II

118TH CONGRESS
1ST SESSION

S. 3234

To implement reforms relating to foreign intelligence surveillance authorities, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 7, 2023

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

---

A BILL

To implement reforms relating to foreign intelligence surveillance authorities, and for other purposes.

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 ''Government Surveillance Reform Act of 2023''.

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

SEC. 2. DEFINITIONS.

(a) AMENDMENTS TO FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—

(1) IN GENERAL.—Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) is amended by adding at the end the following:

''(q) The term 'Foreign Intelligence Surveillance Court' means the court established under section 103(a).

''(r) The terms 'Foreign Intelligence Surveillance Court of Review' and 'Court of Review' mean the court established under section 103(b).

''(s) 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.''.

(2) CONFORMING AMENDMENTS.—Such Act (50 U.S.C. 1801 et seq.) is amended—

(A) in section 102 (50 U.S.C. 1802), by striking ''the court established under section 103(a)'' and inserting ''the Foreign Intelligence Surveillance Court'';

(B) in section 103 (50 U.S.C. 1803)—

(i) in subsection (a)—

(I) in paragraph (2)(A), by striking ''The court established under this subsection'' and inserting ''The Foreign Intelligence Surveillance Court''; and

(II) by striking ''the court established under this subsection'' each place it appears and inserting ''the Foreign Intelligence Surveillance Court'';

(ii) in subsection (g)—

(I) by striking ''the court established pursuant to subsection (a)'' and inserting ''the Foreign Intelligence Surveillance Court'';

(II) by striking ''the court of review established pursuant to subsection (b)'' and inserting ''the Foreign Intelligence Surveillance Court of Review''; and

(III) by striking ''The courts established pursuant to subsections (a) and (b)'' and inserting ''The Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review'';

(iii) in subsection (h), by striking ''a court established under this section'' and inserting ''the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review'';

(iv) in subsection (i)—

(I) in paragraph (1), by striking ''the courts established under subsections (a) and (b)'' and inserting

"the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review";

(II) in paragraph (3)(B), by striking "the courts" and inserting "the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review";

(III) in paragraph (5), by striking "the court" and inserting "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, as the case may be,";

(IV) in paragraph (6), by striking "the court" each place it appears and inserting "the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review";

(V) by striking "a court established under subsection (a) or (b)" each place it appears and inserting "the Foreign Intelligence Surveillance

Court or the Foreign Intelligence Surveillance Court of Review''; and

(VI) by striking ''A court established under subsection (a) or (b)'' each place it appears and inserting ''The Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review'';

(v) in subsection (j)—

(I) by striking ''a court established under subsection (a)'' and inserting ''the Foreign Intelligence Surveillance Court''; and

(II) by striking ''the court determines'' and inserting ''the Foreign Intelligence Surveillance Court determines'';

(vi) by striking ''the court established under subsection (a)'' each place it appears and inserting ''the Foreign Intelligence Surveillance Court''; and

(vii) by striking ''the court established under subsection (b)'' each place it appears and inserting ''the Foreign Intelligence Surveillance Court of Review'';

(C) in section 105(c) (50 U.S.C. 1805(c))—

(i) in paragraph (2)(B), by striking ''the Court'' and inserting ''the Foreign Intelligence Surveillance Court''; and

(ii) in paragraph (3), by striking ''the court'' each place it appears and inserting ''the Foreign Intelligence Surveillance Court'';

(D) in section 401(1) (50 U.S.C. 1841(1)), by striking '', and 'State'' and inserting '' 'State', 'Foreign Intelligence Surveillance Court', and 'Foreign Intelligence Surveillance Court of Review' '';

(E) in section 402 (50 U.S.C. 1842)—

(i) in subsection (b)(1), by striking ''the court established by section 103(a) of this Act'' and inserting ''the Foreign Intelligence Surveillance Court''; and

(ii) in subsection (h)(2), by striking ''the court established under section 103(a)'' and inserting ''the Foreign Intelligence Surveillance Court'';

(F) in section 501 (50 U.S.C. 1861)—

(i) in subsection (b)(1), by striking ''the court established by section 103(a)'' and inserting ''the Foreign Intelligence Surveillance Court'';

(ii) in subsection (g)(3), by striking ''the court established under section 103(a)'' and inserting ''the Foreign Intelligence Surveillance Court''; and

(iii) in subsection (k)(1), by striking '', and 'State'' and inserting '' 'State', and 'Foreign Intelligence Surveillance Court' '';

(G) in section 502(c)(1)(E), by striking ''the court established under section 103'' and inserting ''the Foreign Intelligence Surveillance Court (as defined by section 101)'';

(H) in section 801 (50 U.S.C. 1885)—

(i) in paragraph (8)(B)(i), by striking ''the court established under section 103(a)'' and inserting ''the Foreign Intelligence Surveillance Court''; and

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

''(10) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term 'Foreign Intelligence Surveillance

Court' means the court established under section 103(a).''; and

(I) in section 802(a)(1) (50 U.S.C. 1885a(a)(1)), by striking ''the court established under section 103(a)'' and inserting ''the Foreign Intelligence Surveillance Court''.

(b) TERMS USED IN THIS ACT.—In this Act, the terms ''appropriate committees of Congress'', ''Foreign Intelligence Surveillance Court'', and ''Foreign Intelligence Surveillance Court of Review'' have the meanings given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), as amended by subsection (a).

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

SEC. 101. PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

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

(1) in paragraph (1)—

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

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

(2) by redesignating paragraph (3) as paragraph (5); and

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

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

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

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

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

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

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

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

"(BB) in order to prevent or mitigate this threat, the query must be conducted before author-

ization pursuant to subparagraph (I) can, with due diligence, be obtained; and

''(bb) a description of the query is provided to the Foreign Intelligence Surveillance Court and the appropriate committees of Congress in a timely manner;

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

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

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

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

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

''(ii) LIMITATIONS.—

"(I) USE IN SUBSEQUENT PROCEEDINGS AND INVESTIGATIONS.—No information retrieved pursuant to a query authorized by clause (i)(II) or information derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in proceedings or investigations that arise from the threat that prompted the query.

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

"(C) MATTERS RELATING TO EMERGENCY QUERIES.—

"(i) TREATMENT OF DENIALS.—In the event that a query for communications

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

''(I) no information obtained or evidence derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States,

a State, or political subdivision thereof; and

"(II) no information concerning any United States person or person reasonably believed to be located in the United States at the time of the query or the time of the communication or the creation of the information acquired from such query may subsequently be used or disclosed in any other manner without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

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

"(D) FOREIGN INTELLIGENCE PURPOSE.—Except as provided in subparagraph (B)(i), no officer or employee of the United States may conduct a query of information acquired under this section in an effort to find information of or about 1 or more United States persons or

persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information unless the query is reasonably likely to retrieve foreign intelligence information.

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

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

''(B) The date of the query.

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

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

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

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

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

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

SEC. 102. LIMITATION ON USE OF INFORMATION OBTAINED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 RELATING TO UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES IN CRIMINAL, CIVIL, AND ADMINISTRATIVE ACTIONS.

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

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

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

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

''(i) terrorism (as defined in clauses (i) through (iii) of section 2332b(g)(5)(B) of title 18, United States Code);

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

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

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

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

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

''(vii) international narcotics trafficking.''.

SEC. 103. REPEAL OF AUTHORITY FOR THE RESUMPTION OF ABOUTS COLLECTION.

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

(b) CONFORMING AMENDMENTS.—

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

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

(B) by striking paragraph (4).

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

(A) by striking subsection (b); and

(B) by striking the following:

"(a) IN GENERAL.—".

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), as amended by section 101, is further amended—

(1) in subsection (b)(2)—

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

''(A) intentionally'';

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

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

United States at the time of the query or the time of acquisition or communication;

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

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

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

''(B) in the case of information acquired pursuant to subparagraph (A)(i) or evidence derived from such targeting, be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States,

a State, or political subdivision thereof, except in proceedings or investigations that arise from the threat that prompted the targeting;'';

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

''(A) ensure that—

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

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

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

''(I) ensure that—

''(aa) an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be non-United

States persons located outside the United States; and

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

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

''(i) ensure that—

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

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

of acquisition or communication; and''.

SEC. 105. DATA RETENTION LIMITS FOR INFORMATION COLLECTED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(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. DATA RETENTION LIMITS.

''(a) POLICY.—The Attorney General shall develop, and the heads of the elements of the intelligence community shall implement, procedures governing the retention of information collected pursuant to section 702.

''(b) COVERED INFORMATION.—For purposes of this section, 'covered information' includes—

''(1) any information, including an encrypted communication, to, from, or pertaining to a United States person or person reasonably believed to be located in the United States at the time of acquisition, communication, or creation of the information that has been evaluated and is not specifically known to contain foreign intelligence information; and

''(2) any unevaluated information, unless it can reasonably be determined that the unevaluated infor-

mation does not contain communications to or from or information pertaining to a United States person or person reasonably believed to be located in the United States at the time of acquisition, communication or creation of the information.

''(c) REQUIREMENTS.—The procedures developed and implemented pursuant to subsection (a) shall ensure, with respect to information described in such subsection, that covered information shall be destroyed within 5 years of collection unless the Attorney General determines in writing that—

''(1) the information is the subject of a preservation obligation in pending administrative, civil, or criminal litigation, in which case the information shall be segregated, retained, and used solely for that purpose and shall be destroyed as soon as it is no longer required to be preserved for such litigation; or

''(2) the information is being used in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat identified in section 706(a)(2)(B).''.

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

''Sec. 709. Data retention limits.''.

SEC. 106. FOREIGN INTELLIGENCE SURVEILLANCE COURT SUPERVISION OF DEMANDS FOR TECHNICAL ASSISTANCE FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 702(i)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(i)(1)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and moving such clauses 2 ems to the right;

(2) in the matter before clause (i), as redesignated by paragraph (1), by striking ''With respect to'' and inserting the following:

''(A) IN GENERAL.—Subject to subparagraph (B), in carrying out''; and

(3) by adding at the end the following:

''(B) LIMITATIONS.—The Attorney General or the Director of National Intelligence may not direct technical assistance from an electronic communication service provider under subparagraph (A) without demonstrating that the assistance sought—

''(i) is necessary;

''(ii) is narrowly tailored to the surveillance at issue; and

''(iii) would not pose an undue burden on the electronic communication service provider or its customers who are not intended targets of the surveillance.

''(C) COMPLIANCE.—An electronic communication service provider is not obligated to comply with a directive to provide technical assistance under this paragraph unless—

''(i) such assistance is a manner or method that has been explicitly approved by the Court; and

''(ii) the Court issues an order, which has been delivered to the provider, explicitly describing the assistance to be furnished by the provider that has been approved by the Court.''.

SEC. 107. PROHIBITION ON WARRANTLESS ACQUISITION OF DOMESTIC COMMUNICATIONS PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

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

(1) in subsection (b)(4), by striking ''known at the time of the acquisition'' and inserting ''reason-

ably believed at the time of acquisition or communication'';

(2) in subsection (d)(1)(B), by striking ''known at the time of the acquisition'' and inserting ''reasonably believed at the time of the acquisition or communication'';

(3) in subsection (h)(2)(A)(i)(II), by striking ''known at the time of the acquisition'' and inserting ''reasonably believed at the time of the acquisition or communication''; and

(4) in subsection (j)(2)(B)(ii), by striking ''known at the time of the acquisition'' and inserting ''reasonably believed at the time of the acquisition or communication''.

SEC. 108. REQUIREMENT OF A FOREIGN INTELLIGENCE PURPOSE.

Section 702(h)(2)(A)(v) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(h)(2)(A)(v)) is amended by striking ''a significant'' and inserting ''the''.

SEC. 109. FOUR-YEAR EXTENSION OF SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) EXTENSION.—Section 403(b) of the FISA Amendments Act of 2008 (Public Law 110–261) is amended—

(1) in paragraph (1) (50 U.S.C. 1881–1881g note), by striking ''December 31, 2023'' and inserting ''September 30, 2027''; and

(2) in paragraph (2) (18 U.S.C. 2511 note), in the matter preceding subparagraph (A), by striking ''December 31, 2023'' and inserting ''September 30, 2027''.

(b) CONFORMING AMENDMENT.—The heading of section 404(b)(1) of the FISA Amendments Act of 2008 (Public Law 110–261; 50 U.S.C. 1801 note) is amended by striking ''DECEMBER 31, 2023'' and inserting ''SEPTEMBER 30, 2027''.

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

SEC. 201. COURT SUPERVISION OF COLLECTION TARGETING UNITED STATES PERSONS AND PERSONS LOCATED INSIDE THE UNITED STATES.

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

(1) by striking sections 703, 704, and 705 (50 U.S.C. 1881b, 1881c, and 1881d); and

(2) by inserting after section 702 (50 U.S.C. 1881a) the following:

"SEC. 703. ACQUISITIONS TARGETING UNITED STATES PERSONS AND PERSONS LOCATED INSIDE THE UNITED STATES.

''(a) WARRANT REQUIREMENT.—No officer or employee of the United States may intentionally target any United States person, regardless of location, or person reasonably believed to be located in the United States for the purpose of acquiring foreign intelligence information under circumstances in which the person has a reasonable expectation of privacy or a warrant would be required if

the officer or employee sought to compel production of the information inside the United States for law enforcement purposes, unless such person is the subject of—

''(1) an order or emergency authorization under section 105 or 304 of this Act covering the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such order or authorization; or

''(2) a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction covering the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such warrant.

''(b) PEN REGISTER TRAP AND TRACE.—No officer or employee of the United States may intentionally target any United States person, regardless of location, or person reasonably believed to be located in the United States for the purpose of collecting foreign intelligence information through the installation and use of pen register or trap and trace device, or to acquire information the compelled production of which would require a pen register or trap and trace device order if conducted inside the United States, unless such person is the subject of—

''(1) an order or emergency authorization under title IV of this Act covering the period of the acquisition and the acquisition is subject to the use, dissemination, querying, retention, and other minimization limitations required by such authorization; or

''(2) an order has been issued pursuant to section 3123 of title 18, United States Code, by a court of competent jurisdiction covering the period of the acquisition.

''(c) MATTERS RELATING TO EMERGENCY ACQUISITION.—In the event that an emergency acquisition is conducted pursuant to subsection (a)(1) or (b)(1) and the application for such emergency authorization is denied, or in any other case in which the acquisition has been conducted and no order is issued approving the acquisition—

''(1) no information obtained or evidence derived from such acquisition may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

''(2) no information concerning any United States person or person reasonably believed to be lo-

cated in the United States a may subsequently be used or disclosed in any other manner without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person.

''(d) RULE OF CONSTRUCTION.—Subsections (a) and (b) shall apply regardless of the location of the acquisition.''.

(b) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended—

(1) in section 601(a)(1) (50 U.S.C. 1871(a)(1)—

(A) by striking subparagraphs (D) through (F); and

(B) in subparagraph (B), by striking the semicolon and inserting ''; or'';

(2) in section 603(b)(1) (50 U.S.C. 1873(b)(1)), in the matter before subparagraph (A), by striking ''and sections 703 and 704''; and

(3) in section 706 (50 U.S.C. 1881e), by striking subsection (b).

(c) CLERICAL AMENDMENT.—The table of contents for such Act is amended—

(1) by striking the items relating to sections 703, 704, and 705; and

(2) by inserting after the item relating to section 702 the following:

''Sec. 703. Acquisitions targeting United States persons and persons located inside the United States.''.

SEC. 202. REQUIRED DISCLOSURE OF RELEVANT INFORMATION IN FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 APPLICATIONS.

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

''TITLE IX—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.''.

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

''TITLE IX—DISCLOSURE OF RELEVANT INFORMATION

''Sec. 901. Disclosure of relevant information.''.

SEC. 203. CERTIFICATION REGARDING ACCURACY PROCEDURES.

(a) CERTIFICATION REGARDING ACCURACY PROCEDURES.—Title IX of the Foreign Intelligence Surveillance Act of 1978, as added by section 202, 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, in-

cluding any application for renewal of an existing order, is accurate and complete, including procedures that ensure, at a minimum, that—

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

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

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

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

''(5) before any application targeting a United States person is made, the applicant Federal officer shall document that the officer has collected and re-

viewed for accuracy and completeness supporting documentation for each factual assertion in the application; and

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

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

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

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

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

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

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

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

(b) TECHNICAL AMENDMENT.—The table of contents of the Foreign Intelligence Surveillance Act of 1978, as amended by section 202, is amended by inserting after the item relating to section 901 the following:

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

SEC. 204. CLARIFICATION REGARDING TREATMENT OF INFORMATION AND EVIDENCE ACQUIRED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) IN GENERAL.—Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) is amended by adding at the end the following:

''(q) For the purposes of notification provisions of this Act, information or evidence is 'derived' from an elec-

tronic surveillance, physical search, use of a pen register or trap and trace device, production of tangible things, or acquisition under this Act when the Government would not have originally possessed the information or evidence but for that electronic surveillance, physical search, use of a pen register or trap and trace device, production of tangible things, or acquisition, and regardless of any claim that the information or evidence is attenuated from the surveillance or search, would inevitably have been discovered, or was subsequently reobtained through other means.''.

(b) POLICIES AND GUIDANCE.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Attorney General and the Director of National Intelligence shall publish the following:

(A) Policies concerning the application of subsection (q) of section 101 of such Act, as added by subsection (a).

(B) Guidance for all members of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) and all Federal agencies with law enforcement responsibilities concerning the application of such subsection (q).

(2) MODIFICATIONS.—Whenever the Attorney General and the Director modify a policy or guidance published under paragraph (1), the Attorney General and the Director shall publish such modifications.

SEC. 205. SUNSET ON GRANDFATHER CLAUSE OF SECTION 215 OF THE USA PATRIOT ACT.

Section 102(b)(2) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177; 50 U.S.C. 1805 note) is amended by inserting ", except that title V of the Foreign Intelligence Surveillance Act of 1978, as in effect on March 14, 2020, shall continue in effect until the date that is 180 days after the date of the enactment of the Government Surveillance Reform Act of 2023" after "continue in effect".

SEC. 206. WRITTEN RECORD OF DEPARTMENT OF JUSTICE INTERACTIONS WITH FOREIGN INTELLIGENCE SURVEILLANCE COURT; PROTECTION AGAINST JUDGE SHOPPING BY DOJ.

(a) TRANSCRIPTS OF PROCEEDINGS.—Subsection (c) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended—

(1) by inserting ", and shall be transcribed" before the first period; and

(2) by inserting ", transcriptions," after "applications made".

(b) WRITTEN RECORD OF INTERACTIONS WITH COURT.—Such section is further amended by adding at the end the following:

"(l) WRITTEN RECORD OF INTERACTIONS.—

"(1) WRITTEN COMMUNICATIONS.—The Attorney General shall maintain all written communications with the court established under subsection (a), including the identity of the employees of the court to or from whom the communications were made, regarding an application or order made under this title in a file associated with the application or order.

"(2) ORAL COMMUNICATIONS.—The Attorney General shall—

"(A) document a summary of any oral communications with the court established under subsection (a), including the identity of the employees of the court to or from whom the communications were made, relating to an application or order described in paragraph (1); and

"(B) keep such documentation in a file associated with the application or order.".

(c) EXTENSIONS OF ORDERS.—Section 105(d)(2) of such Act (50 U.S.C. 1805(d)(2)) is amended by adding at the end the following: ''To the extent practicable, an extension of an order issued under this title shall be granted or denied by the same judge who issued the original order.''.

SEC. 207. APPOINTMENT OF AMICI CURIAE AND ACCESS TO INFORMATION.

(a) EXPANSION OF APPOINTMENT AUTHORITY.—

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

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

''(A) shall appoint at least 1 individual who has been designated under paragraph (1) and who possesses expertise in privacy and civil liberties to serve as amicus curiae to assist such court in the consideration of any application or motion for an order or review, unless the court issues a written finding that such application neither presents nor involves—

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

''(ii) a significant concern related to constitutional rights;

''(iii) a sensitive investigative matter;

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

''(v) a request for reauthorization of programmatic surveillance; or

''(vi) any other privacy or civil liberties issue for which an appointment of an amicus curiae to assist the court in the consideration of the application would be appropriate; and'';

(B) in subparagraph (B), by striking ''an individual or organization'' each place it appears and inserting ''1 or more individuals or organizations'';

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

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

''(B) shall appoint at least 1 individual who has been designated under paragraph (1) and who possesses technical expertise to serve as amicus curiae to assist such court in the

consideration of any application for an order or review, unless the court issues a written finding that such application neither presents nor involves—

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

"(ii) a request for approval of a previously authorized program, technology, or use of existing technology for which no prior application for approval of such program, technology, or use was considered by the court with the assistance of an amicus curiae who possesses technical expertise; or

"(iii) a technical issue material to any legal determination for which an appointment of an amicus curiae who possesses technical expertise to assist the court in the consideration of the application would be appropriate;

"(C) shall randomly appoint at least 1 individual with legal expertise and at least 1 individual with technical expertise, from among individuals who have been designated under para-

graph (1), to assist the court in the review of a certification under section 702(j); and''.

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

''(12) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—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 inves-

tigative matter described in subparagraph (A).''.

(3) QUALIFICATIONS.—Section 103(i)(3)(A) of such Act (50 U.S.C. 1803(i)(3)(A)) is amended—

(A) by inserting ''cybersecurity, cryptography,'' after ''communications technology,''; and

(B) by adding at the end the following: ''Of such individuals, at least 1 shall possess legal expertise and at least 1 shall possess technical expertise.''.

(4) NOTIFICATION.—Section 103(i) of such Act (50 U.S.C. 1803(i)) is amended by striking paragraph (7) and inserting the following:

''(7) NOTIFICATION.—A presiding judge of a court established under subsection (a) or (b) shall, not less frequently than quarterly, provide to the Attorney General and the appropriate committees of Congress—

''(A) a notification of each appointment of an individual to serve as amicus curiae under paragraph (2); and

''(B) a copy of each written finding issued under paragraph (2).''.

(5) SECTION 702 RECERTIFICATION SCHEDULE.—Section 702(j)(5)(A) of such Act (50 U.S.C. 1881a(j)(5)(A)) is amended by striking ''at least 30 days prior to the expiration of such authorization'' and inserting ''such number of days, not less than 30 days, before the expiration of such authorization as the Court considers necessary to permit review by amici curiae appointed under section 103(i)(2)(C).''.

(6) CONFORMING AMENDMENTS.—Section 103(i) of such Act (50 U.S.C. 1803(i)) is amended—

(A) in paragraph (4), by striking ''amicus curiae under paragraph (2)(A)'' and inserting ''amicus curiae under subparagraph (A), (B), or (C) of paragraph (2)''; and

(B) in paragraph (5), by striking ''appointed under paragraph (2)(A)'' and inserting ''appointed under subparagraph (A), (B), or (C) of paragraph (2)''.

(b) AUTHORITY TO SEEK REVIEW.—Section 103(i) of such Act (50 U.S.C. 1803(i)), as amended by subsection (a), is further amended—

(1) in paragraph (4)—

(A) in the paragraph heading, by inserting ''; AUTHORITY'' after ''DUTIES'';

(B) by redesignating subparagraphs (A), (B), and (C) as clauses (i), (ii), and (iii), respectively, and moving such clauses, as so redesignated, 2 ems to the right;

(C) in the matter preceding clause (i), as so designated, by striking ''the amicus curiae shall'' and inserting the following: ''the amicus curiae—

''(A) shall'';

(D) in subparagraph (A)(i), as so designated, 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 affected by the application or motion''; and

(E) 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 affecting the legality of the proposed electronic surveillance with the court, regardless of whether the court has requested assistance on that issue.''.

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

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

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

"(A) FOREIGN INTELLIGENCE SURVEILLANCE COURT DECISIONS.—

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

"(ii) DENIALS.—If the Foreign Intelligence Surveillance Court denies a petition described in clause (i), the court shall provide for the record a written statement of the reasons for such denial.

"(iii) CERTIFICATION.—Upon certification of any question of law pursuant to this subparagraph, the Foreign Intelligence

Surveillance Court of Review shall appoint the amicus curiae to assist the Court of Review in its consideration of the certified question, unless the Court of Review issues a finding that such appointment is not appropriate.

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

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

(c) ACCESS TO INFORMATION.—

(1) APPLICATION AND MATERIALS.—Section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is amended—

(A) in subparagraph (A), by striking clauses (i) and (ii) and inserting the following:

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

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

''(II) any other information or materials that the court determines is relevant to the duties of the amicus curiae; and

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

''(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.'';

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

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

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

(2) CLARIFICATION OF ACCESS TO CERTAIN INFORMATION.—Section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is amended—

(A) in subparagraph (B), by striking ''may'' and inserting ''shall''; and

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

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

(3) CONSULTATION AMONG AMICI CURIAE.—Section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)), as amended by paragraphs (1) and (2), is further amended—

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

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

''(B) CONSULTATION.—If the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review determines that it is relevant to the duties of an amicus curiae appointed under paragraph (2), the amicus curiae may consult with 1 or more of the other individuals designated to serve as amicus curiae under paragraph (1) regarding any of the information relevant to any assigned proceeding.''.

SEC. 208. DECLASSIFICATION OF SIGNIFICANT DECISIONS, ORDERS, AND OPINIONS.

Section 602 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1872) is amended by striking subsection (a) and inserting the following:

''(a) DECLASSIFICATION REQUIRED.—

''(1) IN GENERAL.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall—

''(A) conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Re-

view (as defined in section 601(e)) that is described in paragraph (2);

"(B) consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion; and

"(C) complete the declassification review required by subparagraph (A) and public release of each such decision, order, or opinion pursuant to subparagraph (B) by not later than 180 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues such decision, order, or opinion.

"(2) DECISION, ORDER, OR OPINION DESCRIBED.—A decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that is described in this paragraph is any such decision, order, or opinion issued before, on, or after the date of the enactment of this Act that—

"(A) includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of any term; or

''(B) has been nominated for a declassification review by an amicus curiae appointed by the court.''.

SEC. 209. CLARIFICATION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT JURISDICTION OVER RECORDS OF THE COURT AND OTHER ANCILLARY MATTERS.

(a) IN GENERAL.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by sections 206 and 207, is further amended—

(1) by adding at the end the following:

''(m) ANCILLARY CLAIMS.—

''(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to hear claims ancillary to any of its own proceedings, including jurisdiction to hear any claim for access to the court's records, files, and proceedings under the Constitution of the United States, statute, common law, or any other authority. Upon deciding such a claim, such court shall provide immediately for the record a written statement of the reasons for such decision. A party may file a petition for review of such decision with the Foreign Intelligence Surveillance Court of Review, which shall have jurisdiction to consider such

petition and, upon deciding such petition, shall provide for the record a written statement of the reasons for its decision.

''(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The Foreign Intelligence Surveillance Court of Review shall have jurisdiction to hear claims ancillary to any of its own proceedings, including jurisdiction to hear any claim for access to the court's records, files, and proceedings under the Constitution of the United States, statute, common law, or any other authority. Upon deciding such a claim, such court shall provide immediately for the record a written statement of the reasons for such decision.

''(3) SUPREME COURT REVIEW.—A party may file a petition for a writ of certiorari for review of a decision of the Foreign Intelligence Surveillance Court of Review under paragraphs (1) or (2), and the Supreme Court shall have jurisdiction to review such decision.'';

(2) in subsection (a)(2)(A), in the matter preceding clause (i), by inserting ''paragraph (1) of subsection (l) of this section or'' before ''paragraph (4) or (5) of section 702(i)''; and

(3) in subsection (k)(1), by striking ''section 1254(2) of title 28'' and inserting ''section 1254 of title 28''.

(b) TECHNICAL CORRECTIONS.—Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803), as amended by section (a), is further amended—

(1) in subsection (a)(2)(A), in the matter preceding clause (i), by striking ''section 501(f) or''; and

(2) in subsection (e), by striking ''section 501(f)(1) or'' each place it appears.

SEC. 210. GROUNDS FOR DETERMINING INJURY IN FACT IN CIVIL ACTIONS RELATING TO SURVEILLANCE UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 OR PURSUANT TO EXECUTIVE AUTHORITY.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as amended by section 202, is further amended by adding at the end the following:

"TITLE X—ADDITIONAL MATTERS

"SEC. 1001. CHALLENGES TO GOVERNMENT SURVEILLANCE.

''(a) DEFINITIONS.—In this section, the terms 'foreign intelligence information', 'person', 'United States', and 'United States person' have the meaning given such terms in section 101.

''(b) INJURY IN FACT.—In any claim in a civil action brought in a court of the United States relating to the acquisition, copying, querying, retention, access, or use of information acquired under this Act or pursuant to any other authority of the executive branch of the Federal Government, by a United States person or person located inside the United States, the person asserting the claim has suffered an injury-in-fact traceable to that conduct if the person—

''(1)(A) regularly communicates foreign intelligence information with persons who are not United States persons and who are located outside the United States; and

''(B) has taken or is taking objectively reasonable measures to avoid the acquisition, copying, querying, retention, access, or use of the person's information under

this Act or pursuant to another authority of the executive branch of the Federal Government; or

''(2) has a reasonable basis to believe that the person's rights have been, are being, or imminently will be violated by an individual acting under color of Federal law.

''(c) REASONABLE BASIS.—For the purposes of this section, a reasonable basis exists when the person demonstrates a concrete injury arising from a good-faith belief that the person's rights have been, are being, or imminently will be violated through the acquisition, copying, querying, retention, access, or use of the person's information under this Act or pursuant to any other authority of the executive branch of the Federal Government.

''(d) STATE SECRETS PRIVILEGE ABROGATED.—The state secrets privilege is abrogated, and the procedure set forth in section 106(f) shall apply, with respect to any claim where the plaintiff, who is a United States person or person located in the United States, plausibly alleges an injury-in-fact relating to the acquisition, copying, querying, retention, access, or use of information acquired under this Act or pursuant to another authority of the executive branch of the Federal Government and plausibly alleges that the acquisition, copying, querying, retention,

access, or use of information violates the Constitution or laws of the United States.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Foreign Intelligence Surveillance Act of 1978, as amended by section 202, is further amended by adding at the end the following:

SEC. 211. ACCOUNTABILITY PROCEDURES FOR VIOLATIONS BY FEDERAL EMPLOYEES.

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

''SEC. 1002. ACCOUNTABILITY PROCEDURES FOR VIOLATIONS BY FEDERAL EMPLOYEES.

''(a) DEFINITIONS.—In this section:

''(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' has the meaning given such term in section 101.

''(2) COVERED AGENCY.—The term 'covered agency' means the Federal Bureau of Investigation, the Central Intelligence Agency, the National Security Agency, and the National Counterterrorism Center.

''(3) COVERED VIOLATION.—The term 'covered violation' means a violation of this Act or Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, by an employee of a covered agency that results in the inappropriate collection, use, querying, or dissemination of any communication, record, or information of a United States person or a person inside the United States.

''(4) PERSON, UNITED STATES, AND UNITED STATES PERSON.—The terms 'person', 'United States', and 'United States person' have the meanings given such terms in section 101.

''(b) ACCOUNTABILITY PROCEDURES; DESIGNATED INVESTIGATIVE ENTITY.—The head of each covered agency shall—

''(1) establish procedures to hold employees of the covered agency accountable for willful, knowing, reckless, and negligent covered violations; and

''(2)(A) designate an entity within the agency to investigate possible willful, knowing, reckless, and negligent covered violations; and

''(B) establish an internal process for the designated entity to determine culpability for willful, knowing, reckless, and negligent covered violations.

''(c) ELEMENTS.—The procedures established under subsection (b)(1) shall include the following:

''(1) Centralized tracking of individual employee performance incidents involving willful, knowing, reckless, and negligent covered violations, over time.

''(2) Escalating consequences for willful, knowing, reckless, and negligent covered violations, including—

''(A) consequences for an initial reckless or negligent covered violation, including, at a minimum—

''(i) suspension of access to information acquired under this Act or to the dataset that gave rise to the violation for not less than 90 days; and

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

''(B) consequences for a second reckless or negligent covered violation, including, at a minimum—

''(i) suspension of access to information acquired under this Act or to the dataset that gave rise to the violation for not less than 180 days; and

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

"(C) consequences for a third reckless or negligent covered violation, including, at a minimum—

"(i) termination of security clearance; and

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

"(D) consequences for an initial willful or knowing covered violation, including, at a minimum—

"(i) suspension of access to information acquired under this Act or to the dataset that gave rise to the violation for not less than 180 days; and

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

"(E) consequences for a second willful or knowing covered violation, including, at a minimum—

"(i) termination of security clearance; and

"(ii) reassignment or termination of each employee responsible for the violation.

''(d) PRESUMPTION OF TERMINATION.—

''(1) IN GENERAL.—For purposes of subparagraphs (C)(ii) and (E)(ii) of subsection (c)(2), there shall be a presumption in favor of termination of an employee.

''(2) JUSTIFICATION.—If the head of a covered agency determines not to terminate an employee for a third reckless or negligent violation under subparagraph (C)(ii) of subsection (c)(2) or a second willful or knowing violation under subparagraph (E)(ii) of that subsection, the agency head shall submit to the appropriate committees of Congress a written justification for the determination.

''(e) TIMING.—If a covered agency determines, through an investigation, that an employee committed a willful, knowing, reckless, or negligent covered violation, the agency head shall determine what consequences to impose on the employee under subsection (c)(2) not later than 60 days after the conclusion of the investigation.''.

(b) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 1001, as added by this title, the following:

''Sec. 1002. Accountability procedures for violations by Federal employees.''.

(c) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the head

of each covered agency, as defined in section 710 of the Foreign Intelligence Surveillance Act of 1978 (as added by subsection (a)), shall submit to the appropriate committees of Congress a report detailing—

(A) the procedures established under section 710 of the Foreign Intelligence Surveillance Act of 1978, as added by subsection (a); and

(B) a description of any actions taken pursuant to such procedures.

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

TITLE III—REFORMS RELATED TO SURVEILLANCE CONDUCTED UNDER EXECUTIVE ORDER 12333

SEC. 301. DEFINITIONS.

In this title:

(1) INTELLIGENCE, INTELLIGENCE COMMUNITY, AND FOREIGN INTELLIGENCE.—The terms ''intelligence'', ''intelligence community'', and ''foreign intelligence'' have the meanings given such

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

(2) ELECTRONIC SURVEILLANCE, PERSON, STATE, UNITED STATES, AND UNITED STATES PERSON.—The terms ''electronic surveillance'', ''person'', ''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).

SEC. 302. PROHIBITION ON WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) IN GENERAL.—Except as provided in subsections (b) and (c), no officer or employee of the Federal Government may conduct a query of information acquired pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, in an effort to find communications or information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information.

(b) CONCURRENT AUTHORIZATION, CONSENT, AND EXCEPTION FOR EMERGENCY SITUATIONS.—

(1) IN GENERAL.—Subsection (a) shall not apply to a query relating to United States person 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 if—

(A) such persons or person are the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105 or 304 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805, 1824), or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction covering the period of the query;

(B)(i) the officer or employee carrying out the query has a reasonable belief that—

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

(II) in order to prevent or mitigate this threat, the query must be conducted before authorization pursuant to subpara-

graph (A) can, with due diligence, be obtained; and

(ii) a description of the query is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner;

(C) such persons 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 query on a case-by-case basis; or

(D)(i) the query uses a known cybersecurity threat signature as a query term;

(ii) 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;

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

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

(2) LIMITATIONS.—

(A) USE IN SUBSEQUENT PROCEEDINGS AND INVESTIGATIONS.—No information re-

trieved pursuant to a query authorized by paragraph (1)(B) or evidence derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in a proceeding or investigation that arises from the threat that prompted the query.

(B) ASSESSMENT OF COMPLIANCE.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under subparagraphs (A).

(c) MATTERS RELATING TO EMERGENCY QUERIES.—

(1) TREATMENT OF DENIALS.—In the event that a query for communications or information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States relating to 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 communication, or creation of

the information is conducted pursuant to an emergency authorization described in subsection (b)(1)(A) and the application for such emergency authorization is denied, or in any other case in which the query has been conducted and no order is issued approving the query—

(A) no information obtained or evidence derived from such query may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

(B) no information concerning any United States person or person reasonably believed to be located in the United States at the time of acquisition or the time of communication or creation of the information acquired from such query may subsequently be used or disclosed in any other manner without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(2) ASSESSMENT OF COMPLIANCE.—Not less frequently than annually, the Attorney General shall assess compliance with the requirements under paragraph (1).

(d) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—This section shall not apply to queries of communications and information collected pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(e) FOREIGN INTELLIGENCE PURPOSE.—Except as provided in subsection (b)(1), no officer or employee of the United States may conduct a query of information acquired pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, in an effort to find information of our 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 communication or creation of the information unless the query is reasonably likely to retrieve foreign intelligence information.

(f) DOCUMENTATION.—No officer or employee of the Federal Government may conduct a query of information acquired pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, in an effort to find information

of or about 1 or more United States persons or persons reasonably believed to be located in the United States at the time of the query or the time of the communication or creation of the information unless first an electronic record is created, and a system, mechanism, or business practice is in place to maintain such record, that includes the following:

(1) Each term used for the conduct of the query.

(2) The date of the query.

(3) The identifier of the officer or employee.

(4) A statement of facts showing that the use of each query term included under paragraph (1) is reasonably likely to retrieve foreign intelligence information.

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

mation a query for which is otherwise prohibited under this sections.

SEC. 303. PROHIBITION ON REVERSE TARGETING OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.

(a) PROHIBITION ON ACQUISITION.—

(1) PROHIBITION WITH EXCEPTIONS.—No officer or employee of the United States may intentionally target, pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, any person if a significant purpose of the 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, communication, or the creation of the information as prohibited by Section 703 of the Foreign Intelligence Surveillance Act of 1978, as added by section 201 of this Act, unless—

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

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

(iii) a description of the targeting is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner; or

(B) the United States person or persons reasonably believed to be located in the United States at the time of acquisition, communication or creation of the information 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) LIMITATION ON EXCEPTION.—No information acquired pursuant to paragraph (1)(A) or evidence derived from such targeting may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in proceedings or investigations that arise from the threat that prompted the targeting.

(b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AND CRIMINAL WARRANTS.—This section shall not apply to—

(1) an acquisition carried out pursuant to both section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a), as amended by section 103 of this Act, and section 703(b)(2) of the Foreign Intelligence Surveillance Act of 1978, as added by section 201 of this Act;

(2) an acquisition authorized under section 105 or 304 of the Foreign Intelligence Surveillance act of 1978 (50 U.S.C. 1805 and 1824); or

(3) an acquisition pursuant to a warrant issued pursuant to the Federal Rules of Criminal Procedure.

SEC. 304. PROHIBITION ON INTELLIGENCE ACQUISITION OF UNITED STATES PERSON DATA.

(a) DEFINITIONS.—In this section:

(1) 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.

(2) 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 the time of acquisition of the covered data; or

(B) is a United States person.

(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 THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—An element of the intelligence community may acquire covered data if the data has been authorized

for collection pursuant to an order or emergency authorization pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or the Federal Rules of Criminal Procedure 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 community 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 United States Constitution, 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—

(A) there is a reasonable belief that—

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

(ii) in order to prevent or mitigate this threat, the acquisition must be conducted before authorization pursuant to paragraph (2) can, with due diligence, be obtained;

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

(C) the covered data is destroyed at such time as it is no longer necessary for such purpose; and

(D) a description of the acquisition is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner.

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

(A) each covered person linked or reasonably linked 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 acquire a dataset that includes covered data if the covered data is not reasonably segregable prior to ac-

quisition, 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 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

acquired in violation of subsection (b), such covered data shall be promptly 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, 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, 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 this title, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or title 18, United States Code.

SEC. 305. PROHIBITION ON THE WARRANTLESS ACQUISITION OF DOMESTIC COMMUNICATIONS.

(a) IN GENERAL.—No officer or employee of the United States may intentionally acquire pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order,

any communication as to which the sender and all intended recipients are known to be located in the United States at the time of acquisition or the time of communication except—

(1) as authorized under section 105 or 304 the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805 and 1824); or

(2) if—

(A) there is a reasonable belief that—

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

(ii) in order to prevent or mitigate this threat, the acquisition must be conducted before an authorization pursuant to the provisions of law cited in paragraph (1) can, with due diligence, be obtained; and

(B) a description of the acquisition is provided to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) in a timely manner.

(b) USE IN SUBSEQUENT PROCEEDINGS AND INVESTIGATIONS.—No information acquired pursuant to an

emergency described in subsection (a)(2) or information derived from such acquisition may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, except in a proceeding or investigation that arises from the threat that prompted the acquisition.

SEC. 306. DATA RETENTION LIMITS.

(a) PROCEDURES.—Each head of an element of the Intelligence Community shall develop and implement procedures governing the retention of information collected pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order.

(b) REQUIREMENTS.—

(1) COVERED INFORMATION DEFINED.—In this subsection, the term ''covered information'' includes—

(A) any information, including an encrypted communication, to, from, or pertaining to a United States person or person reasonably believed to be located in the United States at the time of acquisition, communica-

tion, or creation of the information that has been evaluated and is not specifically known to contain foreign intelligence information; and

(B) any unevaluated information, unless it can reasonably be determined that the unevaluated information does not contain communications to or from, or information pertaining to a United States person or person reasonably believed to be located in the United States at the time of acquisition, communication, or creation of the information.

(2) IN GENERAL.—The procedures developed and implemented pursuant to subsection (a) shall ensure, with respect to information described in such subsection, that covered information shall be destroyed within 5 years of collection unless the Attorney General determines in writing that—

(A) the information is the subject of a preservation obligation in pending administrative, civil, or criminal litigation, in which case the covered information shall be segregated, retained, and used solely for that purpose and shall be destroyed as soon as it is no longer required to be preserved for such litigation; or

(B) the information is being used in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat identified in section 706(a)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881e(a)(2)(B)), as amended by section 102.

SEC. 307. REPORTS ON VIOLATIONS OF LAW OR EXECUTIVE ORDER.

Section 511 of the National Security Act of 1947 (50 U.S.C. 3110) is amended by adding at the end the following:

''(c) PUBLIC AVAILABILITY.—The Director of National Intelligence shall make each report submitted under subsection (a) publicly available on an internet website, with such redactions as may be necessary to protect sources and methods.

''(d) DEPARTMENT OF JUSTICE REPORT.—The Attorney General, in consultation with the Director of National Intelligence, shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a version of the report described in subsection (a) that only addresses violations of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).''.

TITLE IV—INDEPENDENT OVERSIGHT

SEC. 401. INSPECTOR GENERAL OVERSIGHT OF ORDERS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) AUDIT.—Not later than 1 year after the date of the enactment of this Act, the Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community shall each initiate an audit of the applications for court orders made under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) and directives issued under section 702(i) of such Act by the Department or the element, respectively.

(b) SCOPE; CONTENTS.—In conducting an audit under subsection (a)—

(1) an Inspector General shall—

(A) review such sample of applications and directives described in such subsection as the Inspector General determines appropriate in order to carry out the objectives of this section;

(B) assess whether—

(i) adequate safeguards are in place to ensure that the assertions made in applications are scrupulously accurate;

(ii) adequate safeguards are in place to ensure that each application includes all material information, including any information that suggests that the court should deny the application or that the court should include one or more conditions in an order, as required under section 901 of the Foreign Intelligence Surveillance Act of 1978, as added by section 202(a); and

(iii) in the determination of the Inspector General, there are any other areas of potential risk or violation; and

(C) make recommendations to address any deficiencies identified by the Inspector General; and

(2) the Inspector General of the Department of Justice shall assess the information provided by the Department of Justice under section 903 and include a determination on the accuracy and completeness of the information provided under that section.

(c) REPORT.—

(1) IN GENERAL.—For each audit conducted by an Inspector General under subsection (a), such Inspector General shall submit to the persons specified in paragraph (2) a report of the audit, including

findings and recommendations of the Inspector General and any remediations taken by the Department or element, respectively.

(2) PERSONS SPECIFIED.—The persons specified in this paragraph are the following:

(A) The Attorney General.

(B) The Director of National Intelligence.

(C) The Privacy and Civil Liberties Oversight Board.

(D) The appropriate committees of Congress.

(E) The Foreign Intelligence Surveillance Court (as defined in section 601(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(e))).

(F) Any amicus curiae appointed under section 103(i)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)).

(d) COOPERATION.—The Attorney General and head of each element of the intelligence community shall ensure full and complete cooperation with the respective Inspector General conducting an audit under subsection (a), including by providing access to all evidence and information relevant to the assessments required under subsection

(b)(2), subject to such procedures as are necessary to protect the national security of the United States.

(e) AVAILABILITY TO THE PUBLIC.—The Inspector General of each element of the intelligence community shall each make publicly available on a website of the relevant element an unclassified version of any report submitted under subsection (c) by the respective Inspector General.

SEC. 402. DEPARTMENT OF JUSTICE INSPECTOR GENERAL REVIEW OF HIGH INTENSITY DRUG TRAFFICKING AREA SURVEILLANCE PROGRAMS.

(a) DEFINITION.—In this section:

(1) COVERED HIDTA SURVEILLANCE PROGRAM.—The term ''covered HIDTA surveillance program'' means a HIDTA surveillance program in which a non-Federal Government entity provides to law enforcement agencies access to a database maintained by that entity containing information on more than 1,000,000 United States persons or persons in the United States.

(2) HIDTA SURVEILLANCE PROGRAM.—The term ''HIDTA surveillance program'' means a program that—

(A) enables law enforcement agencies to share, query, receive, or process information on United States persons;

(B) is operated by, or receives funding from 1 or more high intensity drug trafficking areas; and

(C) is supported financially, in whole or in part, with Federal funds.

(3) UNITED STATES PERSON.—The term ''United States person'' has the meaning given the term in the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) REVIEW.—The Inspector General of the Department of Justice shall—

(1) in the case of a HIDTA surveillance program established before the date of the enactment of this Act, conduct a review of such HIDTA surveillance program—

(A) not later than 180 days after the earlier of—

(i) the date of the enactment of this Act; or

(ii) the date such HIDTA surveillance program becomes a covered HIDTA surveillance program; and

(B) not less frequently than once every 5 years for as long as such HIDTA surveillance program is a covered HIDTA surveillance program; and

(2) in the case of a HIDTA surveillance program established after the date of the enactment of this Act, conduct a review of such HIDTA surveillance program—

(A) not later than 180 days after the HIDTA surveillance program becomes a covered HIDTA surveillance program; and

(B) not less frequently than once every 5 years for as long as such HIDTA surveillance program is a covered HIDTA surveillance program.

SEC. 403. 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 subsection 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.''.

SEC. 404. CONGRESSIONAL OVERSIGHT OF GRANTS OF IMMUNITY BY THE ATTORNEY GENERAL FOR WARRANTLESS SURVEILLANCE ASSISTANCE.

(a) IN GENERAL.—Section 2511(2)(a) of title 18, United States Code, is amended by adding at the end the following:

''(iv) Not later than 30 days after providing a certification described in clause (B) of the first sentence of sub-

paragraph (ii) to a provider of wire or electronic communication service, an officer, employee, or agent thereof, a landlord, a custodian, or another person, the person providing the certification shall submit the certification to the appropriate committees of Congress, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''.

(b) ONGOING PROGRAMS.—

(1) DEFINITIONS.—In this subsection—

(A) the term ''appropriate committees of Congress'' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), as amended by section 2 of this Act;

(B) the terms ''electronic communication'', ''electronic communication service'', and ''wire communication'' have the meanings given such terms in section 2510 of title 18, United States Code; and

(C) the term ''ongoing certification'' means a certification described in clause (B) of the first sentence of section 2511(2)(a)(ii) of title 18, United States Code, pursuant to which a provider of wire or electronic communication service, an officer, employee, or agent thereof,

a landlord, a custodian, or another person is providing information, facilities, or technical assistance on the date of enactment of this Act.

(2) SUBMISSION.—Not later than 90 days after the date of enactment of this Act, the person that provided an ongoing certification to a provider of wire or electronic communication service, an officer, employee, or agent thereof, a landlord, a custodian, or another person shall submit the ongoing certification to the appropriate committees of Congress.

TITLE V—REFORMS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

SEC. 501. WARRANT PROTECTIONS FOR LOCATION INFORMATION, WEB BROWSING RECORDS, AND SEARCH QUERY RECORDS.

(a) HISTORICAL LOCATION, WEB BROWSING, AND SEARCH QUERIES.—

(1) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(A) in subsection (a)—

(i) in the subsection heading, by striking "CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS" and inserting "LOCATION INFORMATION, WEB BROWSING

RECORDS, SEARCH QUERY RECORDS, OR CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS''; and

(ii) in the first sentence, by inserting ''location information, a web browsing record, a search query record, or'' before ''the contents of a wire''; and

(B) in subsection (c)(1), in the matter preceding subparagraph (A), by inserting ''location information, a web browsing record, a search query record, or'' before ''the contents''.

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

(A) in the matter preceding paragraph (1), by inserting ''(a) IN GENERAL.—'' before ''As used'';

(B) in subsection (a), as so designated—

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

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

(iii) by adding at the end the following:

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

''(6) the term 'web browsing record'—

''(A) means a record that reveals, in part or in whole, the identity of a service provided by an online service provider, or the identity of a customer, subscriber, user, or device, for any attempted or successful communication or transmission between an online service provider and such a customer, subscriber, user, or device;

''(B) includes a record that reveals, in part or in whole—

''(i) the domain name, uniform resource locator, internet protocol address, or other identifier for a service provided by an online service provider with which a customer, subscriber, user, or device has exchanged or attempted to exchange a communication or transmission; or

''(ii) the network traffic generated by an attempted or successful communication

or transmission between a service provided by an online service provider and a customer, subscriber, user, or device; and

''(C) does not include a record that reveals information about an attempted or successful communication or transmission between a known service and a particular, known customer, subscriber, user, or device, if the record is maintained by the known service and is limited to revealing additional identifying information about the particular, known customer, subscriber, user, or device;

''(7) the term 'search query record'—

''(A) means a record that reveals a query term or instruction submitted, in written, verbal, or other format, by a customer, subscriber, user, or device to any service provided by an online service provider, including a search engine, voice assistant, chat bot, or navigation service; and

''(B) includes a record that reveals the response provided by any service provided by an online service provider to a query term or instruction by a customer, subscriber, user, or device;''; and

(C) by adding at the end the following:

''(b) RULE OF CONSTRUCTION.—Nothing in this section or section 2510 shall be construed to mean that a record may not be more than 1 of the following types of record:

''(1) The contents of a communication.

''(2) Location information.

''(3) A web browsing record.

''(4) A search query record.''.

(b) REAL-TIME SURVEILLANCE OF LOCATION INFORMATION.—

(1) IN GENERAL.—Section 3117 of title 18, United States Code, is amended—

(A) in the section heading, by striking ''**Mobile tracking devices**'' and inserting ''**Tracking orders**'';

(B) by striking subsection (b);

(C) by redesignating subsection (a) as subsection (c);

(D) by inserting before subsection (c), as so redesignated, the following:

''(a) IN GENERAL.—No officer or employee of a governmental entity may install or direct the installation of a tracking device, except pursuant to a warrant issued using the procedures described in the Federal Rules of

Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction.

''(b) EMERGENCIES.—

''(1) IN GENERAL.—Subject to paragraph (2), the prohibition under subsection (a) does not apply in a instance in which an investigative or law enforcement officer reasonably determines that—

''(A) a circumstance described in subparagraph (i), (ii), or (iii) of section 2518(7)(a) exists; and

''(B) there are grounds upon which a warrant could be issued to authorize the installation of the tracking device.

''(2) APPLICATION DEADLINE.—If a tracking device is installed under the authority under paragraph (1), an application for a warrant shall be made within 48 hours after the installation.

''(3) TERMINATION ABSENT WARRANT.—In the absence of a warrant, use of a tracking device under the authority under paragraph (1) shall immediately

terminate when the investigative information sought is obtained or when the application for the warrant is denied, whichever is earlier.

''(4) LIMITATION.—In the event an application for a warrant described in paragraph (2) is denied, or in any other case where the use of a tracking device under the authority under paragraph (1) is terminated without a warrant having been issued, the information obtained shall be treated as having been obtained in violation of this section, and an inventory describing the installation and use of the tracking device shall be served on the person named in the warrant application.'';

(E) in subsection (c), as so redesignated—

(i) in the subsection heading, by striking ''IN GENERAL'' and inserting ''JURISDICTION'';

(ii) by striking ''or other order'';

(iii) by striking ''mobile'';

(iv) by striking ''such order'' and inserting ''such warrant''; and

(v) by adding at the end the following: ''For purposes of this subsection, the installation of a tracking device occurs within the jurisdiction in which the device is

physically located when the installation is complete.''; and

(F) by adding at the end the following:

''(d) DEFINITIONS.—As used in this section—

''(1) the term 'computer' has the meaning given that term in section 1030(e);

''(2) the terms 'court of competent jurisdiction' and 'governmental entity' have the meanings given such terms in section 2711;

''(3) the term 'installation of a tracking device' means, whether performed by an officer or employee of a governmental entity or by a provider at the direction of a governmental entity—

''(A) the physical placement of a tracking device;

''(B) the remote activation of the tracking software or functionality of a tracking device; or

''(C) the acquisition of a radio signal transmitted by a tracking device; and

''(4) the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object, including a phone, wearable device, connected vehicle, or other computer owned, used, or possessed by the target of surveillance.''.

(2) CONFORMING AMENDMENTS.—

(A) The table of sections for chapter 205 of title 18, United States Code, is amended by striking the item relating to section 3117 and inserting the following:

"3117. Tracking orders.".

(B) Section 2510(12)(C) of title 18, United States Code, is amended to read as follows:

"(C) a communication from a lawfully installed tracking device (as defined in section 3117 of this title), if—

"(i) the tracking device is physically placed; or

"(ii) the tracking software or functionality of the tracking device is remotely activated and the communication is transmitted by the tracking software or functionality as a result of the remote activation; or".

(c) PROSPECTIVE SURVEILLANCE OF WEB BROWSING RECORDS AND LOCATION INFORMATION.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(i) PROSPECTIVE DISCLOSURE OF WEB BROWSING RECORDS.—

''(1) IN GENERAL.—A governmental entity may require the prospective disclosure by an online service provider of a web browsing record only pursuant to a warrant issued using the procedures described in subsection (a).

''(2) TIME RESTRICTIONS.—A warrant requiring the prospective disclosure by an online service provider of web browsing records may require disclosure of web browsing records for only a period as is necessary to achieve the objective of the disclosure, not to exceed 30 days from issuance of the warrant. Extensions of such a warrant may be granted, but only upon satisfaction of the showings necessary for issuance of the warrant in the first instance.

''(j) PROSPECTIVE DISCLOSURE OF LOCATION RECORDS.—A governmental entity may require the prospective disclosure by an online service provider of location information only pursuant to a warrant issued using the procedures described in subsection (a), that satisfies the restrictions imposed on warrants for tracking devices imposed by section 3117 of this title and rule 41 of the Federal Rules of Criminal Procedure.''.

SEC. 502. CONSISTENT PROTECTIONS FOR PHONE AND APP-BASED CALL AND TEXTING RECORDS.

Section 2703(c)(2)(C) of title 18, United States Code, is amended by striking ''local and long distance telephone connection records, or''.

SEC. 503. EMAIL PRIVACY ACT.

(a) SHORT TITLE.—This section may be cited as the ''Email Privacy Act''.

(b) VOLUNTARY DISCLOSURE CORRECTIONS.—Section 2702 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by striking ''while in electronic storage by that service'' and inserting ''that is in electronic storage with or otherwise stored, held, or maintained by that service'';

(B) in paragraph (2)—

(i) by striking ''to the public'';

(ii) by striking ''divulge'' and inserting ''disclose''; and

(iii) by striking ''which is carried or maintained on that service'' and inserting

''that is stored, held, or maintained by that service''; and

(C) in paragraph (3)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by striking ''a provider of'' and inserting ''a person or entity providing'';

(2) in subsection (b)—

(A) in the matter preceding paragraph (1), by inserting ''wire or electronic'' before ''communication'';

(B) by amending paragraph (1) to read as follows:

''(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication, or to an agent of such addressee, intended recipient, subscriber, or customer;''; and

(C) by amending paragraph (3) to read as follows:

''(3) with the lawful consent of the originator, addressee, or intended recipient of such communication, or of the subscriber or customer on whose be-

half the provider stores, holds, or maintains such communication;'';

(3) in subsection (c) by inserting ''wire or electronic'' before ''communications'';

(4) in each of subsections (b) and (c), by striking ''divulge'' and inserting ''disclose''; and

(5) in subsection (c), by amending paragraph (2) to read as follows:

''(2) with the lawful consent of the subscriber or customer;''.

(c) AMENDMENTS TO REQUIRED DISCLOSURE SECTION.—Section 2703 of title 18, United States Code, as amended by this Act, is amended—

(1) in subsection (a)—

(A) by striking ''A governmental entity'' and inserting ''Except as provided in subsections (l) and (m), a governmental entity'';

(B) by striking ''pursuant to'' and inserting ''if the governmental entity obtains''; and

(C) by striking ''by a court of competent jurisdiction.'' and inserting ''that is issued by a court of competent jurisdiction and that may indicate the date by which the provider must make the disclosure to the governmental entity. In the absence of a date on the warrant indi-

cating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.'';

(2) in subsection (c)—

(A) in paragraph (1)—

(i) in the matter preceding subparagraph (A)—

(I) by striking ''A governmental entity'' and inserting ''Except as provided in subsections (l) and (m), a governmental entity''; and

(II) by striking ''only when the governmental entity—'' and inserting ''only—''

(ii) in subparagraph (A)—

(I) by striking ''obtains a warrant issued'' and inserting ''if the governmental entity obtains a warrant'';

(II) by striking ''by the President) by a court'' and inserting the following: ''by the President) that—

''(i) is issued by a court'';

(III) by inserting ''and'' after ''jurisdiction;''; and

(IV) by adding at the end the following:

''(ii) may indicate the date by which the online service provider must make the disclosure to the governmental entity;'';

(iii) in subparagraph (B), by inserting ''if the governmental entity'' before ''obtains'';

(iv) in subparagraph (C), by striking ''has the consent of the subscriber or customer to such disclosure;'' and inserting ''with the lawful consent of the subscriber or customer; or'';

(v) by striking subparagraph (D);

(vi) by redesignating subparagraph (E) as subparagraph (D);

(vii) in subparagraph (D), as so redesignated, by striking ''seeks information'' and inserting ''as otherwise authorized''; and

(B) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by inserting '', in response to an administrative subpoena authorized by Federal or State statute, a grand jury,

trial, or civil discovery subpoena, or any means available under paragraph (1),'' after ''shall''; and

(ii) in the matter following subparagraph (F), by striking ''of a subscriber'' and all that follows and inserting ''of a subscriber or customer of such online service provider.'';

(3) in subsection (d)—

(A) by striking ''the contents of a wire or electronic communication, or'';

(B) by striking ''sought,'' and inserting ''sought''; and

(C) by striking ''section'' and inserting ''subsection''; and

(4) by adding after subsection (j), as added by section 501(c) of this Act, the following:

''(k) NOTICE.—Except as provided in section 2705, an online service provider may notify a subscriber or customer of a receipt of a warrant, court order, subpoena, or request under subsection (a), (c), or (d) of this section.

''(l) RULE OF CONSTRUCTION RELATED TO LEGAL PROCESS.—Nothing in this section or in section 2702 shall limit the authority of a governmental entity to use an administrative subpoena authorized by Federal or

State statute, a grand jury, trial, or civil discovery subpoena, or a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction to—

''(1) require an originator, addressee, or intended recipient of a wire or electronic communication that is not acting as an online service provider with regard to that wire or electronic communication to disclose a wire or electronic communication (including the contents of that communication) to the governmental entity;

''(2) require a person or entity that provides an electronic communication service to the officers, directors, employees, or agents of the person or entity (for the purpose of carrying out their duties) to disclose a wire or electronic communication (including location information, a web browsing record, a search query record, or the contents of that communication) to or from the person or entity itself or to or from an officer, director, employee, or agent of the entity to a governmental entity, if the wire or electronic communication is stored, held, or maintained on an electronic communications system

owned, operated, or controlled by the person or entity; or

''(3) require an online service provider to disclose a wire or electronic communication (including the contents of that communication) that advertises or promotes a product or service and that has been made readily accessible to the general public.

''(m) RULE OF CONSTRUCTION RELATED TO CONGRESSIONAL SUBPOENAS.—Nothing in this section or in section 2702 shall limit the power of inquiry vested in the Congress by article I of the Constitution of the United States, including the authority to compel the production of a wire or electronic communication (including location information, a web browsing record, a search query record, or the contents of a wire or electronic communication) that is stored, held, or maintained by an online service provider.''.

(d) WARRANT REQUIREMENT FOR STORED COMMUNICATIONS CONTENT.—

(1) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(A) in subsection (a)—

(i) by striking '', that is in electronic storage in an electronic communications

system for one hundred and eighty days or less,''; and

(ii) by striking the last sentence;

(B) by striking subsection (b) and inserting the following:

''(b) [Repealed].''; and

(C) in subsection (d) by striking ''(b) or''.

(2) CONFORMING AMENDMENTS.—Chapter 121 of title 18, United States Code, is amended—

(A) in the table of sections, by striking the item relating to section 2704;

(B) in section 2701(c)(3), by striking '', 2704'';

(C) by striking section 2704; and

(D) in section 2706(a), by striking '', 2703, or 2704'' and inserting ''or 2703''.

SEC. 504. CONSISTENT PROTECTIONS FOR DEMANDS FOR DATA HELD BY INTERACTIVE COMPUTING SERVICES.

(a) DEFINITION.—Subsection (a) of section 2711 of title 18, United States Code, as so designated and amended by section 501 of this Act, is amended by adding at the end the following:

''(8) the term 'online service provider' means a provider of electronic communication service, a pro-

vider of remote computing service, or a provider of an interactive computer service (as defined in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f))); 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''.

SEC. 505. CONSISTENT PROTECTIONS FOR REAL-TIME AND HISTORICAL METADATA.

Chapter 206 of title 18, United States Code, is amended—

(1) in section 3122(b)(2), by striking ''that the information likely to be obtained is relevant'' and inserting ''providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained is relevant and material''; and

(2) in section 3123(a)—

(A) in paragraph (1), in the first sentence—

(i) by striking ''the court shall enter'' and inserting ''the court may enter''; and

(ii) by striking ''certified to the court that the information likely to be obtained by such installation and use is relevant'' and inserting ''submitted a certification providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained by such installation and use is relevant and material''; and

(B) in paragraph (2)—

(i) by striking ''the court shall enter'' and inserting ''the court may enter''; and

(ii) by striking ''certified to the court that the information likely to be obtained by such installation and use is relevant'' and inserting ''submitted a certification providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained by such installation and use is relevant and material''.

SEC. 506. SUBPOENAS FOR CERTAIN SUBSCRIBER INFORMATION.

Section 2703(c)(2) of title 18, United States Code, is amended, in the matter following subparagraph (F), as amended by section 503(c) of this Act, by inserting ''with respect to whom the governmental entity identifies the name, address, temporarily assigned network address, or account identifier (such as a user name)'' before the period at the end.

SEC. 507. MINIMIZATION STANDARDS FOR VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall

issue and make publicly available minimization procedures applicable to disclosures to a Federal agency under paragraph (5) or (8) of subsection (b) or paragraph (3) or (4) of subsection (c) of section 2702 of title 18, United States Code.

(b) CONTENTS.—The procedures issued under subsection (a) shall include provisions to—

(1) limit, to the greatest extent possible, the acquisition, use, and dissemination of the contents of communication and records and other information to that which is required for the specific purpose for which the disclosure was intended;

(2) to the greatest extent possible, remove personally identifiable information prior to acquisition;

(3) to the extent personally identifiable information cannot be removed prior to acquisition, mask such information prior to its use or dissemination, consistent with the purpose for which the disclosure was intended; and

(4) ensure that no contents of communications or records or other information are retained by the agency to which the disclosure was made, or any agency to which the contents of communications or records or other information were disclosed, after

the completion of the investigation or action for which the disclosure was intended.

SEC. 508. PROHIBITION 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 particular 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 data that is lawfully available through Federal, State, or local government records or through widely distributed media.

''(2) LIMITATION.—

''(A) IN GENERAL.—

''(i) PROHIBITION.—Subject to clauses (ii) through (vii), 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 organiza-

tion 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 employee 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.

"(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.

"(4) PROHIBITION ON USE AS EVIDENCE BY COVERED GOVERNMENTAL ENTITIES.—

"(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, trial, hearing, or other

proceeding by, 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 (vii) of subsection (e)(2)(A) from the data obtained; and

"(B) to remove and delete covered personal data described in subparagraph (A) after a compilation 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 paragraph (2)(B), 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 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 officer or employee of a covered governmental entity carrying out the query has a reasonable belief that the life or safety of such covered person is threatened and the information is sought for the purpose of assisting that person, in which case information resulting from the query may be accessed or used solely for that purpose and shall be destroyed at such time as it is no longer necessary for such purpose; or

''(iii) such covered person has consented to the query.

''(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; and

''(ii) any personal data of covered persons returned pursuant to a query shall not be reviewed and shall immediately be destroyed.''.

SEC. 509. CONSISTENT PRIVACY PROTECTIONS FOR DATA HELD BY DATA BROKERS.

Section 2703 of title 18, United States Code, as amended by section 503 of this Act, is amended by adding at the end the following:

''(n) 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. 510. PROTECTION OF DATA ENTRUSTED TO INTERMEDIARY OR ANCILLARY SERVICE PROVIDERS.

(a) DEFINITION.—Subsection (a) of section 2711 of title 18, United States Code, as so designated and amended by sections 501 and 504 of this Act, is amended by adding at the end the following:

''(9) 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 communica-

tion 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)).''.

SEC. 511. MODERNIZING CRIMINAL SURVEILLANCE REPORTS.

(a) REPORTS CONCERNING ACCESS TO CUSTOMER COMMUNICATIONS OR RECORDS.—

(1) IN GENERAL.—Section 2703 of title 18, United States Code, as amended by section 509 of this Act, is amended by adding at the end the following:

''(o) REPORTS CONCERNING ACCESS TO CUSTOMER COMMUNICATIONS OR RECORDS.—

''(1) IN GENERAL.—In January of each year, any judge who has issued an order under this section or a warrant to obtain records described in this section, or who has denied approval of an application under this section during the preceding year, shall report to the Administrative Office of the United States Courts—

"(A) the fact that the order or warrant was applied for;

"(B) the type of records sought in the order or warrant;

"(C) whether the order or warrant was—

"(i) granted as applied for;

"(ii) granted as modified; or

"(iii) denied;

"(D) the subsection of this section under which the application for the order or warrant was filed;

"(E) the nature of the offense or criminal investigation that was the basis for the application for the order or warrant;

"(F) the name of each provider of electronic communication service or remote computing service served with the order or warrant, if so granted; and

"(G) the investigative or law enforcement agency that submitted the application.

"(2) PUBLIC REPORT.—In June of each year, the Director of the Administrative Office of the United States Courts shall publish on the website of the Administrative Office of the United States

Courts and include in the report required under section 2519(3)—

"(A) a full and complete report concerning the number of applications for orders or warrants requiring the disclosure of, during the preceding calendar year—

"(i) the contents of wire or electronic communications in electronic storage under subsection (a); and

"(ii) records concerning electronic communication service or remote computer service under subsection (c);

"(B) the number of orders and warrants granted or denied under this section during the preceding calendar year; and

"(C) a detailed summary and analysis of each category of data required to be filed with the Administrative Office of the United States Courts under paragraph (1).

"(3) FORMAT.—Not later than 180 days after the date of enactment of the Government Surveillance Reform Act of 2023, the Director of the Administrative Office of the United States Courts shall, in consultation with the National Institute of Standards and Technology, the Administrator of General

Services, the Electronic Public Access Public User Group, private entities offering electronic case management software, the National Center for State Courts, and the National American Indian Court Judges Association, publish a machine readable form that shall be used for any report required under paragraph (1).

''(4) REGULATIONS.—The Director of the Administrative Office of the United States Courts may issue binding regulations with respect to the content and form of the reports required under paragraph (1).''.

(2) TECHNICAL AND CONFORMING AMENDMENT.—Section 2519(3) of title 18, United States Code, is amended, in the first sentence, by inserting ''publish on the website of the Administrative Office of the United States Courts and'' before ''transmit''.

(b) REPORTS CONCERNING PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 3126 of title 18, United States Code, is amended to read as follows:

''§ 3126. Reports concerning pen registers and trap and trace devices

''(a) IN GENERAL.—In January of each year, any judge who has issued an order (or an extension thereof) under section 3123 that expired during the preceding

year, or who has denied approval of an installation and use of a pen register or trap and trace device during that year, shall report to the Administrative Office of the United States Courts—

''(1) the fact that an order or extension was applied for;

''(2) the kind of order or extension applied for;

''(3) the fact that the order or extension was granted as applied for, was modified, or was denied;

''(4) the period of installation and use of a pen register or trap and trace device authorized by the order, and the number and duration of any extensions of the order;

''(5) the offense specified in the order or application, or extension of an order;

''(6) the precise nature of the facilities affected and the precise nature of the information sought; and

''(7) the investigative or law enforcement agency that submitted the application.

''(b) PUBLIC REPORT.—In June of each year, the Director of the Administrative Office of the United States Courts shall publish on the website of the Administrative Office of the United States Courts and include in the report required under section 2519(3)—

''(1) a full and complete report concerning—

''(A) the number of applications for orders authorizing or approving the installation and use of a pen register or trap and trace device pursuant to this chapter; and

''(B) the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year; and

''(2) a detailed summary and analysis of each category of data required to be reported under subsection (a).

''(c) FORMAT.—Not later than 180 days after the date of enactment of the Government Surveillance Reform Act of 2023, the Director of the Administrative Office of the United States Courts shall, in consultation with the National Institute of Standards and Technology and the Administrator of General Services, private entities offering electronic case management software, the National Center for State Courts, and the National American Indian Court Judges Association, publish a machine readable form that shall be used for any report required under subsection (a).

''(d) REGULATIONS.—The Director of the Administrative Office of the United States Courts may issue binding regulations with respect to the content and form of the reports required under subsection (a).''.

(c) REPORTING OF VOLUNTARY DISCLOSURES.—Section 2702(d) of title 18, United States Code, is amended—

(1) in the heading, by striking ''EMERGENCY'' and inserting ''VOLUNTARY'';

(2) in the matter preceding paragraph (1), by inserting ''and publish on the website of the Department of Justice'' after ''Senate''; and

(3) in paragraph (1)—

(A) by striking ''the Department of Justice'' and inserting ''each Federal agency''; and

(B) by striking ''subsection (b)(8)'' and inserting ''paragraph (5) or (8) of subsection (b) or paragraph (3) or (4) of subsection (c), broken down by each such paragraph'';

(4) in paragraph (2)(A)—

(A) by striking ''Department of Justice'' and inserting ''Federal agency''; and

(B) by striking ''subsection (b)(8)'' and inserting ''paragraph (5) or (8) of subsection (b) or paragraph (3) or (4) of subsection (c)''; and

(5) by striking paragraph (3).

TITLE VI—REGULATION OF GOVERNMENT SURVEILLANCE USING CELL SITE SIMULATORS, GENERAL PROHIBITION ON PRIVATE, NON-RESEARCH USE

SEC. 601. CELL SITE SIMULATORS.

(a) PROHIBITION.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3119. Cell-site simulators

"(a) GENERAL PROHIBITION OF USE.—

"(1) IN GENERAL.—Except as provided in subsection (d), it shall be unlawful—

"(A) for any individual or entity to knowingly use a cell-site simulator in the United States; or

"(B) for an element of the intelligence community to use a cell-site simulator outside the United States if the subject of the surveillance is a United States person.

"(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to authorize a law enforcement agency of a governmental entity to use a cell-site simulator outside the United States.

''(b) PENALTY.—Any individual or entity that violates subsection (a)(1) shall be fined not more than $250,000.

''(c) PROHIBITION OF USE AS EVIDENCE.—

''(1) IN GENERAL.—Except as provided in paragraph (2), no information acquired through the use of a cell-site simulator in violation of subsection (a)(1), and no evidence derived therefrom, may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding by, 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.

''(2) EXCEPTION FOR ENFORCEMENT.—Information acquired through the use of a cell-site simulator in violation of subsection (a)(1) by a person, and evidence derived therefrom, may be used, received in evidence, or otherwise disseminated in any investigation trial, hearing, or other proceeding described in paragraph (1) of this subsection relating to the alleged violation of subsection (a)(1) in connection with such use.

''(d) EXCEPTIONS.—

''(1) IN GENERAL.—

"(A) WARRANT.—

"(i) IN GENERAL.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity under a warrant issued—

"(I) in accordance with this subparagraph; and

"(II) using the procedures described in, and in accordance with the requirements for executing and returning a warrant under, the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant and execution and return procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title and in accordance with the requirements for executing and returning such a warrant, in accordance with regulations prescribed by the President) by a court of competent jurisdiction.

''(ii) REQUIREMENTS.—A court may issue a warrant described in clause (i) (except, with respect to a State court, to the extent use of a cell-site simulator by a law enforcement agency of a governmental entity is prohibited by the law of the State) only if the law enforcement agency—

''(I) demonstrates that other investigative procedures, including electronic location tracking methods that solely collect records of the investigative target—

''(aa) have been tried and have failed; or

''(bb) reasonably appear to be—

''(AA) unlikely to succeed if tried; or

''(BB) too dangerous;

''(II) specifies the likely area of effect of the cell-site simulator to be used and the time that the cell-site simulator will be in operation;

''(III) certifies that the requested area of effect and time of operation

are the narrowest reasonably possible to obtain the necessary information; and

''(IV) demonstrates that the requested use of a cell-site simulator would be in compliance with applicable provisions of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and the rules of the Federal Communications Commission.

''(iii) CONSIDERATIONS.—In considering an application for a warrant described in clause (i), the court shall—

''(I) consider—

''(aa) the number of individuals impacted;

''(bb) the nature of any communications to be obtained; and

''(cc) the type of activities in which users of an electronic device are engaged;

''(II) direct the law enforcement agency of the governmental entity to take steps to ensure heightened pro-

tections for constitutionally protected activities and to minimize the collection of information relating to individuals who are not the subject of the warrant;

''(III) weigh the need of the government to enforce the law and apprehend criminals against the likelihood and impact of any potential negative side effects, including those disclosed by the government under subparagraph (C); and

''(IV) not grant a request for a warrant that would put public safety at risk or unreasonably inconvenience the community.

''(iv) PERIOD OF INITIAL AUTHORIZATION.—No warrant described in clause (i) may authorize the use of a cell site simulator for any period longer than is necessary to achieve the objective of the authorization, nor in any event for longer than 30 days.

''(v) EXTENSIONS.—

"(I) IN GENERAL.—A court may grant extensions of a warrant described in clause (i), but only upon application for an extension made in accordance with clause (i) and the court considering the factors described in clause (iii) and determining the requirements under clause (ii) are met.

"(II) PERIOD OF EXTENSION.—The period of an extension of a warrant shall be no longer than the authorizing judge determines necessary to achieve the purposes for which the extension was granted, nor in any event for longer than 30 days.

"(vi) TERMINATION PROVISION.—Each warrant described in clause (i), and each extension thereof, shall contain a provision that the authorization to use the cell site simulator shall be executed as soon as practicable and shall terminate upon attainment of the authorized objective, or in any event in 30 days.

"(vii) START OF 30-DAY PERIODS.—The 30-day periods described in clauses

(iv), (v)(II), and (vi) shall begin on the earlier of—

"(I) the date on which a law enforcement agency first begins to use the cell site simulator as authorized by the warrant, or extension thereof; or

"(II) the date that is 10 days after the warrant, or extension thereof, is issued.

"(B) EMERGENCY.—

"(i) IN GENERAL.—Subject to clause (ii), subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity, or use of a cell-site simulator as part of assistance provided by a component of the Department of Defense or an Armed Force to such a law enforcement agency, if—

"(I) the governmental entity reasonably determines an emergency exists that—

"(aa) involves—

"(AA) immediate danger of death or serious physical injury to any person;

"(BB) conspiratorial activities characteristic of organized crime; or

"(CC) an immediate threat to a national security interest; and

"(bb) requires use of a cell-site simulator before a warrant described in subparagraph (A) can, with due diligence, be obtained; and

"(II) except in an instance in which the governmental entity is trying to locate a lost or missing person, locate someone believed to have been abducted or kidnaped, or find victims, dead or alive, in an area where a natural disaster, terrorist attack, or other mass casualty event has taken place—

"(aa) there are grounds upon which a warrant described

in subparagraph (A) could be entered to authorize such use; and

''(bb) the governmental entity applies for a warrant described in subparagraph (A) approving such use not later than 48 hours after such use begins, and takes such steps to expedite the consideration of such application as may be possible.

''(ii) TERMINATION OF EMERGENCY USE.—

''(I) IN GENERAL.—A law enforcement agency of a governmental entity shall immediately terminate use of a cell-site simulator under clause (i) of this subparagraph at the earlier of the time the information sought is obtained or the time the application for a warrant described in subparagraph (A) is denied.

''(II) WARRANT DENIED.—If an application for a warrant described in clause (i)(II)(bb) is denied—

"(aa) any information or evidence derived from use of the cell-site simulator shall be subject to subsection (c);

"(bb) the attorney for the governmental entity submitting the application shall—

"(AA) retain, until the date that is 1 year after the date of the denial, a single copy of any information or evidence derived from use of the cell-site simulator for potential use by a person about whose electronic device the government obtained information with the cell site simulator, which may not be used for any other purpose; and

"(BB) promptly destroy any other copies of such information or evidence; and

"(cc) the applicable law enforcement agency shall serve no-

tice in accordance with subparagraph (D).

''(C) DISCLOSURES REQUIRED IN APPLICATION.—In any application for a warrant authorizing the use of a cell-site simulator under subparagraph (A) or (B), the governmental entity shall include the following:

''(i) A disclosure of any potential disruption of the ability of the subject of the surveillance or bystanders to use commercial mobile radio services or private mobile services, including using advanced communications services, to make or receive, as applicable—

''(I) emergency calls (including 9–1–1 calls);

''(II) calls to the universal telephone number within the United States for the purpose of the national suicide prevention and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act of 1934 (47 U.S.C. 251(e));

"(III) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71);

"(IV) calls using telecommunications relay services; or

"(V) any other communications or transmissions.

"(ii) A certification that the specific model of the cell-site simulator to be used has been inspected by a third party that is an accredited testing laboratory recognized by the Federal Communications Commission to verify the accuracy of the disclosure under clause (i).

"(iii) A disclosure of the methods and precautions that will be used to minimize disruption, including—

"(I) any limit on the length of time the cell-site simulator can be in continuous operation; and

"(II) any user-defined limit on the transmission range of the cell-site simulator.

''(iv) A disclosure as to whether the cell-site simulator will be used in an area or at a gathering where constitutionally protected activity, including speech or religious observance, will occur.

''(v) A disclosure as to whether sensitive matters, such as attorney-client communications, political campaign or political party deliberations, medical information, or communications among elected political representatives of a State or the Federal Government, will be implicated.

''(vi) A disclosure as to the estimated number of individuals whose communications, electronic device, or location information will be implicated.

''(D) NOTICE.—

''(i) IN GENERAL.—Notice regarding the use of a cell-site simulator shall include an inventory, containing—

''(I) the fact of the entry of the warrant or the application;

''(II) the date of the entry and the period of authorized, approved or

disapproved use of a cell-site simulator, or the denial of the application;

"(III) whether, during the period—

"(aa) information about their electronic device was, or was not, obtained by the government;

"(bb) their location was, or was not, tracked; and

"(cc) their communications were, or were not, intercepted; and

"(IV) confirmation that all information unrelated to the individual towards whom the warrant was directed has been destroyed.

"(ii) PROVISION OF NOTICE TO OTHER PARTIES.—The court issuing a warrant authorizing the use of a cell-site simulator may also require that notice be provided to other persons not named in the application, whose electronic devices the governmental entity obtained information with the cell site simulator.

''(2) FOREIGN INTELLIGENCE SURVEILLANCE.—Use of a cell-site simulator by an element of the intelligence community shall not be subject to subsection (a)(1) if it is conducted in a manner that is in accordance with title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) (including testing or training authorized under paragraph (1) or (3) of section 105(g) of such Act (50 U.S.C. 1805(g)) (including such testing or training conducted in conjunction with a component of the Department of Defense or an Armed Force), if any information obtained during such testing or training (including metadata) is destroyed after its use for such testing or training).

''(3) RESEARCH.—Subsection (a)(1) shall not apply to the use of a cell-site simulator in order to engage, in good-faith, in research or teaching by a person that is not—

''(A) a law enforcement agency of a governmental entity;

''(B) an element of the intelligence community; or

''(C) acting as an agent thereof.

''(4) PROTECTIVE SERVICES.—

"(A) IN GENERAL.—Subsection (a)(1) shall not apply to the use of a cell-site simulator in the performance of protective duties pursuant to section 3056 of this title or as otherwise authorized by law.

"(B) PROHIBITION ON USE AS EVIDENCE.—No information acquired through the use of a cell-site simulator under the authority under subparagraph (A), and no evidence derived therefrom, may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding by, 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.

"(C) NO BAR TO OTHER AUTHORIZED USE.—Nothing in subparagraph (A) or (B) shall be construed to prohibit the United States Secret Service from using a cell-site simulator in accordance with a provision of this section other than subparagraph (A).

"(5) CONTRABAND INTERDICTION BY CORRECTIONAL FACILITIES.—Subsection (a)(1) shall not apply to the use of a contraband interdiction system

if the correctional facility or the entity operating the contraband interdiction system for the benefit of the correctional facility—

"(A) has—

"(i) taken reasonable steps to restrict transmissions by the contraband interdiction system to cellular devices physically located within the property of the correctional facility;

"(ii) posted signs around the correctional facility informing visitors and staff that the correctional facility employs such a contraband interdiction system; and

"(iii) complied with any relevant regulations promulgated by the Federal Communications Commission and, as applicable, policies issued by the National Telecommunications and Information Administration;

"(B) annually tests and evaluates compliance with subparagraph (A) in accordance with best practices, which shall be issued by the Federal Communications Commission; and

"(C) not later than 10 business days after identifying an issue relating to the use of the

contraband interdiction system, whether in the course of normal business operations or conducting testing and evaluation, submits to the Federal Communications Commission a report describing the issues identified and the steps taken to address the issues.

''(6) TESTING AND TRAINING BY LAW ENFORCEMENT.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by a law enforcement agency of a governmental entity in the normal course of official duties that is not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

''(A) test the capability of electronic equipment, if—

''(i) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

''(ii) the test is limited in extent and duration to that necessary to determine to capability of the equipment;

''(iii) any information obtained during such testing (including metadata) is retained and used only for the purpose of de-

termining the capability of the equipment, is disclosed only to test personnel, and is destroyed before or immediately upon completion of the test; and

''(iv) the test is for a period of not longer than 90 days, unless the law enforcement agency obtains the prior approval of the Attorney General; or

''(B) train law enforcement personnel in the use of electronic surveillance equipment, if—

''(i) it is not reasonable to—

''(I) obtain the consent of the persons incidentally subjected to the surveillance;

''(II) train persons in the course of otherwise authorized law enforcement activities; or

''(III) train persons in the use of such equipment without engaging in surveillance;

''(ii) such surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

"(iii) any information obtained during such training (including metadata) is destroyed after its use for such training.

"(7) FCC TESTING.—Subsection (a)(1) shall not apply to the use of a cell-site simulator by the Federal Communications Commission, or an accredited testing laboratory recognized by the Federal Communications Commission, in order to test the cell-site simulator.

"(8) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to exempt a State or local government from complying with regulations promulgated by the Federal Communications Commission, including the requirement to obtain authorization to transmit on spectrum regulated by the Federal Communications Commission.

"(e) LIMIT ON CERTAIN USE NOT CONDUCTED PURSUANT TO WARRANTS AND ORDERS.—The use of a cell-site simulator under subsection (d)(1)(B) of this section (which shall not include such a use by a component of the Department of Defense or an Armed Force providing assistance to a law enforcement agency of a governmental entity under such subsection (d)(1)(B)), under section 105(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)), or under clause (i) or (ii) of

section 102(a)(1)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802(a)(1)(A)) may only be carried out lawfully using a specific model of a cell-site simulator for which the disclosures required under clauses (i) and (ii) of subsection (d)(1)(C) were included with respect to the specific model in connection with—

"(1) for use by an element of the intelligence community under title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), an application for an order under such Act that was approved; or

"(2) for use by a law enforcement agency of a governmental entity, an application for a warrant—

"(A) under the Federal Rules of Criminal Procedure that was approved by a judge of the judicial district in which the law enforcement agency intends to use the cell-site simulator; or

"(B) using State warrant procedures that was approved by a judge of the State in which the law enforcement agency intends to use the cell-site simulator.

"(f) MINIMIZATION.—

"(1) IN GENERAL.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention,

provide for the destruction, and prohibit the dissemination, of information obtained through the use of a cell-site simulator under an exception under paragraph (1) or (2) of subsection (d) that pertains to any person who is not an authorized subject of the use.

''(2) PUBLICATION.—The Attorney General shall make publicly available on the website of the Department of Justice the procedures adopted under paragraph (1) and any revisions to such procedures.

''(3) USE BY AGENCIES.—If a law enforcement agency of a governmental entity or element of the intelligence community acquires information pertaining to a person who is not an authorized subject of the use of a cell-site simulator under an exception under paragraph (1) or (2) of subsection (d), the law enforcement agency or element of the intelligence community shall—

''(A) minimize the acquisition and retention, and prohibit the dissemination, of the information in accordance with the procedures adopted under paragraph (1); and

''(B) destroy the information (including metadata) at the earliest possible opportunity.

''(g) DISCLOSURE TO DEFENDANT.—Any information acquired through the operation of a cell-site simulator, or derived from such information, including the fact that the information was obtained or derived, as the case may be, from a cell-site simulator, shall be disclosed to the defendant in any action in which the information is introduced into evidence.

''(h) SCOPE OF COLLECTION.—

''(1) AUTHORIZED USE.—Information collected under this section may only include information identifying nearby electronic devices communicating with the cell-site simulator and the strength and direction of transmissions from those electronic devices.

''(2) COMPLIANCE WITH WIRETAPPING REQUIREMENTS TO OBTAIN CONTENTS.—In the case of any interception of a wire or electronic communication by the cell-site simulator—

''(A) with respect to an interception by a law enforcement agency of a governmental entity, the provisions of chapter 119 shall apply in addition to the provisions of this section; and

''(B) with respect to an interception by an element of the intelligence community targeted against a United States person or person lo-

cated in the United States, the element of the intelligence community may only conduct the surveillance using the cell-site simulator in accordance with an order authorizing the use issued in accordance with title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), in addition to complying with the provisions of this section.

''(3) COMPLIANCE WITH TRACKING DEVICE REQUIREMENTS.—

''(A) IN GENERAL.—If a cell-site simulator is to be used by a law enforcement agency of a governmental entity to locate or track the movement of a person or object, the provisions of section 3117 and rule 41 of the Federal Rules of Criminal Procedure shall apply in addition to the provisions of this section.

''(B) COURT.—For purposes of applying section 3117 and rule 41 of the Federal Rules of Criminal Procedure to the use of a cell-site simulator, a Federal court may authorize such use within the jurisdiction of the court, and outside that jurisdiction if—

''(i) the use commences within that jurisdiction; or

''(ii) at the time the application is presented to the court, the governmental entity certifies that it has probable cause to believe that the target is physically located within that jurisdiction.

''(i) CIVIL ACTION.—Any person subject to an unlawful operation of a cell-site simulator may bring a civil action for appropriate relief (including declaratory and injunctive relief, actual damages, statutory damages of not more than $500 for each violation, and attorney fees) against the person, including a governmental entity, that conducted that unlawful operation.

''(j) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this section, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is war-

ranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

''(k) DEFINITIONS.—As used in this section—

''(1) the terms defined in section 2711 have, respectively, the definitions given such terms in that section;

''(2) the term 'advanced communications services' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

''(3) the term 'cell-site simulator' means any device that functions as or simulates a base station for commercial mobile services or private mobile services in order to identify, locate, or intercept transmissions from cellular devices for purposes other than providing ordinary commercial mobile services or private mobile services;

''(4) the term 'commercial mobile radio service' has the meaning given that term in section 20.3 of title 47, Code of Federal Regulations, or any successor thereto;

''(5) the term 'contraband interdiction system' means any device that functions as or simulates a base station for commercial mobile services or private mobile services for purposes of identifying, locating, or intercepting transmissions from contraband cellular devices in correctional facilities;

''(6) the term 'derived' means, with respect to information or evidence, that the government would not have originally possessed the information or evidence but for the use of a cell-site simulator, and regardless of any claim that the information or evidence is attenuated from the surveillance would inevitably have been discovered, or was subsequently reobtained through other means;

''(7) the term 'electronic communication' has the meaning given that term in section 2510;

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

''(9) the term 'emergency call' has the meaning given that term in section 6001 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1401);

''(10) the term 'intelligence community' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003);

''(11) the term 'mitigation' means the deletion of all information collected about a person who is not the subject of the warrant or investigation;

''(12) the term 'private mobile service' has the meaning given that term in section 332 of the Communications Act of 1934 (47 U.S.C. 332);

''(13) the term 'telecommunications relay service' has the meaning given that term in section 225 of the Communications Act of 1934 (47 U.S.C. 225); and

''(14) the term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''.

(b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 REQUIREMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) in section 101 (50 U.S.C. 1801), as amended by section 203 of this Act, by adding at the end the following:

''(r) 'Cell-site simulator' has the meaning given that term in section 3119 of title 18, United States Code.'';

(2) in section 102(a) (50 U.S.C. 1802(a)), by adding at the end the following:

''(5) The Government may only use a cell-site simulator pursuant to the authority under clause (i) or (ii) of paragraph (1)(A) without obtaining an order under this title authorizing such use if the Government has implemented measures that are reasonably likely to limit the collection activities to—

''(A) means of communications used exclusively between or among foreign powers, as defined in paragraph (1), (2), or (3) of section 101(a); or

''(B) property or premises under the open and exclusive control of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a).''; and

(3) in section 105 (50 U.S.C. 1805), by adding at the end the following:

''(k)(1) A judge having jurisdiction under section 103 may issue an order under this section that authorizes the use of a cell-site simulator only if the applicant—

''(A) demonstrates that other investigative procedures, including electronic location tracking methods that solely collect records of the investigative target—

''(i) have been tried and have failed; or

''(ii) reasonably appear to be—

''(I) unlikely to succeed if tried; or

''(II) too dangerous;

''(B) specifies the likely area of effect of the cell-site simulator to be used and the time that the cell-site simulator will be in operation;

''(C) certifies that the requested area of effect and time of operation are the narrowest reasonably possible to obtain the necessary information;

''(D) specifies the procedures in place to ensure that information unrelated to the target of the application will be promptly destroyed; and

''(E) demonstrates that the requested use of a cell-site simulator would be in compliance with applicable provisions of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and the rules of the Federal Communications Commission.

''(2) In any application for an order under this section authorizing the use of a cell-site simulator, the applicant shall include the following:

''(A) A disclosure of any potential disruption of the ability of the subject of the surveillance or bystanders to use commercial mobile radio services or private mobile services, including using advanced communications services, to make or receive, as applicable—

''(i) emergency calls (including 9–1–1 calls);

''(ii) calls to the universal telephone number within the United States for the purpose of the national suicide

prevention and mental health crisis hotline system under designated under paragraph (4) of section 251(e) of the Communications Act of 1934 (47 U.S.C. 251(e));

''(iii) calls to the nationwide toll-free number for the poison control centers established under section 1271 of the Public Health Service Act (42 U.S.C. 300d–71);

''(iv) calls using telecommunications relay services; or

''(v) any other communications or transmissions.

''(B) A certification that the specific model of the cell-site simulator to be used has been inspected by a third party that is an accredited testing laboratory recognized by the Federal Communications Commission to verify the accuracy of the disclosure under paragraph (1).

''(C) A disclosure of the methods and precautions that will be used to minimize disruption, including—

''(i) any limit on the length of time the cell-site simulator can be in continuous operation; and

''(ii) any user-defined limit on the transmission range of the cell-site simulator.

''(D) A disclosure as to whether the cell-site simulator will be used in an area or at a gathering where constitutionally protected activity, including speech or religious observation, will occur.

''(E) A disclosure as to whether sensitive matters, such as attorney-client communications, political cam-

paign or political party deliberations, medical information, or communications among elected political representatives of a State or the Federal Government, will be implicated.

''(F) A disclosure as to the estimated number of individuals whose communications, devices, or location information will be implicated.

''(3) In considering an application for an order under this section that authorizes the use of a cell-site simulator, the court shall—

''(A) consider—

''(i) the number of individuals impacted;

''(ii) the nature of any communications to be obtained; and

''(iii) the type of activities in which users of an electronic device (as defined in section 3119(k) of title 18, United States Code) are engaged;

''(B) direct the Government to take steps to ensure heightened protections for constitutionally protected activities and to minimize the collection of any information relating to individuals for whom the Government has not established probable cause as to their status as a foreign power or an agent of a foreign power;

''(C) weigh the need of the Government to obtain the information sought against the likelihood and impact of

any potential negative side effects, including those disclosed by the Government under paragraph (2); and

''(D) not grant a request for an order that would put public safety at risk or unreasonably inconvenience the community.''.

(c) CONFORMING AMENDMENT.—Section 3127 of title 18, United States Code, is amended—

(1) in paragraph (3) by striking ''but such term does not include any'' and inserting ''except such term does not include any cell-site simulator, as that term is defined in section 3119, or''; and

(2) in paragraph (4) by striking ''of any communication'' and inserting ''of any communication, except such term does not include any cell-site simulator, as that term is defined in section 3119''.

(d) INSPECTOR GENERAL REPORTS.—

(1) DEFINITION.—In this subsection, the term ''covered Federal entity'' means—

(A) a law enforcement agency of a department or agency of the Federal Government; and

(B) an element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(2) REPORTS.—The Inspector General of the Department of Justice, the Inspector General of the

Department of Homeland Security, the Inspector General of the Department of Defense, and the Inspector General of the Intelligence Community shall annually submit to Congress a joint report, and publish an unclassified version of the report on the website of each such inspector general, on—

(A) the overall compliance of covered Federal entities with this title and the amendments made by this title;

(B) the number of applications by covered Federal entities for use of a cell-site simulator that were applied for and the number that were granted;

(C) the number of emergency uses of a cell-site simulator under section 3119(d)(1)(B) of title 18, United States Code, as added by this title;

(D) the number of such emergency uses for which a court subsequently issued a warrant authorizing the use and the number of such emergency uses in which an application for a warrant was denied;

(E) the number of devices that were targeted with a cell-site simulator, which shall be provided separately for targeting conducted

pursuant to a warrant or court order and targeting conducted pursuant to an authority to use a cell-site simulator without a warrant or order;

(F) the number of devices that were not the target of the use of a cell-site simulator about which information was obtained with the cell-site simulator, which shall—

(i) be provided separately for use conducted pursuant to a warrant or court order and use conducted pursuant to an authority to use a cell-site simulator without a warrant or order; and

(ii) include the number of such devices about which the information was not destroyed as a result of the minimization requirements under section 3119(f) of title 18, United States Code, as added by this section, which shall be provided separately for use conducted pursuant to a warrant or court order and use conducted pursuant to an authority to use a cell-site simulator without a warrant or order;

(G) which components of a law enforcement agency of a department or agency of the

Federal Government are using cell-site simulators and how many are available to that component; and

(H) instances in which a law enforcement agency of a department or agency of the Federal Government made cell-site simulators available to a State or unit of local government.

(3) FORM OF REPORTS.—Each report submitted under paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(e) FCC REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Federal Communications Commission shall initiate any proceeding that may be necessary to promulgate or modify regulations promulgated by the Federal Communications Commission to implement this title and the amendments made by this title.

(2) CONSTRUCTION.—Nothing in this title or an amendment made by this title shall be construed to expand or contract the authority of the Federal Communications Commission.

(f) EFFECTIVE DATE.—

(1) IN GENERAL.—Except as provided in paragraph (2), subsections (a), (b), (c), and (d) of this section, and the amendments made by such subsections, shall apply on and after the date that is 2 years after the date of enactment of this Act.

(2) EXCEPTIONS.—

(A) DEFINITION.—In this paragraph, the term ''cell-site simulator'' has the meaning given that term in section 3119 of title 18, United States Code, as added by subsection (a).

(B) EXTENSION FOR EXISTING CELL-SITE SIMULATORS.—For any model of a cell-site simulator in use before the date of enactment of this Act, including such use in a contraband interdiction system at a correctional facility, if the Attorney General certifies that additional time is necessary to obtain independent tests of the model of cell-site simulator, subsections (a), (b), (c), and (d) of this section, and the amendments made by such subsections, shall apply to the use of the model of cell-site simulator on and after the date that is 3 years after the date of enactment of this Act.

TITLE VII—PROTECTION OF CAR DATA FROM WARRANTLESS SEARCHES

SEC. 701. PROTECTION OF CAR DATA FROM WARRANTLESS SEARCHES.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by adding at the end the following:

"CHAPTER 124—ACCESSING VEHICLE DATA.

"§ 2730. Definitions

"In this chapter:

"(1) ACCESS.—The term 'access'—

"(A) means any retrieval of covered vehicle data, regardless of—

"(i) whether the data is obtained as the information is being produced or from digital storage; and

"(ii) where the vehicle data is stored or transmitted, including by wire or radio; and

"(B) does not include data covered by chapter 119 of this title or section 104 of the

Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804).

''(2) CONSENT.—The term 'consent'—

''(A) means an affirmative, express, and voluntary agreement that—

''(i) states that the person providing the consent is providing consent to a government official to access the digital contents, access credential, or online account information, or other information being sought;

''(ii) specifies the type of content, access credential, or online account information the person is providing access to;

''(iii) specifies the time period of the covered vehicle data to be accessed;

''(iv) informs the person providing consent that consent is optional and that the government official attempting to obtain consent must otherwise acquire a warrant if consent is not obtained;

''(v) does not involve sanctions or the threat of sanctions for withholding consent; and

''(vi) uses clear, simple, and comprehensible language that is presented in a way that is accessible to the person providing consent; and

''(B) does not include consent obtained through agreement to a generic privacy policy.

''(3) COVERED VEHICLE DATA.—The term 'covered vehicle data'—

''(A) means all onboard and telematics data generated by, processed by, or stored on a noncommercial vehicle using computing, storage and communication systems installed, attached to, or carried in the vehicle, including diagnostic data, entertainment system data, navigation data, images or data captured by onboard sensors, or cameras, including images or data used to support automated features or autonomous driving, internet access, and communication to and from vehicle occupants;

''(B) includes data gathered by event data recorders; and

''(C) does not include—

''(i) automotive software installed by the manufacturer, as defined by applicable industry standards or regulations;

"(ii) any data subject to chapter 119 of this title or section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804); or

"(iii) data that is collected from outside the vehicle, including speed data and geolocation data, for purposes of traffic, law enforcement, or toll collection.

"(4) EVENT DATA RECORDER.—The term 'event data recorder' has the meaning given the term in section 563.5 of title 49, Code of Federal Regulations (as in effect on March 5, 2019).

"(5) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term 'investigative or law enforcement officer' means any officer of the United States or of a State or political subdivision thereof and any Tribal justice official, who is empowered by law to execute searches, to seize evidence, or to make arrests for a violation of Federal or State law.

"(6) NONCOMMERCIAL VEHICLE.—The term 'noncommercial vehicle' has the meaning given the term 'non-CMV' in section 383.5 of title 49, Code of Federal Regulations.

''(7) STATE.—The term 'State' means any State of the United States, the District of Columbia, and any territory or possession of the United States.

''(8) VEHICLE OPERATOR.—The term 'vehicle operator' means—

''(A) a person who controls the operation of a vehicle at the time consent is sought; and

''(B) with respect to a vehicle that is not classified as a highly autonomous vehicle by the Secretary of Transportation, the driver of the vehicle.

"§ 2731. Prohibition on access to vehicle data

''(a) IN GENERAL.—Except as provided in subsection (b), an investigative or law enforcement officer may not access covered vehicle data unless pursuant to a warrant issued in accordance with the procedures described in rule 41 of the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction, or as otherwise provided in this chapter or sections 104 and 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804, 1823).

''(b) EXCEPTIONS.—

''(1) CONSENT.—

"(A) IN GENERAL.—An investigative or law enforcement officer may access covered vehicle data if—

"(i) the vehicle operator provides prior consent to such access; and

"(ii) no passenger 14 years of age or older objects to the access.

"(B) VEHICLE OWNER.—If the vehicle operator cannot be located with reasonable effort, the vehicle owner or, in the case of a leased vehicle, the lessee, may provide consent under this paragraph.

"(C) UNLAWFUL POSSESSION.—No individual may provide or withhold consent under this paragraph or object to another individual accessing covered vehicle data if the individual—

"(i) is the vehicle operator who is in unlawful possession of the vehicle; or

"(ii) is a passenger who unlawfully obtained access to the vehicle.

"(D) ORAL CONSENT.—Consent provided under this paragraph shall be in writing unless—

"(i) the person providing the consent requests that the consent be made orally; and

"(ii) the request for consent and the consent are recorded.

"(E) CONSENT OF VEHICLE OPERATOR.—If the vehicle operator is not the owner of the vehicle and provides consent under this paragraph, the consent is valid only with respect to covered vehicle data generated during the lawful possession and use of the vehicle by the vehicle operator.

"(2) EMERGENCY.—

"(A) IN GENERAL.—An investigative or law enforcement officer, the Attorney General, the Deputy Attorney General, the Associate Attorney General, or the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, may access covered vehicle data if—

"(i) such officer reasonably determines that an emergency situation exists that—

''(I) involves immediate danger of death or serious physical injury to any person; and

''(II) requires access to covered vehicle data before such officer can, with due diligence, obtain a warrant;

''(ii) there are grounds upon which a warrant could be granted to authorize such access; and

''(iii) an application for a warrant approving such access is submitted to a court within 48 hours after the access has occurred or begins to occur.

''(B) DENIAL.—If an application for a warrant submitted pursuant to subparagraph (A)(iii) is denied, any covered vehicle data accessed under this paragraph shall be treated as having been obtained in violation of this chapter.

''(3) EVENT DATA RECORDER FOR MOTOR VEHICLE SAFETY.—In addition to the exceptions in paragraphs (1) and (2), data recorded or transmitted by an event data recorder may be accessed from a noncommercial vehicle if authorized by para-

graph (3), (4), or (5) of section 24302(b) of the Driver Privacy Act of 2015 (49 U.S.C. 30101 note).

''(4) RULE OF CONSTRUCTION.—Nothing in this section shall be interpreted to require the transmission or storage of data that is not otherwise transmitted or stored, or the retrieval of data that is not generally retrievable.

''§ 2732. Prohibition on use of acquired information as evidence

''(a) IN GENERAL.—If any covered vehicle data has been acquired in violation of this chapter, no part of such information and no evidence derived therefrom may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding by, 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) PROBABLE CAUSE.—No data described in section 2731(b)(3) may be used to establish probable cause.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) DRIVER PRIVACY ACT OF 2015.—Section 24302 of the Driver Privacy Act of 2015 (49 U.S.C. 30101 note) is amended—

(A) in subsection (b), in the matter preceding paragraph (1), by striking ''Data'' and inserting ''Except as provided in subsection (c), data''; and

(B) by adding at the end the following:

''(c) INVESTIGATIVE OR LAW ENFORCEMENT OFFICERS.—An investigative or law enforcement officer may only access or retrieve data recorded or transmitted by an event data recorder described in subsection (a) in accordance with chapter 124 of title 18, United States Code.''.

(2) TABLE OF CHAPTERS.—The table of chapters for part 1 of title 18, United States Code, is amended by adding at the end the following:

''124. Accessing vehicle data ..... 2730''.

TITLE VIII—INTELLIGENCE TRANSPARENCY

SEC. 801. ENHANCED ANNUAL REPORTS BY DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.

Section 603(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1873(a)(1)) is amended—

(1) in subparagraph (E), by striking ''; and'' and inserting a semicolon;

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

(3) by adding at the end the following:

"(G) the number of certifications by the Foreign Intelligence Surveillance Court pursuant to section 103(j);

"(H) the number of petitions to certify a question made by an amicus curiae pursuant to section 103(i)(7)(A);

"(I) the number of hearings or rehearings by the Foreign Intelligence Surveillance Court en banc pursuant to section 103(a)(2), disaggregated by hearings or rehearings by such court en banc pursuant to clause (i) or (ii) of such section; and

"(J) the number of times amici curiae have been appointed pursuant to section 103(i)(2).".

SEC. 802. ENHANCED ANNUAL REPORTS BY DIRECTOR OF NATIONAL INTELLIGENCE.

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

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

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

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

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

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

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

(4) by adding at the end the following:

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

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

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

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

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

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

''(12)(A) 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 that required a warrant pursuant to section 302; and

''(B) 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 that did not require a warrant pursuant to section 302; and

''(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 pursuant to Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, outside the authorities provided by this Act.''.

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

(1) by striking paragraph (2); and

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

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

SEC. 803. ANNUAL REPORTING ON ACCURACY AND COMPLETENESS OF APPLICATIONS.

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

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

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

''(e) ANNUAL REPORT BY ATTORNEY GENERAL ON ACCURACY AND COMPLETENESS OF APPLICATIONS.—

''(1) REPORT REQUIRED.—In April each year, the Attorney General shall submit to the appropriate committees of Congress and publish on the website of the Department of Justice, subject to a declassification review, a report setting forth, with respect to the preceding calendar year, the following:

''(A) A summary of all accuracy or completeness reviews of applications for court orders submitted to the Foreign Intelligence Surveillance Court by the Federal Bureau of Investigation under this Act.

''(B) The total number of such applications reviewed for accuracy or completeness.

''(C) The total number of material errors or omissions identified during such reviews.

"(D) The total number of nonmaterial errors or omissions identified during such reviews.

"(E) The total number of instances in which facts contained in an application were not supported by documentation that existed in the applicable file being reviewed at the time of the review.

"(F) An explanation for any increase or decrease in the number of errors identified under subparagraphs (C) and (D), and in the event of an increase in the number of errors, a description of any action taken by the Department to improve compliance and accuracy.

"(2) INSPECTOR GENERAL RISK ASSESSMENT.—In addition to conducting audits under section 401 of the Government Surveillance Reform Act of 2023, the Inspector General of the Department of Justice shall—

"(A) periodically assess the reports required by paragraph (1); and

"(B) as determined by the Inspector General, report any risks identified through such assessments to the appropriate committees of Congress.

''(3) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term 'appropriate committees of Congress' has the meaning given that term in section 101.''.

SEC. 804. ALLOWING MORE GRANULAR AGGREGATE REPORTING BY RECIPIENTS OF FOREIGN INTELLIGENCE SURVEILLANCE ORDERS.

(a) MODIFICATION OF AGGREGATION BANDING.—Subsection (a) of section 604 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1874) is amended—

(1) by striking paragraphs (1) through (3) and inserting the following:

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

''(A) the number of national security letters received, reported—

''(i) for the first 1000 national security letters received, in bands of 200 starting with 1–200; and

''(ii) for more than 1000 national security letters received, the precise number of national security letters received;

''(B) the number of customer selectors targeted by national security letters, reported—

''(i) for the first 1000 customer selectors targeted, in bands of 200 starting with 1–200; and

''(ii) for more than 1000 customer selectors targeted, the precise number of customer selectors targeted;

''(C) the number of orders or directives received, combined, under this Act for contents—

''(i) reported—

''(I) for the first 1000 orders and directives received, in bands of 200 starting with 1–200; and

''(II) for more than 1000 orders and directives received, the precise number of orders received; and

''(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702;

''(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents—

''(i) reported—

''(I) for the first 1000 customer selectors targeted, in bands of 200 starting with 1–200; and

''(II) for more than 1000 customer selectors targeted, the precise number of customer selectors targeted; and

''(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702;

''(E) the number of orders or directives received under this Act for noncontents—

''(i) reported—

''(I) for the first 1000 orders or directives received, in bands of 200 starting with 1–200; and

''(II) for more than 1000 orders or directives received, the precise number of orders received; and

''(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702; and

''(F) the number of customer selectors targeted under orders or directives under this Act for noncontents—

"(i) reported—

"(I) for the first 1000 customer selectors targeted, in bands of 200 starting with 1–200; and

"(II) for more than 1000 customer selectors targeted, the precise number of customer selectors targeted; and

"(ii) disaggregated by whether the order or directive was issued under section 105, 402, or 702."; and

(2) by redesignating paragraph (4) as paragraph (2).

(b) ADDITIONAL DISCLOSURES.—Such section is amended—

(1) by redesignating subsections (b) through (d) as subsections (c) through (e), respectively; and

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

"(b) ADDITIONAL DISCLOSURES.—A person who publicly reports information under subsection (a) may also publicly report, using a semiannual report, information relating to the previous 180 days that indicates whether the person was or was not required to comply with an order, directive, or national security letter issued under each of

sections 105, 402, and 702 and the provisions listed in section 603(f)(3).''.

(c) CONFORMING AMENDMENTS.—Subsection (c) of such section, as redesignated by subsection (b)(1) of this section, is amended—

(1) in paragraph (1), by striking ''or (2)'';

(2) by striking paragraph (2);

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

(4) in paragraph (2), as so redesignated, by striking ''(4)'' and inserting ''(2)''.

SEC. 805. REPORT ON USE OF FOREIGN INTELLIGENCE SURVEILLANCE AUTHORITIES REGARDING PROTECTED ACTIVITIES AND PROTECTED CLASSES.

(a) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Privacy and Civil Liberties Oversight Board shall make publicly available and submit to the appropriate committees of Congress a report on the use of activities and protected classes described in subsection (b) in—

(1) applications for orders made by the United States Government under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.); and

(2) investigations for which such orders are sought.

(b) ACTIVITIES AND PROTECTED CLASSES DESCRIBED.—The activities and protected classes described in this subsection are the following:

(1) Activities and expression protected by the First Amendment to the Constitution of the United States.

(2) Race, ethnicity, national origin, and religious affiliation.

(c) FORM.—In addition to the report made publicly available and submitted under subsection (a), the Board may submit to the appropriate committees of Congress a classified annex.

SEC. 806. PUBLICATION OF ESTIMATES REGARDING COMMUNICATIONS COLLECTED UNDER CERTAIN PROVISIONS OF FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall publish a good faith estimate of—

(1) the number of United States persons whose communications are collected under section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a); or

(2) the number of communications collected under such section to which a party is a person located in the United States at the time of communication.

SEC. 807. ENHANCED REPORTING OF ASSESSMENTS OF COMPLIANCE WITH EMERGENCY ORDER REQUIREMENTS UNDER CERTAIN PROVISIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) ELECTRONIC SURVEILLANCE.—

(1) ANNUAL ASSESSMENT.—Section 105(e)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(6)) is amended by striking ''shall assess compliance'' and inserting ''shall not less frequently than annually assess compliance''.

(2) REPORTING.—Section 108(a)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1808(a)(2)) is amended—

(A) in subparagraph (C), by striking ''; and'' and inserting a semicolon;

(B) in subparagraph (D), by striking ''section 301(e).'' and inserting ''section 304(e); and''; and

(C) by adding at the end the following:

''(E) the annual assessment conducted pursuant to section 105(e)(6).''.

(b) PHYSICAL SEARCHES.—

(1) ANNUAL ASSESSMENT.—Section 304(e)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(e)(6)) is amended by striking ''shall assess compliance'' and inserting ''shall not less frequently than annually assess compliance''.

(2) REPORTING.—Section 306 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1826) is amended—

(A) in paragraph (3), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (4), by striking the period and inserting ''; and''; and

(C) by adding at the end the following:

''(5) the annual assessment conducted pursuant to section 304(e)(6).''.

TITLE IX—SEVERABILITY AND LIMITED DELAYS IN IMPLEMENTATION

SEC. 901. SEVERABILITY.

If any provision of this Act, an amendment made by this Act, or the application of such a provision or amendment to any person or circumstance, is held to be uncon-

stitutional, the remaining provisions of and amendments made by this Act, and the application of the provision or amendment held to be unconstitutional to any other person or circumstance, shall not be affected thereby.

SEC. 902. LIMITED DELAYS IN IMPLEMENTATION.

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.

○