the intelligence community in violation of subsection (b), and any evidence derived therefrom, may not be used, received in evidence, or otherwise disseminated in any investigation by or 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.

(e) REPORTING REQUIREMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress and the Privacy and Civil Liberties Oversight Board a report on the acquisition of datasets that the Director anticipates will contain information of covered persons that is significant in volume, proportion, or sensitivity.

(2) CONTENTS.—The report submitted pursuant to paragraph (1) shall include the following:

(A) A description of the covered person information in each dataset.

(B) An estimate of the amount of covered person information in each dataset.

(3) NOTIFICATIONS.—After submitting the report required by paragraph (1), the Director shall,

in coordination with the Under Secretary of Defense for Intelligence and Security, notify the appropriate committees of Congress of any changes to the information contained in such report.

(4) AVAILABILITY TO THE PUBLIC.—The Director shall make available to the public on the website of the Director—

(A) the unclassified portion of the report submitted pursuant to paragraph (1); and

(B) any notifications submitted pursuant to paragraph (3).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall authorize an acquisition otherwise prohibited by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or title 18, United States Code.

SEC. 502. LIMITATION ON LAW ENFORCEMENT PURCHASE OF PERSONAL DATA FROM 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 PERSONAL DATA BY LAW ENFORCEMENT AGENCIES.—

''(1) DEFINITIONS.—In this subsection and subsection (f)—

"(A) the term 'covered governmental entity' means a law enforcement agency of a governmental entity;

"(B) the term 'covered organization' means a person who—

"(i) is not a governmental entity; and

"(ii) is not an individual;

"(C) the term 'covered person' means an individual who—

"(i) is reasonably believed to be located inside the United States at the time of the creation of the covered personal data; or

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

"(D) the term 'covered personal data' means personal data relating to a covered person;

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

"(F) the term 'lawfully obtained public data' means personal data obtained by a par-

ticular covered organization that the covered organization—

"(i) reasonably understood to have been voluntarily made available to the general public by the covered person; and

"(ii) obtained in compliance with all applicable laws, regulations, contracts, privacy policies, and terms of service;

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

"(H) the term 'personal data'—

"(i) means data, derived data, or any unique identifier that is linked to, or is reasonably linkable to, an individual or to an electronic device that is linked to, or is reasonably linkable to, 1 or more individuals in a household;

"(ii) includes anonymized data that, if combined with other data, can be linked to, or is reasonably linkable to, an individual

or to an electronic device that identifies, is linked to, or is reasonably linkable to 1 or more individuals in a household; and

''(iii) does not include—

''(I) data that is lawfully available through Federal, State, or local government records or through widely distributed media; or

''(II) a specific communication or transaction with a targeted individual who is not a covered person.

''(2) LIMITATION.—

''(A) IN GENERAL.—

''(i) PROHIBITION.—Subject to clauses (ii) through (x), a covered governmental entity may not obtain in exchange for anything of value covered personal data if—

''(I) the covered personal data is directly or indirectly obtained from a covered organization; or

''(II) the covered personal data is derived from covered personal data that was directly or indirectly obtained from a covered organization.

''(ii) EXCEPTION FOR CERTAIN COMPILATIONS OF DATA.—A covered governmental entity may obtain in exchange for something of value covered personal data as part of a larger compilation of data which includes personal data about persons who are not covered persons, if—

''(I) the covered governmental entity is unable through reasonable means to exclude covered personal data from the larger compilation obtained; and

''(II) the covered governmental entity minimizes any covered personal data from the larger compilation, in accordance with subsection (f).

''(iii) EXCEPTION FOR WHISTLEBLOWER DISCLOSURES TO LAW ENFORCEMENT.—Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity under a program established by an Act of Congress under which a portion of a penalty or a similar payment or bounty is paid to an individual who discloses information about

an unlawful activity to the Government, such as the program authorized under section 7623 of the Internal Revenue Code of 1986 (relating to awards to whistleblowers in cases of underpayments or fraud).

''(iv) EXCEPTION FOR COST REIMBURSEMENT UNDER COMPULSORY LEGAL PROCESS.—Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity from a covered organization in accordance with compulsory legal process that—

''(I) is established by a Federal or State statute; and

''(II) provides for the reimbursement of costs of the covered organization that are incurred in connection with providing the record or information to the covered governmental entity, such as the reimbursement of costs under section 2706.

''(v) EXCEPTION FOR EMPLOYMENT-RELATED USE.—Clause (i) shall not apply to covered personal data about an em-

ployee of, or applicant for employment by, a covered governmental entity that is—

"(I) obtained by the covered governmental entity for employment-related purposes;

"(II) accessed and used by the covered governmental entity only for employment-related purposes; and

"(III) destroyed at such time as the covered personal data is no longer needed for employment-related purposes.

"(vi) EXCEPTION FOR USE IN BACKGROUND CHECKS.—Clause (i) shall not apply to covered personal data about a covered person that is—

"(I) obtained by a covered governmental entity for purposes of conducting a background check of the covered person with the written consent of the covered person;

"(II) accessed and used by the covered governmental entity only for background check-related purposes; and

''(III) destroyed at such time as the covered personal data is no longer needed for background check-related purposes.

''(vii) EXCEPTION FOR LAWFULLY OBTAINED PUBLIC DATA.—Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity if—

''(I) the covered personal data is lawfully obtained public data; or

''(II) the covered personal data is derived from covered personal data that solely consists of lawfully obtained public data.

''(viii) EXCEPTION FOR LIFE OR SAFETY.—Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity if there is a reasonable belief than an emergency exists involving an imminent threat of death or serious bodily harm to a covered person and the covered data is necessary to mitigate that threat, provided that—

''(I) access to and use of the covered personal data is limited to addressing the threat; and

''(II) the covered personal data is destroyed at such time as it is no longer necessary for such purpose.

''(ix) EXCEPTION FOR COMPLIANCE PURPOSES.—Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity for the purpose of supporting compliance with collection limitations and minimization requirements imposed by statute, guidelines, procedures, or the Constitution of the United States, provided that—

''(I) access to and use of the covered personal data is limited to such purpose; and

''(II) the covered personal data is destroyed at such time as it is no longer necessary for such purpose.

''(x) EXCEPTION FOR CONSENT.—Clause (i) shall not apply to covered personal data that is obtained by a covered governmental entity if—

"(I) each covered person linked or reasonably linkable to the covered personal data, or, if such covered person is incapable of providing consent, a third party legally authorized to consent on behalf of the covered person, has provided consent to the acquisition and use of the data on a case-by-case basis;

"(II) access to and use of the covered personal data is limited to the purposes for which the consent was provided; and

"(III) the covered personal data is destroyed at such time as it is no longer necessary for such purposes.

"(B) INDIRECTLY ACQUIRED RECORDS AND INFORMATION.—The limitation under subparagraph (A) shall apply without regard to whether the covered organization possessing the covered personal data is the covered organization that initially obtained or collected, or is the covered organization that initially received the disclosure of, the covered personal data.

''(3) LIMIT ON SHARING BETWEEN AGENCIES.—An agency of a governmental entity that is not a covered governmental entity may not provide to a covered governmental entity covered personal data that was obtained in a manner that would violate paragraph (2) if the agency of a governmental entity were a covered governmental entity, unless the covered governmental entity would have been permitted to obtain the covered personal data under an exception set forth in paragraph (2)(A).

''(4) PROHIBITION ON USE OF DATA OBTAINED IN VIOLATION OF THIS SECTION.—

''(A) IN GENERAL.—Covered personal data obtained by or provided to a covered governmental entity in violation of paragraph (2) or (3), and any evidence derived therefrom, may not be used, received in evidence, or otherwise disseminated by, on behalf of, or upon a motion or other action by a covered governmental entity in any investigation by or 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.

''(B) USE BY AGGRIEVED PARTIES.—Nothing in subparagraph (A) shall be construed to limit the use of covered personal data by a covered person aggrieved of a violation of paragraph (2) or (3) in connection with any action relating to such a violation.

''(f) MINIMIZATION PROCEDURES.—

''(1) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and to restrict the querying, of covered personal data, and prohibit the dissemination of information derived from covered personal data.

''(2) ACQUISITION AND RETENTION.—The procedures adopted under paragraph (1) shall require covered governmental entities to exhaust all reasonable means—

''(A) to exclude covered personal data that is not subject to 1 or more of the exceptions set forth in clauses (iii) through (x) of subsection (e)(2)(A) from the data obtained; and

''(B) to remove and delete covered personal data described in subparagraph (A) not subject to 1 or more exceptions set forth in clauses (iii) through (x) of subsection (e)(2)(A) after a com-

pilation is obtained and before operational use of the compilation or inclusion of the compilation in a dataset intended for operational use.

''(3) DESTRUCTION.—The procedures adopted under paragraph (1) shall require that, if a covered governmental entity identifies covered personal data in a compilation described in clause (ii) of subsection (e)(2)(A) not subject to 1 or more exceptions set forth in clauses (iii) through (x) of such subsection, the covered governmental entity shall promptly destroy the covered personal data and any dissemination of information derived from the covered personal data shall be prohibited.

''(4) QUERYING.—

''(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C), no officer or employee of a covered governmental entity may conduct a query of personal data, including personal data already subjected to minimization, in an effort to find records of or about a particular covered person.

''(B) EXCEPTIONS.—Subparagraph (A) shall not apply to a query related to a particular covered person if—

''(i) such covered person is the subject of a court order or emergency authorization issued under this title that would authorize the covered governmental entity to compel the production of the covered personal data, during the effective period of that order;

''(ii) the purpose of the query is to retrieve information obtained by a covered governmental entity under a program established by an Act of Congress under which a portion of a penalty or a similar payment or bounty is paid to an individual who discloses information about an unlawful activity to the Government, such as the program authorized under section 7623 of the Internal Revenue Code of 1986 (relating to awards to whistleblowers in cases of underpayments or fraud), provided that any covered personal data accessed through such query is used only for such purpose;

''(iii) the purpose of the query is to retrieve information about an employee of, or applicant for employment by, a covered

governmental entity that has been obtained by the covered governmental entity for employment-related purposes, provided that any covered personal data accessed through such query is used only for such purposes;

''(iv) the purpose of the query is to retrieve information obtained by a covered governmental entity for purposes of conducting a background check of the covered person with the written consent of the covered person, provided that any covered personal data accessed through such query is used only for such purposes;

''(v) the purpose of the query is to retrieve, and the query is reasonably designed to retrieve, only lawfully obtained public data, and only lawfully obtained public data is accessed and used as a result of the query;

''(vi) the officer or employee of a covered governmental entity carrying out the query has a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm, and in

order to prevent or mitigate that threat, the query must be conducted before a court order can, with due diligence, be obtained, provided that any covered personal data accessed through such query is used only for such purpose;

''(vii) the query is conducted for the purpose of supporting compliance with collection limitations and minimization requirements imposed by statute, guidelines, procedures, or the Constitution of the United States, provided that any covered personal data accessed through such query is used only for such purpose; or

''(viii) such covered person or, if such covered person is incapable of providing consent, a third party legally authorized to consent on behalf of the covered person has consented to the query, provided that any use of covered personal data accessed through such query is limited to the purposes for which the consent was provided.

''(C) SPECIAL RULE FOR COMPILATIONS OF DATA.—For a query of a compilation of data obtained under subsection (e)(2)(A)(ii)—

''(i) each query shall be reasonably designed to exclude personal data of covered persons, unless the query is subject to an exception set forth in subparagraph (B); and

''(ii) any personal data of covered persons returned pursuant to a query that is not subject to an exception set forth in clauses (ii) through (iii) of subsection (e)(2)(A) shall not be reviewed and shall immediately be destroyed.''.

SEC. 503. CONSISTENT PROTECTIONS FOR DEMANDS FOR DATA HELD BY INTERACTIVE COMPUTING SERVICES.

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

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

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

(3) by adding at the end the following:

''(5) the term 'online service provider' means a provider of electronic communication service, a provider of remote computing service, any information service, system, or access software provider that pro-

vides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions; and''.

(b) REQUIRED DISCLOSURE.—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (a), in the first sentence, by striking ''a provider of electronic communication service'' and inserting ''an online service provider'';

(2) in subsection (c)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking ''a provider of electronic communication service or remote computing service'' and inserting ''an online service provider''; and

(B) in paragraph (2), in the matter preceding subparagraph (A), by striking ''A provider of electronic communication service or remote computing service'' and inserting ''An online service provider''; and

(3) in subsection (g), by striking ''a provider of electronic communications service or remote computing service'' and inserting ''an online service provider''.

(c) LIMITATION ON VOLUNTARY DISCLOSURE.—Section 2702(a) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking ''a person or entity providing an electronic communication service to the public'' and inserting ''an online service provider'';

(2) in paragraph (2), by striking ''a person or entity providing remote computing service to the public'' and inserting ''an online service provider''; and

(3) in paragraph (3), by striking ''a provider of remote computing service or electronic communication service to the public'' and inserting ''an online service provider''.

SEC. 504. CONSISTENT PRIVACY PROTECTIONS FOR DATA HELD BY DATA BROKERS.

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

''(i) COVERED PERSONAL DATA.—

''(1) DEFINITIONS.—In this subsection, the terms 'covered personal data' and 'covered organization' 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 covered organization that is not an online service provider to disclose covered personal data if a court order would be required for the governmental entity to require an online service provider to disclose such covered personal data that is a record of a customer or subscriber of the online service provider.

''(3) ORDERS.—

''(A) IN GENERAL.—A court may only issue an order requiring a covered organization that is not an online service provider to disclose covered personal data on the same basis and subject to the same limitations as would apply to a court order to require disclosure by an online service 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 an online service provider of a customer or subscriber of the online service provider.''.

SEC. 505. PROTECTION OF DATA ENTRUSTED TO INTERMEDIARY OR ANCILLARY SERVICE PROVIDERS.

(a) DEFINITION.—Section 2711 of title 18, United States Code, as amended by section 503 of this Act, is amended by adding at the end the following:

''(6) the term 'intermediary or ancillary service provider' means an entity or facilities owner or operator that directly or indirectly delivers, transmits, stores, or processes communications or any other covered personal data (as defined in section 2702(e) of this title) for, or on behalf of, an online service provider.''.

(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)(B), 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 or ancillary service provider may not knowingly disclose—

''(A) to any person or entity the contents of a communication while in electronic storage

by that intermediary or ancillary service 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 online service provider for, or on behalf of, which the intermediary or ancillary service provider directly or indirectly delivers, transmits, stores, or processes communications or any other covered personal data (as defined in subsection (e)).''.

TITLE VI—TRANSPARENCY

SEC. 601. ENHANCED REPORTS BY DIRECTOR OF NATIONAL INTELLIGENCE.

(a) IN GENERAL.—Section 603(b) 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 targeted and the number of selectors used under section 702(a), disaggregated by the certification under which the person 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 section 701(b)(4);'';

(4) in paragraph (9), as so redesignated, by striking ''and'' at the end;

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

(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 and conducted under procedures ap-

proved by the Attorney General 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 and conducted under procedures approved by the Attorney General 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 and conducted under procedures approved by the Attorney General containing the identities of United States persons in which the identi-

ties 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 under procedures approved by the Attorney General and 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 under procedures approved by the Attorney General and 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 Intel-

ligence Authorization Act for Fiscal Year 2015 (50 U.S.C. 1813(b)(3))—

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

"(B) are retained for more than 5 years because, in whole or in part, the communications are encrypted.".

(b) REPEAL OF NONAPPLICABILITY TO FEDERAL BUREAU OF INVESTIGATION OF CERTAIN REQUIREMENTS.—Section 603(d) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873(d)) is amended—

(1) by striking paragraph (2); and

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

(c) CONFORMING AMENDMENT.—Section 603(d)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873(d)(1)) is amended by striking "paragraphs (3), (5), or (6)" and inserting "paragraph (6), (8), or (9)".

TITLE VII—LIMITED DELAYS IN IMPLEMENTATION

SEC. 701. LIMITED DELAYS IN IMPLEMENTATION.

(a) DEFINITION.—In this section, the term "appropriate committees of Congress" means—

(1) the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003));

(2) the Committee on the Judiciary of the Senate; and

(3) the Committee on the Judiciary of the House of Representatives.

(b) AUTHORITY.—The Attorney General may, in coordination with the Director of National Intelligence as may be appropriate, delay implementation of a provision of this Act or an amendment made by this Act for a period of not more than 1 year upon a showing to the appropriate committees of Congress that the delay is necessary—

(1) to develop and implement technical systems needed to comply with the provision or amendment; or

(2) to hire or train personnel needed to comply with the provision or amendment.

○