

118TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself and Mr. LEE) introduced the following bill; which
was read twice and referred to the Committee on _____

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Government Surveillance Reform Act of 2023”.

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

Sec. 1. Short title; table of contents.

2

Sec. 2. Definitions.

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.
- 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.
- Sec. 103. Repeal of authority for the resumption of abouts collection.
- Sec. 104. Prohibition on reverse targeting of United States persons and persons located in the United States.
- Sec. 105. Data retention limits for information collected under section 702 of the Foreign Intelligence Surveillance Act of 1978.
- 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.
- Sec. 107. Prohibition on warrantless acquisition of domestic communications pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978.
- Sec. 108. Requirement of a foreign intelligence purpose.
- Sec. 109. Four-year extension of section 702 of the Foreign Intelligence Surveillance Act of 1978.

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.
- Sec. 202. Required disclosure of relevant information in Foreign Intelligence Surveillance Act of 1978 applications.
- Sec. 203. Certification regarding accuracy procedures.
- Sec. 204. Clarification regarding treatment of information and evidence acquired under the Foreign Intelligence Surveillance Act of 1978.
- Sec. 205. Sunset on grandfather clause of Section 215 of the USA PATRIOT Act.
- Sec. 206. Written record of Department of Justice interactions with Foreign Intelligence Surveillance court; protection against judge shopping by DOJ.
- Sec. 207. Appointment of amici curiae and access to information.
- Sec. 208. Declassification of significant decisions, orders, and opinions.
- Sec. 209. Clarification of Foreign Intelligence Surveillance Court jurisdiction over records of the court and other ancillary matters.
- 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.
- Sec. 211. Accountability procedures for violations by Federal employees.

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

3

- Sec. 301. Definitions.
- Sec. 302. Prohibition on warrantless queries for the communications of United States persons and persons located in the United States.
- Sec. 303. Prohibition on reverse targeting of United States persons and persons located in the United States.
- Sec. 304. Prohibition on intelligence acquisition of United States person data.
- Sec. 305. Prohibition on the warrantless acquisition of domestic communications.
- Sec. 306. Data retention limits.
- Sec. 307. Reports on violations of law or Executive order.

TITLE IV—INDEPENDENT OVERSIGHT

- Sec. 401. Inspector General oversight of orders under the Foreign Intelligence Surveillance Act of 1978.
- Sec. 402. Department of Justice inspector general review of high intensity drug trafficking area surveillance programs.
- Sec. 403. Intelligence community parity and communications with Privacy and Civil Liberties Oversight Board.
- Sec. 404. Congressional oversight of grants of immunity by the Attorney General for warrantless surveillance assistance.

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.
- Sec. 502. Consistent protections for phone and app-based call and texting records.
- Sec. 503. Email Privacy Act.
- Sec. 504. Consistent protections for demands for data held by interactive computing services.
- Sec. 505. Consistent protections for real-time and historical metadata.
- Sec. 506. Subpoenas for certain subscriber information.
- Sec. 507. Minimization standards for voluntary disclosure of customer communications or records.
- Sec. 508. Prohibition on law enforcement purchase of personal data from data brokers.
- Sec. 509. Consistent privacy protections for data held by data brokers.
- Sec. 510. Protection of data entrusted to intermediary or ancillary service providers.
- Sec. 511. Modernizing criminal surveillance reports.

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

- Sec. 601. Cell site simulators.

TITLE VII—PROTECTION OF CAR DATA FROM WARRANTLESS
SEARCHES

- Sec. 701. Protection of car data from warrantless searches.

TITLE VIII—INTELLIGENCE TRANSPARENCY

- Sec. 801. Enhanced annual reports by Director of the Administrative Office of the United States Courts.
- Sec. 802. Enhanced annual reports by Director of National Intelligence.
- Sec. 803. Annual reporting on accuracy and completeness of applications.
- Sec. 804. Allowing more granular aggregate reporting by recipients of foreign intelligence surveillance orders.
- Sec. 805. Report on use of foreign intelligence surveillance authorities regarding protected activities and protected classes.
- Sec. 806. Publication of estimates regarding communications collected under certain provisions of Foreign Intelligence Surveillance Act of 1978.
- Sec. 807. Enhanced reporting of assessments of compliance with emergency order requirements under certain provisions of the Foreign Intelligence Surveillance Act of 1978.

TITLE IX—SEVERABILITY AND LIMITED DELAYS IN
IMPLEMENTATION

- Sec. 901. Severability.
- Sec. 902. Limited delays in implementation.

1 SEC. 2. DEFINITIONS.

2 (a) AMENDMENTS TO FOREIGN INTELLIGENCE SUR-
3 VEILLANCE ACT OF 1978.—

4 (1) IN GENERAL.—Section 101 of the Foreign
5 Intelligence Surveillance Act of 1978 (50 U.S.C.
6 1801) is amended by adding at the end the fol-
7 lowing:

8 “(q) The term ‘Foreign Intelligence Surveillance
9 Court’ means the court established under section 103(a).

10 “(r) The terms ‘Foreign Intelligence Surveillance
11 Court of Review’ and ‘Court of Review’ mean the court
12 established under section 103(b).

13 “(s) The term ‘appropriate committees of Congress’
14 means—

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

4 “(2) the Committee on the Judiciary of the
5 Senate; and

6 “(3) the Committee on the Judiciary of the
7 House of Representatives.”.

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

10 (A) in section 102 (50 U.S.C. 1802), by
11 striking “the court established under section
12 103(a)” and inserting “the Foreign Intelligence
13 Surveillance Court”;

14 (B) in section 103 (50 U.S.C. 1803)—

15 (i) in subsection (a)—

16 (I) in paragraph (2)(A), by strik-
17 ing “The court established under this
18 subsection” and inserting “The For-
19 eign Intelligence Surveillance Court”;
20 and

21 (II) by striking “the court estab-
22 lished under this subsection” each
23 place it appears and inserting “the
24 Foreign Intelligence Surveillance
25 Court”;

1 (ii) in subsection (g)—

2 (I) by striking “the court estab-
3 lished pursuant to subsection (a)” and
4 inserting “the Foreign Intelligence
5 Surveillance Court”;

6 (II) by striking “the court of re-
7 view established pursuant to sub-
8 section (b)” and inserting “the For-
9 eign Intelligence Surveillance Court of
10 Review”; and

11 (III) by striking “The courts es-
12 tablished pursuant to subsections (a)
13 and (b)” and inserting “The Foreign
14 Intelligence Surveillance Court and
15 the Foreign Intelligence Surveillance
16 Court of Review”;

17 (iii) in subsection (h), by striking “a
18 court established under this section” and
19 inserting “the Foreign Intelligence Surveil-
20 lance Court or the Foreign Intelligence
21 Surveillance Court of Review”;

22 (iv) in subsection (i)—

23 (I) in paragraph (1), by striking
24 “the courts established under sub-
25 sections (a) and (b)” and inserting

1 “the Foreign Intelligence Surveillance
2 Court and the Foreign Intelligence
3 Surveillance Court of Review”;

4 (II) in paragraph (3)(B), by
5 striking “the courts” and inserting
6 “the Foreign Intelligence Surveillance
7 Court and the Foreign Intelligence
8 Surveillance Court of Review”;

9 (III) in paragraph (5), by strik-
10 ing “the court” and inserting “the
11 Foreign Intelligence Surveillance
12 Court or the Foreign Intelligence Sur-
13 veillance Court of Review, as the case
14 may be,”;

15 (IV) in paragraph (6), by strik-
16 ing “the court” each place it appears
17 and inserting “the Foreign Intel-
18 ligence Surveillance Court or the For-
19 eign Intelligence Surveillance Court of
20 Review”;

21 (V) by striking “a court estab-
22 lished under subsection (a) or (b)”
23 each place it appears and inserting
24 “the Foreign Intelligence Surveillance

1 Court or the Foreign Intelligence Sur-
2veillance Court of Review”; and

3 (VI) by striking “A court estab-
4lished under subsection (a) or (b)”
5each place it appears and inserting
6“‘The Foreign Intelligence Surveillance
7Court or the Foreign Intelligence Sur-
8veillance Court of Review”;
9(v) in subsection (j)—

10 (I) by striking “a court estab-
11lished under subsection (a)” and in-
12serting “the Foreign Intelligence Sur-
13veillance Court”; and

14 (II) by striking “the court deter-
15mines” and inserting “the Foreign In-
16telligence Surveillance Court deter-
17mines”;

18 (vi) by striking “the court established
19under subsection (a)” each place it appears
20and inserting “the Foreign Intelligence
21Surveillance Court”; and

22 (vii) by striking “the court established
23under subsection (b)” each place it appears
24and inserting “the Foreign Intelligence
25Surveillance Court of Review”;

1 (C) in section 105(c) (50 U.S.C.
2 1805(c))—

3 (i) in paragraph (2)(B), by striking
4 “the Court” and inserting “the Foreign
5 Intelligence Surveillance Court”; and

6 (ii) in paragraph (3), by striking “the
7 court” each place it appears and inserting
8 “the Foreign Intelligence Surveillance
9 Court”;

10 (D) in section 401(1) (50 U.S.C. 1841(1)),
11 by striking “, and ‘State’” and inserting
12 “‘State’, ‘Foreign Intelligence Surveillance
13 Court’, and ‘Foreign Intelligence Surveillance
14 Court of Review’”;

15 (E) in section 402 (50 U.S.C. 1842)—

16 (i) in subsection (b)(1), by striking
17 “the court established by section 103(a) of
18 this Act” and inserting “the Foreign Intel-
19 ligence Surveillance Court”; and

20 (ii) in subsection (h)(2), by striking
21 “the court established under section
22 103(a)” and inserting “the Foreign Intel-
23 ligence Surveillance Court”;

24 (F) in section 501 (50 U.S.C. 1861)—

1 (i) in subsection (b)(1), by striking
2 “the court established by section 103(a)”
3 and inserting “the Foreign Intelligence
4 Surveillance Court”;

5 (ii) in subsection (g)(3), by striking
6 “the court established under section
7 103(a)” and inserting “the Foreign Intel-
8 ligence Surveillance Court”; and

9 (iii) in subsection (k)(1), by striking
10 “, and ‘State’” and inserting “‘State’, and
11 ‘Foreign Intelligence Surveillance Court’”;

12 (G) in section 502(c)(1)(E), by striking
13 “the court established under section 103” and
14 inserting “the Foreign Intelligence Surveillance
15 Court (as defined by section 101)”;

16 (H) in section 801 (50 U.S.C. 1885)—

17 (i) in paragraph (8)(B)(i), by striking
18 “the court established under section
19 103(a)” and inserting “the Foreign Intel-
20 ligence Surveillance Court”; and

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

23 “(10) FOREIGN INTELLIGENCE SURVEILLANCE
24 COURT.—The term ‘Foreign Intelligence Surveillance

1 Court’ means the court established under section
2 103(a).”; and

3 (I) in section 802(a)(1) (50 U.S.C.
4 1885a(a)(1)), by striking “the court established
5 under section 103(a)” and inserting “the For-
6 eign Intelligence Surveillance Court”.

7 (b) TERMS USED IN THIS ACT.—In this Act, the
8 terms “appropriate committees of Congress”, “Foreign
9 Intelligence Surveillance Court”, and “Foreign Intel-
10 ligence Surveillance Court of Review” have the meanings
11 given such terms in section 101 of the Foreign Intelligence
12 Surveillance Act of 1978 (50 U.S.C. 1801), as amended
13 by subsection (a).

1 **TITLE I—PROTECTIONS FOR**
2 **UNITED STATES PERSONS**
3 **WHOSE COMMUNICATIONS**
4 **ARE COLLECTED UNDER SEC-**
5 **TION 702 OF THE FOREIGN IN-**
6 **TELLIGENCE SURVEILLANCE**
7 **ACT OF 1978**

8 **SEC. 101. PROHIBITION ON WARRANTLESS QUERIES FOR**
9 **THE COMMUNICATIONS OF UNITED STATES**
10 **PERSONS AND PERSONS LOCATED IN THE**
11 **UNITED STATES.**

12 Section 702(f) of the Foreign Intelligence Surveil-
13 lance Act of 1978 (50 U.S.C. 1881a(f)) is amended—

14 (1) in paragraph (1)—

15 (A) in subparagraph (A), by inserting
16 “and the limitations and requirements in para-
17 graph (2)” after “Constitution of the United
18 States”; and

19 (B) in subparagraph (B), by striking
20 “United States person query term used for a
21 query” and inserting “term for a United States
22 person or person reasonably believed to be in
23 the United States used for a query as required
24 by paragraph (3)”;

1 (2) by redesignating paragraph (3) as para-
2 graph (5); and

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

5 “(2) PROHIBITION ON WARRANTLESS QUERIES
6 FOR THE COMMUNICATIONS AND OTHER INFORMA-
7 TION OF UNITED STATES PERSONS AND PERSONS
8 LOCATED IN THE UNITED STATES.—

9 “(A) IN GENERAL.—Except as provided in
10 subparagraphs (B) and (C), no officer or em-
11 ployee of the United States may conduct a
12 query of information acquired under this sec-
13 tion in an effort to find communications or in-
14 formation the compelled production of which
15 would require a probable cause warrant if
16 sought for law enforcement purposes in the
17 United States, of or about 1 or more United
18 States persons or persons reasonably believed to
19 be located in the United States at the time of
20 the query or the time of the communication or
21 creation of the information.

22 “(B) EXCEPTIONS FOR CONCURRENT AU-
23 THORIZATION, CONSENT, EMERGENCY SITUA-
24 TIONS, AND CERTAIN DEFENSIVE CYBERSECU-
25 RITY QUERIES.—

1 “(i) IN GENERAL.—Subparagraph (A)
2 shall not apply to a query related to a
3 United States person or person reasonably
4 believed to be located in the United States
5 at the time of the query or the time of the
6 communication or creation of the informa-
7 tion if—

8 “(I) such person is the subject of
9 an order or emergency authorization
10 authorizing electronic surveillance or
11 physical search under section 105 or
12 304 of this Act, or a warrant issued
13 pursuant to the Federal Rules of
14 Criminal Procedure by a court of
15 competent jurisdiction covering the
16 period of the query;

17 “(II)(aa) the officer or employee
18 carrying out the query has a reason-
19 able belief that—

20 “(AA) an emergency exists
21 involving an imminent threat of
22 death or serious bodily harm; and

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

ization pursuant to subparagraph
(I) can, with due diligence, be ob-
tained; and

4 “(bb) a description of the query is provided
5 to the Foreign Intelligence Surveillance Court
6 and the appropriate committees of Congress in
7 a timely manner;

8 “(III) such person or, if such
9 person is incapable of providing con-
10 sent, a third party legally authorized
11 to consent on behalf of such person,
12 has provided consent to the query on
13 a case-by-case basis; or

14 “(IV)(aa) the query uses a
15 known cybersecurity threat signature
16 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 communica-
tions retrieved as a result of the query are
accessed or reviewed; and

1 “(dd) all such queries are reported to the
2 Foreign Intelligence Surveillance Court.

3 “(ii) LIMITATIONS.—

4 “(I) USE IN SUBSEQUENT PRO-
5 CEEDINGS AND INVESTIGATIONS.—No
6 information retrieved pursuant to a
7 query authorized by clause (i)(II) or
8 information derived from such query
9 may be used, received in evidence, or
10 otherwise disseminated in any inves-
11 tigation, trial, hearing, or other pro-
12 ceeding in or before any court, grand
13 jury, department, office, agency, regu-
14 latory body, legislative committee, or
15 other authority of the United States,
16 a State, or political subdivision there-
17 of, except in proceedings or investiga-
18 tions that arise from the threat that
19 prompted the query.

20 “(II) ASSESSMENT OF COMPLI-
21 ANCE.—The Attorney General shall
22 not less frequently than annually as-
23 sess compliance with the requirements
24 under subclause (I).

1 “(C) MATTERS RELATING TO EMERGENCY
2 QUERIES.—

3 “(i) TREATMENT OF DENIALS.—In
4 the event that a query for communications
5 or information, the compelled production of
6 which would require a probable cause war-
7 rant if sought for law enforcement pur-
8 poses in the United States, of or about 1
9 more United States persons or persons
10 reasonably believed to be located in the
11 United States at the time of the query or
12 the time of the communication or creation
13 of the information is conducted pursuant
14 to an emergency authorization described in
15 subparagraph (B)(i)(I) and the application
16 for such emergency authorization is denied,
17 or in any other case in which the query has
18 been conducted and no order is issued ap-
19 proving the query—

20 “(I) no information obtained or
21 evidence derived from such query may
22 be used, received in evidence, or other-
23 wise disseminated in any investiga-
24 tion, trial, hearing, or other pro-
25 ceeding in or before any court, grand

1 jury, department, office, agency, regu-
2 latory body, legislative committee, or
3 other authority of the United States,
4 a State, or political subdivision there-
5 of; and

6 “(II) no information concerning
7 any United States person or person
8 reasonably believed to be located in
9 the United States at the time of the
10 query or the time of the communica-
11 tion or the creation of the information
12 acquired from such query may subse-
13 quently be used or disclosed in any
14 other manner without the consent of
15 such person, except with the approval
16 of the Attorney General if the infor-
17 mation indicates a threat of death or
18 serious bodily harm to any person.

19 “(ii) ASSESSMENT OF COMPLIANCE.—
20 The Attorney General shall not less fre-
21 quently than annually assess compliance
22 with the requirements under clause (i).

23 “(D) FOREIGN INTELLIGENCE PURPOSE.—
24 Except as provided in subparagraph (B)(i), no
25 officer or employee of the United States may

1 conduct a query of information acquired under
2 this section in an effort to find information of
3 or about 1 or more United States persons or
4 persons reasonably believed to be located in the
5 United States at the time of the query or the
6 time of the communication or creation of the in-
7 formation unless the query is reasonably likely
8 to retrieve foreign intelligence information.

9 “(3) DOCUMENTATION.—No officer or employee
10 of the United States may conduct a query of infor-
11 mation acquired under this section in an effort to
12 find information of or about 1 or more United
13 States persons or persons reasonably believed to be
14 located in the United States at the time of query or
15 the time of the communication or the creation of the
16 information, unless first an electronic record is cre-
17 ated, and a system, mechanism, or business practice
18 is in place to maintain such record, that includes the
19 following:

20 “(A) Each term used for the conduct of
21 the query.

22 “(B) The date of the query.

23 “(C) The identifier of the officer or em-
24 ployee.

1 “(D) A statement of facts showing that the
2 use of each query term included under subpara-
3 graph (A) is—

4 “(i) reasonably likely to retrieve for-
5 eign intelligence information; or

6 “(ii) in furtherance of the exceptions
7 described in paragraph (2)(B)(i).

8 “(4) PROHIBITION ON RESULTS OF METADATA
9 QUERY AS A BASIS FOR ACCESS TO COMMUNICA-
10 TIONS AND OTHER PROTECTED INFORMATION.—If a
11 query of information acquired under this section is
12 conducted in an effort to find communications
13 metadata of 1 or more United States persons or per-
14 sons reasonably believed to be located in the United
15 States at the time of the query or communication
16 and the query returns such metadata, the results of
17 the query shall not be used as a basis for reviewing
18 communications or information a query for which is
19 otherwise prohibited under this section.

20 “(5) FEDERATED DATASETS.—The prohibitions
21 and requirements in this section shall apply to que-
22 ries of federated and mixed datasets that include in-
23 formation acquired under this section, unless a
24 mechanism exists to limit the query to information
25 not acquired under this section.”.

1 **SEC. 102. LIMITATION ON USE OF INFORMATION OBTAINED**
2 **UNDER SECTION 702 OF THE FOREIGN INTEL-**
3 **LIGENCE SURVEILLANCE ACT OF 1978 RELAT-**
4 **ING TO UNITED STATES PERSONS AND PER-**
5 **SONS LOCATED IN THE UNITED STATES IN**
6 **CRIMINAL, CIVIL, AND ADMINISTRATIVE AC-**
7 **TIONS.**

8 Paragraph (2) of section 706(a) of the Foreign Intel-
9 ligence Surveillance Act of 1978 (50 U.S.C. 1881e(a)) is
10 amended to read as follows:

11 “(2) LIMITATION ON USE IN CRIMINAL, CIVIL,
12 AND ADMINISTRATIVE PROCEEDINGS AND INVES-
13 TIGATIONS.—No information acquired pursuant to
14 section 702(f) of or about a United States person or
15 person reasonably believed to be located in the
16 United States at the time of acquisition or commu-
17 nication may be introduced as evidence against such
18 person in any criminal, civil, or administrative pro-
19 ceeding or used as part of any criminal, civil, or ad-
20 ministrative investigation, except—

21 “(A) with the prior approval of the Attor-
22 ney General; and

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

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

4 “(ii) counterintelligence (as defined in
5 section 3 of the National Security Act of
6 1947 (50 U.S.C. 3003));

7 “(iii) proliferation or use of a weapon
8 of mass destruction (as defined in section
9 2332a(c) of title 18, United States Code);

10 “(iv) a cybersecurity breach or attack
11 from a foreign country;

12 “(v) incapacitation or destruction of
13 critical infrastructure (as defined in section
14 1016(e) of the Uniting and Strengthening
15 America by Providing Appropriate Tools
16 Required to Intercept and Obstruct Ter-
17 rorism (USA PATRIOT ACT) Act of 2001
18 (42 U.S.C. 5195c(e));

19 “(vi) an attack against the armed
20 forces of the United States or an ally of
21 the United States or to other personnel of
22 the United States Government or a govern-
23 ment of an ally of the United States; or

24 “(vii) international narcotics traf-
25 ficking.”.

1 **SEC. 103. REPEAL OF AUTHORITY FOR THE RESUMPTION**
2 **OF ABOUTS COLLECTION.**

3 (a) IN GENERAL.—Section 702(b)(5) of the Foreign
4 Intelligence Surveillance Act of 1978 (50 U.S.C.
5 1881a(b)(5)) is amended by striking “, except as provided
6 under section 103(b) of the FISA Amendments Reauthor-
7 ization Act of 2017”.

8 (b) CONFORMING AMENDMENTS.—

9 (1) FOREIGN INTELLIGENCE SURVEILLANCE
10 ACT OF 1978.—Section 702(m) of the Foreign Intel-
11 ligence Surveillance Act of 1978 (50 U.S.C.
12 1881a(m)) is amended—

13 (A) in the subsection heading, by striking
14 “REVIEWS, AND REPORTING” and inserting
15 “AND REVIEWS”; and

16 (B) by striking paragraph (4).

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

21 (A) by striking subsection (b); and

22 (B) by striking the following:

23 “(a) IN GENERAL.—”.

1 **SEC. 104. PROHIBITION ON REVERSE TARGETING OF**
2 **UNITED STATES PERSONS AND PERSONS LO-**
3 **CATED IN THE UNITED STATES.**

4 Section 702 of the Foreign Intelligence Surveillance
5 Act of 1978 (50 U.S.C. 1881a), as amended by section
6 101, is further amended—

7 (1) in subsection (b)(2)—

8 (A) by striking “may not intentionally”
9 and inserting the following “may not—

10 “(A) intentionally”;

11 (B) in subparagraph (A), as designated by
12 subparagraph (A) of this paragraph, by striking
13 “if the purpose of such acquisition is to target
14 a particular, known person reasonably believed
15 to be in the United States;” and inserting the
16 following: “if a significant purpose of such ac-
17 quisition is to acquire the information of 1 or
18 more United States persons or persons reason-
19 ably believed to be located in the United States
20 at the time of acquisition or communication,
21 unless—

22 “(i)(I) there is a reasonable belief that
23 an emergency exists involving an imminent
24 threat of death or serious bodily harm to
25 such United States person or person rea-
26 sonably believed to be located in the

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

3 “(II) the information is sought for the
4 purpose of assisting that person; and

5 “(III) a description of the targeting is
6 provided to the Foreign Intelligence Sur-
7 veillance Court and the appropriate com-
8 mittees of Congress in a timely manner; or

9 “(ii) the United States person or per-
10 sons reasonably believed to be located in
11 the United States at the time of acquisi-
12 tion or communication has provided con-
13 sent to the targeting, or if such person is
14 incapable of providing consent, a third
15 party legally authorized to consent on be-
16 half of such person has provided consent;
17 and

18 “(B) in the case of information acquired
19 pursuant to subparagraph (A)(i) or evidence de-
20 rived from such targeting, be used, received in
21 evidence, or otherwise disseminated in any in-
22 vestigation, trial, hearing, or other proceeding
23 in or before any court, grand jury, department,
24 office, agency, regulatory body, legislative com-
25 mittee, or other authority of the United States,

1 a State, or political subdivision thereof, except
2 in proceedings or investigations that arise from
3 the threat that prompted the targeting;”;

4 (2) in subsection (d)(1), by amending subpara-
5 graph (A) to read as follows:

6 “(A) ensure that—

7 “(i) any acquisition authorized under
8 subsection (a) is limited to targeting per-
9 sons reasonably believed to be non-United
10 States persons located outside the United
11 States; and

12 “(ii) except as provided in subsection
13 (b)(2), a significant purpose of an acquisi-
14 tion is not to acquire the information of 1
15 or more United States persons or persons
16 reasonably believed to be in the United
17 States at the time of acquisition or com-
18 munication; and”;

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

21 “(I) ensure that—

22 “(aa) an acquisition author-
23 ized under subsection (a) is lim-
24 ited to targeting persons reason-
25 ably believed to be non-United

1 States persons located outside
2 the United States; and

3 “(bb) except as provided in
4 subsection (b)(2), a significant
5 purpose of an acquisition is not
6 to acquire the information of 1 or
7 more United States persons or
8 persons reasonably believed to be
9 in the United States at the time
10 of acquisition or communication;
11 and”; and

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

14 “(i) ensure that—

15 “(I) an acquisition authorized
16 under subsection (a) is limited to tar-
17 geting persons reasonably believed to
18 be non-United States persons located
19 outside the United States; and

20 “(II) except as provided in sub-
21 section (b)(2), a significant purpose of
22 an acquisition is not to acquire the in-
23 formation of 1 or more United States
24 persons or persons reasonably believed
25 to be in the United States at the time

1 of acquisition or communication;
2 and”.

3 **SEC. 105. DATA RETENTION LIMITS FOR INFORMATION**
4 **COLLECTED UNDER SECTION 702 OF THE**
5 **FOREIGN INTELLIGENCE SURVEILLANCE ACT**
6 **OF 1978.**

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

10 **“SEC. 709. DATA RETENTION LIMITS.**

11 “(a) POLICY.—The Attorney General shall develop,
12 and the heads of the elements of the intelligence commu-
13 nity shall implement, procedures governing the retention
14 of information collected pursuant to section 702.

15 “(b) COVERED INFORMATION.—For purposes of this
16 section, ‘covered information’ includes—

17 “(1) any information, including an encrypted
18 communication, to, from, or pertaining to a United
19 States person or person reasonably believed to be lo-
20 cated in the United States at the time of acquisition,
21 communication, or creation of the information that
22 has been evaluated and is not specifically known to
23 contain foreign intelligence information; and

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

1 mation does not contain communications to or from
2 or information pertaining to a United States person
3 or person reasonably believed to be located in the
4 United States at the time of acquisition, communica-
5 tion or creation of the information.

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

12 “(1) the information is the subject of a preser-
13 vation obligation in pending administrative, civil, or
14 criminal litigation, in which case the information
15 shall be segregated, retained, and used solely for
16 that purpose and shall be destroyed as soon as it is
17 no longer required to be preserved for such litiga-
18 tion; or

19 “(2) the information is being used in a pro-
20 ceeding or investigation in which the information is
21 directly related to and necessary to address a spe-
22 cific threat identified in section 706(a)(2)(B).”.

23 (b) CLERICAL AMENDMENT.—The table of contents
24 for such Act is amended by inserting after the item relat-
25 ing to section 708 the following:

“Sec. 709. Data retention limits.”.

1 **SEC. 106. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
2 **SUPERVISION OF DEMANDS FOR TECHNICAL**
3 **ASSISTANCE FROM ELECTRONIC COMMU-**
4 **NICATION SERVICE PROVIDERS UNDER SEC-**
5 **TION 702 OF THE FOREIGN INTELLIGENCE**
6 **SURVEILLANCE ACT OF 1978.**

7 Section 702(i)(1) of the Foreign Intelligence Surveil-
8 lance Act of 1978 (50 U.S.C. 1881a(i)(1)) is amended—

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

12 (2) in the matter before clause (i), as redesign-
13 nated by paragraph (1), by striking “With respect
14 to” and inserting the following:

15 “(A) IN GENERAL.—Subject to subpara-
16 graph (B), in carrying out”; and

17 (3) by adding at the end the following:

18 “(B) LIMITATIONS.—The Attorney Gen-
19 eral or the Director of National Intelligence
20 may not direct technical assistance from an
21 electronic communication service provider under
22 subparagraph (A) without demonstrating that
23 the assistance sought—

24 “(i) is necessary;

25 “(ii) is narrowly tailored to the sur-
26 veillance at issue; and

1 “(iii) would not pose an undue burden
2 on the electronic communication service
3 provider or its customers who are not in-
4 tended targets of the surveillance.

5 “(C) COMPLIANCE.—An electronic commu-
6 nication service provider is not obligated to
7 comply with a directive to provide technical as-
8 sistance under this paragraph unless—

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

12 “(ii) the Court issues an order, which
13 has been delivered to the provider, explic-
14 itly describing the assistance to be fur-
15 nished by the provider that has been ap-
16 proved by the Court.”.

17 **SEC. 107. PROHIBITION ON WARRANTLESS ACQUISITION OF**
18 **DOMESTIC COMMUNICATIONS PURSUANT TO**
19 **SECTION 702 OF THE FOREIGN INTEL-**
20 **LIGENCE SURVEILLANCE ACT OF 1978.**

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

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

1 ably believed at the time of acquisition or commu-
2 nication”;

3 (2) in subsection (d)(1)(B), by striking “known
4 at the time of the acquisition” and inserting “rea-
5 sonably believed at the time of the acquisition or
6 communication”;

7 (3) in subsection (h)(2)(A)(i)(II), by striking
8 “known at the time of the acquisition” and inserting
9 “reasonably believed at the time of the acquisition or
10 communication”; and

11 (4) in subsection (j)(2)(B)(ii), by striking
12 “known at the time of the acquisition” and inserting
13 “reasonably believed at the time of the acquisition or
14 communication”.

15 **SEC. 108. REQUIREMENT OF A FOREIGN INTELLIGENCE**
16 **PURPOSE.**

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

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

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

7 (1) in paragraph (1) (50 U.S.C. 1881–1881g
8 note), by striking “December 31, 2023” and insert-
9 ing “September 30, 2027”; and

10 (2) in paragraph (2) (18 U.S.C. 2511 note), in
11 the matter preceding subparagraph (A), by striking
12 “December 31, 2023” and inserting “September 30,
13 2027”.

14 (b) CONFORMING AMENDMENT.—The heading of sec-
15 tion 404(b)(1) of the FISA Amendments Act of 2008
16 (Public Law 110–261; 50 U.S.C. 1801 note) is amended
17 by striking “DECEMBER 31, 2023” and inserting “SEP-
18 TEMBER 30, 2027”.

1 **TITLE II—ADDITIONAL RE-**
2 **FORMS RELATING TO ACTIVI-**
3 **TIES UNDER THE FOREIGN**
4 **INTELLIGENCE SURVEIL-**
5 **LANCE ACT OF 1978**

6 **SEC. 201. COURT SUPERVISION OF COLLECTION TAR-**
7 **GETING UNITED STATES PERSONS AND PER-**
8 **SONS LOCATED INSIDE THE UNITED STATES.**

9 (a) IN GENERAL.—Title VII of the Foreign Intel-
10 ligence Surveillance Act of 1978 (50 U.S.C. 50 U.S.C.
11 1881 et seq.) is amended—

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

14 (2) by inserting after section 702 (50 U.S.C.
15 1881a) the following:

16 **“SEC. 703. ACQUISITIONS TARGETING UNITED STATES PER-**
17 **SONS AND PERSONS LOCATED INSIDE THE**
18 **UNITED STATES.**

19 “(a) WARRANT REQUIREMENT.—No officer or em-
20 ployee of the United States may intentionally target any
21 United States person, regardless of location, or person
22 reasonably believed to be located in the United States for
23 the purpose of acquiring foreign intelligence information
24 under circumstances in which the person has a reasonable
25 expectation of privacy or a warrant would be required if

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

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

10 “(2) a warrant issued pursuant to the Federal
11 Rules of Criminal Procedure by a court of competent
12 jurisdiction covering the period of the acquisition
13 and the acquisition is subject to the use, dissemina-
14 tion, querying, retention, and other minimization
15 limitations required by such warrant.

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

1 “(1) an order or emergency authorization under
2 title IV of this Act covering the period of the acqui-
3 sition and the acquisition is subject to the use, dis-
4 semination, querying, retention, and other minimiza-
5 tion limitations required by such authorization; or

6 “(2) an order has been issued pursuant to sec-
7 tion 3123 of title 18, United States Code, by a court
8 of competent jurisdiction covering the period of the
9 acquisition.

10 “(c) MATTERS RELATING TO EMERGENCY ACQUI-
11 TION.—In the event that an emergency acquisition is con-
12 ducted pursuant to subsection (a)(1) or (b)(1) and the ap-
13 plication for such emergency authorization is denied, or
14 in any other case in which the acquisition has been con-
15 ducted and no order is issued approving the acquisition—

16 “(1) no information obtained or evidence de-
17 rived from such acquisition may be used, received in
18 evidence, or otherwise disseminated in any investiga-
19 tion, trial, hearing, or other proceeding in or before
20 any court, grand jury, department, office, agency,
21 regulatory body, legislative committee, or other au-
22 thority of the United States, a State, or political
23 subdivision thereof; and

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

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

7 “(d) RULE OF CONSTRUCTION.—Subsections (a) and
8 (b) shall apply regardless of the location of the acquisi-
9 tion.”.

10 (b) CONFORMING AMENDMENTS.—The Foreign In-
11 telligence Surveillance Act of 1978 (50 U.S.C. 1801 et
12 seq.) is further amended—

13 (1) in section 601(a)(1) (50 U.S.C.
14 1871(a)(1)—

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

17 (B) in subparagraph (B), by striking the
18 semicolon and inserting “; or”;

19 (2) in section 603(b)(1) (50 U.S.C.
20 1873(b)(1)), in the matter before subparagraph (A),
21 by striking “and sections 703 and 704”; and

22 (3) in section 706 (50 U.S.C. 1881e), by strik-
23 ing subsection (b).

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

1 (1) by striking the items relating to sections
2 703, 704, and 705; and

3 (2) by inserting after the item relating to sec-
4 tion 702 the following:

“Sec. 703. Acquisitions targeting United States persons and persons located in-
side the United States.”.

5 **SEC. 202. REQUIRED DISCLOSURE OF RELEVANT INFORMA-**
6 **TION IN FOREIGN INTELLIGENCE SURVEIL-**
7 **LANCE ACT OF 1978 APPLICATIONS.**

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

11 **“TITLE IX—REQUIRED DISCLO-**
12 **SURE OF RELEVANT INFOR-**
13 **MATION**

14 **“SEC. 901. DISCLOSURE OF RELEVANT INFORMATION.**

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

18 “(1) all information in the possession of the
19 Government that is material to determining whether
20 the application satisfies the applicable requirements
21 under this Act, including any exculpatory informa-
22 tion; and

23 “(2) all information in the possession of the
24 Government that might reasonably—

1 “(A) call into question the accuracy of the
2 application or the reasonableness of any assess-
3 ment in the application conducted by the de-
4 partment or agency on whose behalf the appli-
5 cation is made; or

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

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

“TITLE IX—DISCLOSURE OF RELEVANT INFORMATION

“Sec. 901. Disclosure of relevant information.”.

13 **SEC. 203. CERTIFICATION REGARDING ACCURACY PROCE-**
14 **DURES.**

15 (a) CERTIFICATION REGARDING ACCURACY PROCE-
16 DURES.—Title IX of the Foreign Intelligence Surveillance
17 Act of 1978, as added by section 202, is amended by add-
18 ing at the end the following:

19 **“SEC. 902. CERTIFICATION REGARDING ACCURACY PROCE-**
20 **DURES.**

21 “(a) DEFINITION OF ACCURACY PROCEDURES.—In
22 this section, the term ‘accuracy procedures’ means specific
23 procedures, adopted by the Attorney General, to ensure
24 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 en-
sure, at a minimum, that—

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

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

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

“(4) the applicant coordinates with the appro-
priate elements of the intelligence community (as de-
fined in section 3 of the National Security Act of
1947 (50 U.S.C. 3003)), concerning any prior or ex-
isting relationship with the target of any surveil-
lance, 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-

1 viewed for accuracy and completeness supporting
2 documentation for each factual assertion in the ap-
3 plication; and

4 “(6) the applicant Federal agency establish
5 compliance and auditing mechanisms on an annual
6 basis to assess the efficacy of the accuracy proce-
7 dures that have been adopted and report such find-
8 ings to the Attorney General.

9 “(b) STATEMENT AND CERTIFICATION OF ACCURACY
10 PROCEDURES.—Any Federal officer making an applica-
11 tion for a court order under this Act shall include with
12 the application—

13 “(1) a description of the accuracy procedures
14 employed by the officer or the officer’s designee; and

15 “(2) a certification that the officer or the offi-
16 cer’s designee has collected and reviewed for accu-
17 racy and completeness—

18 “(A) supporting documentation for each
19 factual assertion contained in the application;

20 “(B) all information that might reasonably
21 call into question the accuracy of the informa-
22 tion or the reasonableness of any assessment in
23 the application, or otherwise raises doubts
24 about the requested findings; and

1 “(C) all material information that might
2 reasonably call into question the reliability and
3 reporting of any information from any confiden-
4 tial human source that is used in the applica-
5 tion.

6 “(3) NECESSARY FINDING FOR COURT OR-
7 DERS.—A judge may not enter an order under this
8 Act unless the judge finds, in addition to any other
9 findings required under this Act, that the accuracy
10 procedures described in the application for the order,
11 as required under subsection (b)(1), are actually ac-
12 curacy procedures as defined in this section.”.

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

 “Sec. 902. Certification regarding accuracy procedures.”.

17 **SEC. 204. CLARIFICATION REGARDING TREATMENT OF IN-**
18 **FORMATION AND EVIDENCE ACQUIRED**
19 **UNDER THE FOREIGN INTELLIGENCE SUR-**
20 **VEILLANCE ACT OF 1978.**

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

24 “(q) For the purposes of notification provisions of
25 this Act, information or evidence is ‘derived’ from an elec-

1 tronic surveillance, physical search, use of a pen register
2 or trap and trace device, production of tangible things,
3 or acquisition under this Act when the Government would
4 not have originally possessed the information or evidence
5 but for that electronic surveillance, physical search, use
6 of a pen register or trap and trace device, production of
7 tangible things, or acquisition, and regardless of any claim
8 that the information or evidence is attenuated from the
9 surveillance or search, would inevitably have been discov-
10 ered, or was subsequently reobtained through other
11 means.”.

12 (b) POLICIES AND GUIDANCE.—

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

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

20 (B) Guidance for all members of the intel-
21 ligence community (as defined in section 3 of
22 the National Security Act of 1947 (50 U.S.C.
23 3003)) and all Federal agencies with law en-
24 forcement responsibilities concerning the appli-
25 cation of such subsection (q).

1 (2) MODIFICATIONS.—Whenever the Attorney
2 General and the Director modify a policy or guid-
3 ance published under paragraph (1), the Attorney
4 General and the Director shall publish such modi-
5 fications.

6 **SEC. 205. SUNSET ON GRANDFATHER CLAUSE OF SECTION**
7 **215 OF THE USA PATRIOT ACT.**

8 Section 102(b)(2) of the USA PATRIOT Improve-
9 ment and Reauthorization Act of 2005 (Public Law 109–
10 177; 50 U.S.C. 1805 note) is amended by inserting “, ex-
11 cept that title V of the Foreign Intelligence Surveillance
12 Act of 1978, as in effect on March 14, 2020, shall con-
13 tinue in effect until the date that is 180 days after the
14 date of the enactment of the Government Surveillance Re-
15 form Act of 2023” after “continue in effect”.

16 **SEC. 206. WRITTEN RECORD OF DEPARTMENT OF JUSTICE**
17 **INTERACTIONS WITH FOREIGN INTEL-**
18 **LIGENCE SURVEILLANCE COURT; PROTEC-**
19 **TION AGAINST JUDGE SHOPPING BY DOJ.**

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

23 (1) by inserting “, and shall be transcribed” be-
24 fore the first period; and

1 (2) by inserting “, transcriptions,” after “appli-
2 cations made”.

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

6 “(1) WRITTEN RECORD OF INTERACTIONS.—

7 “(1) WRITTEN COMMUNICATIONS.—The Attor-
8 ney General shall maintain all written communica-
9 tions with the court established under subsection
10 (a), including the identity of the employees of the
11 court to or from whom the communications were
12 made, regarding an application or order made under
13 this title in a file associated with the application or
14 order.

15 “(2) ORAL COMMUNICATIONS.—The Attorney
16 General shall—

17 “(A) document a summary of any oral
18 communications with the court established
19 under subsection (a), including the identity of
20 the employees of the court to or from whom the
21 communications were made, relating to an ap-
22 plication or order described in paragraph (1);
23 and

24 “(B) keep such documentation in a file as-
25 sociated with the application or order.”.

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

7 **SEC. 207. APPOINTMENT OF AMICI CURIAE AND ACCESS TO**
8 **INFORMATION.**

9 (a) EXPANSION OF APPOINTMENT AUTHORITY.—

10 (1) IN GENERAL.—Section 103(i)(2) of the For-
11 eign Intelligence Surveillance Act of 1978 (50
12 U.S.C. 1803(i)(2)) is amended—

13 (A) by striking subparagraph (A) and in-
14 serting the following:

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

23 “(i) a novel or significant interpreta-
24 tion of the law;

1 “(ii) a significant concern related to
2 constitutional rights;

3 “(iii) a sensitive investigative matter;

4 “(iv) a request for approval of a new
5 program, a new technology, or a new use
6 of existing technology;

7 “(v) a request for reauthorization of
8 programmatic surveillance; or

9 “(vi) any other privacy or civil lib-
10 erties issue for which an appointment of an
11 amicus curiae to assist the court in the
12 consideration of the application would be
13 appropriate; and”;

14 (B) in subparagraph (B), by striking “an
15 individual or organization” each place it ap-
16 pears and inserting “1 or more individuals or
17 organizations”;

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

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

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

1 consideration of any application for an order or
2 review, unless the court issues a written finding
3 that such application neither presents nor in-
4 volves—

5 “(i) a request for approval of a new
6 program, a new technology, or a new use
7 of existing technology;

8 “(ii) a request for approval of a pre-
9 viously authorized program, technology, or
10 use of existing technology for which no
11 prior application for approval of such pro-
12 gram, technology, or use was considered by
13 the court with the assistance of an amicus
14 curiae who possesses technical expertise; or

15 “(iii) a technical issue material to any
16 legal determination for which an appoint-
17 ment of an amicus curiae who possesses
18 technical expertise to assist the court in
19 the consideration of the application would
20 be appropriate;

21 “(C) shall randomly appoint at least 1 in-
22 dividual with legal expertise and at least 1 indi-
23 vidual with technical expertise, from among in-
24 dividuals who have been designated under para-

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

3 (2) DEFINITION OF SENSITIVE INVESTIGATIVE
4 MATTER.—Section 103(i) of such Act (50 U.S.C.
5 1803(i)) is amended by adding at the end the fol-
6 lowing:

7 “(12) DEFINITION OF SENSITIVE INVESTIGA-
8 TIVE MATTER.—In this subsection, the term ‘sen-
9 sitive investigative matter’ means—

10 “(A) an investigative matter involving the
11 activities of—

12 “(i) a domestic public official or polit-
13 ical candidate, or an individual serving on
14 the staff of such an official or candidate;

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

19 “(iii) the domestic news media; or

20 “(B) any other investigative matter involv-
21 ing a domestic entity or a known or suspected
22 United States person that, in the judgment of
23 the applicable court established under sub-
24 section (a) or (b), is as sensitive as an inves-

1 tigative matter described in subparagraph
2 (A).”.

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

5 (A) by inserting “cybersecurity, cryptog-
6 raphy,” after “communications technology,”;
7 and

8 (B) by adding at the end the following:
9 “Of such individuals, at least 1 shall possess
10 legal expertise and at least 1 shall possess tech-
11 nical expertise.”.

12 (4) NOTIFICATION.—Section 103(i) of such Act
13 (50 U.S.C. 1803(i)) is amended by striking para-
14 graph (7) and inserting the following:

15 “(7) NOTIFICATION.—A presiding judge of a
16 court established under subsection (a) or (b) shall,
17 not less frequently than quarterly, provide to the At-
18 torney General and the appropriate committees of
19 Congress—

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

23 “(B) a copy of each written finding issued
24 under paragraph (2).”.

1 (5) SECTION 702 RECERTIFICATION SCHED-
2 ULE.—Section 702(j)(5)(A) of such Act (50 U.S.C.
3 1881a(j)(5)(A)) is amended by striking “at least 30
4 days prior to the expiration of such authorization”
5 and inserting “such number of days, not less than
6 30 days, before the expiration of such authorization
7 as the Court considers necessary to permit review by
8 amici curiae appointed under section 103(i)(2)(C).”.

9 (6) CONFORMING AMENDMENTS.—Section
10 103(i) of such Act (50 U.S.C. 1803(i)) is amend-
11 ed—

12 (A) in paragraph (4), by striking “amicus
13 curiae under paragraph (2)(A)” and inserting
14 “amicus curiae under subparagraph (A), (B),
15 or (C) of paragraph (2)”; and

16 (B) in paragraph (5), by striking “ap-
17 pointed under paragraph (2)(A)” and inserting
18 “appointed under subparagraph (A), (B), or
19 (C) of paragraph (2)”.

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

23 (1) in paragraph (4)—

24 (A) in the paragraph heading, by inserting
25 “; AUTHORITY” after “DUTIES”;

1 (B) by redesignating subparagraphs (A),
2 (B), and (C) as clauses (i), (ii), and (iii), re-
3 spectively, and moving such clauses, as so re-
4 designated, 2 ems to the right;

5 (C) in the matter preceding clause (i), as
6 so designated, by striking “the amicus curiae
7 shall” and inserting the following: “the amicus
8 curiae—

9 “(A) shall”;

10 (D) in subparagraph (A)(i), as so des-
11 ignated, by inserting before the semicolon at the
12 end the following: “, including legal arguments
13 regarding any privacy or civil liberties interest
14 of any United States person that would be sig-
15 nificantly affected by the application or mo-
16 tion”; and

17 (E) by striking the period at the end and
18 inserting the following: “; and

19 “(B) may seek leave to raise any novel or
20 significant privacy or civil liberties issue rel-
21 evant to the application or motion or other
22 issue directly affecting the legality of the pro-
23 posed electronic surveillance with the court, re-
24 gardless of whether the court has requested as-
25 sistance on that issue.”.

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

4 (3) by inserting after paragraph (6) the fol-
5 lowing:

6 “(7) AUTHORITY TO SEEK REVIEW OF DECISIONS.—
7

8 “(A) FOREIGN INTELLIGENCE SURVEILLANCE COURT DECISIONS.—
9

10 “(i) PETITION.—Following issuance of
11 an order under this Act by the Foreign In-
12 telligence Surveillance Court, an amicus
13 curiae appointed under paragraph (2) may
14 petition the Foreign Intelligence Surveil-
15 lance Court to certify for review to Foreign
16 Intelligence Surveillance Court of Review a
17 question of law pursuant to subsection (j).

18 “(ii) DENIALS.—If the Foreign Intel-
19 ligence Surveillance Court denies a petition
20 described in clause (i), the court shall pro-
21 vide for the record a written statement of
22 the reasons for such denial.

23 “(iii) CERTIFICATION.—Upon certifi-
24 cation of any question of law pursuant to
25 this subparagraph, the Foreign Intelligence

1 Surveillance Court of Review shall appoint
2 the amicus curiae to assist the Court of
3 Review in its consideration of the certified
4 question, unless the Court of Review issues
5 a finding that such appointment is not ap-
6 propriate.

7 “(B) FOREIGN INTELLIGENCE SURVEIL-
8 LANCE COURT OF REVIEW DECISIONS.—An
9 amicus curiae appointed under paragraph (2)
10 may petition the Foreign Intelligence Surveil-
11 lance Court of Review to certify for review to
12 the Supreme Court of the United States any
13 question of law pursuant to section 1254(2) of
14 title 28, United States Code.

15 “(C) DECLASSIFICATION OF REFER-
16 RALS.—For purposes of section 602, a petition
17 filed under subparagraph (A) or (B) of this
18 paragraph and all of its content shall be consid-
19 ered a decision, order, or opinion issued by the
20 Foreign Intelligence Surveillance Court or the
21 Foreign Intelligence Surveillance Court of Re-
22 view described in paragraph (2) of section
23 602(a).”.

24 (c) ACCESS TO INFORMATION.—

1 (1) APPLICATION AND MATERIALS.—Section
2 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is
3 amended—

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

6 “(i) shall have access to, to the extent
7 such information is available to the Gov-
8 ernment—

9 “(I) the application, certification,
10 petition, motion, and other informa-
11 tion and supporting materials, includ-
12 ing any information described in sec-
13 tion 901, submitted to the Foreign In-
14 telligence Surveillance Court in con-
15 nection with the matter in which the
16 amicus curiae has been appointed, in-
17 cluding access to any relevant legal
18 precedent (including any such prece-
19 dent that is cited by the Government,
20 including in such an application);

21 “(II) any other information or
22 materials that the court determines is
23 relevant to the duties of the amicus
24 curiae; and

1 “(III) an unredacted copy of
2 each relevant decision made by the
3 Foreign Intelligence Surveillance
4 Court or the Foreign Intelligence Sur-
5 veillance Court of Review in which the
6 court decides a question of law, with-
7 out regard to whether the decision is
8 classified; and

9 “(ii) may make a submission to the
10 court requesting access to any other par-
11 ticular materials or information (or cat-
12 egory of materials or information) that the
13 amicus curiae believes to be relevant to the
14 duties of the amicus curiae.”;

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

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

19 “(D) SUPPORTING DOCUMENTATION RE-
20 GARDING ACCURACY.—The Foreign Intelligence
21 Surveillance Court, upon the motion of an ami-
22 cus curiae appointed under paragraph (2) or
23 upon its own motion, may require the Govern-
24 ment to make available the supporting docu-
25 mentation described in section 902.”.

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

4 (A) in subparagraph (B), by striking
5 “may” and inserting “shall”; and

6 (B) by striking subparagraph (C) and in-
7 serting the following:

8 “(C) CLASSIFIED INFORMATION.—An ami-
9 cus curiae appointed by the court shall have ac-
10 cess to, to the extent such information is avail-
11 able to the Government, unredacted copies of
12 each opinion, order, transcript, pleading, or
13 other document of the Foreign Intelligence Sur-
14 veillance Court and the Foreign Intelligence
15 Surveillance Court of Review, including, if the
16 individual is eligible for access to classified in-
17 formation, any classified documents, informa-
18 tion, and other materials or proceedings.”.

19 (3) CONSULTATION AMONG AMICI CURIAE.—
20 Section 103(i)(6) of such Act (50 U.S.C.
21 1803(i)(6)), as amended by paragraphs (1) and (2),
22 is further amended—

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

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

3 “(B) CONSULTATION.—If the Foreign In-
4 telligence Surveillance Court or the Foreign In-
5 telligence Surveillance Court of Review deter-
6 mines that it is relevant to the duties of an
7 amicus curiae appointed under paragraph (2),
8 the amicus curiae may consult with 1 or more
9 of the other individuals designated to serve as
10 amicus curiae under paragraph (1) regarding
11 any of the information relevant to any assigned
12 proceeding.”.

13 **SEC. 208. DECLASSIFICATION OF SIGNIFICANT DECISIONS,**
14 **ORDERS, AND OPINIONS.**

15 Section 602 of the Foreign Intelligence Surveillance
16 Act of 1978 (50 U.S.C. 1872) is amended by striking sub-
17 section (a) and inserting the following:

18 “(a) DECLASSIFICATION REQUIRED.—

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

22 “(A) conduct a declassification review of
23 each decision, order, or opinion issued by the
24 Foreign Intelligence Surveillance Court or the
25 Foreign Intelligence Surveillance Court of Re-

1 view (as defined in section 601(e)) that is de-
2 scribed in paragraph (2);

3 “(B) consistent with that review, make
4 publicly available to the greatest extent prac-
5 ticable each such decision, order, or opinion;
6 and

7 “(C) complete the declassification review
8 required by subparagraph (A) and public re-
9 lease of each such decision, order, or opinion
10 pursuant to subparagraph (B) by not later than
11 180 days after the date on which the Foreign
12 Intelligence Surveillance Court or the Foreign
13 Intelligence Surveillance Court of Review issues
14 such decision, order, or opinion.

15 “(2) DECISION, ORDER, OR OPINION DE-
16 SCRIBED.—A decision, order, or opinion issued by
17 the Foreign Intelligence Surveillance Court or the
18 Foreign Intelligence Surveillance Court of Review
19 that is described in this paragraph is any such deci-
20 sion, order, or opinion issued before, on, or after the
21 date of the enactment of this Act that—

22 “(A) includes a significant construction or
23 interpretation of any provision of law, including
24 any novel or significant construction or inter-
25 pretation of any term; or

1 “(B) has been nominated for a declas-
2 sification review by an amicus curiae appointed
3 by the court.”.

4 **SEC. 209. CLARIFICATION OF FOREIGN INTELLIGENCE SUR-**
5 **VEILLANCE COURT JURISDICTION OVER**
6 **RECORDS OF THE COURT AND OTHER ANCIL-**
7 **LARY MATTERS.**

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

11 (1) by adding at the end the following:

12 “(m) ANCILLARY CLAIMS.—

13 “(1) FOREIGN INTELLIGENCE SURVEILLANCE
14 COURT.—The Foreign Intelligence Surveillance
15 Court shall have jurisdiction to hear claims ancillary
16 to any of its own proceedings, including jurisdiction
17 to hear any claim for access to the court’s records,
18 files, and proceedings under the Constitution of the
19 United States, statute, common law, or any other
20 authority. Upon deciding such a claim, such court
21 shall provide immediately for the record a written
22 statement of the reasons for such decision. A party
23 may file a petition for review of such decision with
24 the Foreign Intelligence Surveillance Court of Re-
25 view, which shall have jurisdiction to consider such

1 petition and, upon deciding such petition, shall pro-
2 vide for the record a written statement of the rea-
3 sons for its decision.

4 “(2) FOREIGN INTELLIGENCE SURVEILLANCE
5 COURT OF REVIEW.—The Foreign Intelligence Sur-
6 veillance Court of Review shall have jurisdiction to
7 hear claims ancillary to any of its own proceedings,
8 including jurisdiction to hear any claim for access to
9 the court’s records, files, and proceedings under the
10 Constitution of the United States, statute, common
11 law, or any other authority. Upon deciding such a
12 claim, such court shall provide immediately for the
13 record a written statement of the reasons for such
14 decision.

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

21 (2) in subsection (a)(2)(A), in the matter pre-
22 ceding clause (i), by inserting “paragraph (1) of
23 subsection (l) of this section or” before “paragraph
24 (4) or (5) of section 702(i)”;

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

4 (b) TECHNICAL CORRECTIONS.—Section 103 of the
5 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.
6 1803), as amended by section (a), is further amended—

7 (1) in subsection (a)(2)(A), in the matter pre-
8 ceding clause (i), by striking “section 501(f) or”;
9 and

10 (2) in subsection (e), by striking “section
11 501(f)(1) or” each place it appears.

12 **SEC. 210. GROUNDS FOR DETERMINING INJURY IN FACT IN**
13 **CIVIL ACTIONS RELATING TO SURVEILLANCE**
14 **UNDER THE FOREIGN INTELLIGENCE SUR-**
15 **VEILLANCE ACT OF 1978 OR PURSUANT TO**
16 **EXECUTIVE AUTHORITY.**

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

1 **“TITLE X—ADDITIONAL**
2 **MATTERS**

3 **“SEC. 1001. CHALLENGES TO GOVERNMENT SURVEIL-**
4 **LANCE.**

5 “(a) DEFINITIONS.—In this section, the terms ‘for-
6 eign intelligence information’, ‘person’, ‘United States’,
7 and ‘United States person’ have the meaning given such
8 terms in section 101.

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

18 “(1)(A) regularly communicates foreign intel-
19 ligence information with persons who are not United
20 States persons and who are located outside the
21 United States; and

22 “(B) has taken or is taking objectively reasonable
23 measures to avoid the acquisition, copying, querying, re-
24 tention, access, or use of the person’s information under

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

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

7 “(c) REASONABLE BASIS.—For the purposes of this
8 section, a reasonable basis exists when the person dem-
9 onstrates a concrete injury arising from a good-faith belief
10 that the person’s rights have been, are being, or immi-
11 nently will be violated through the acquisition, copying,
12 querying, retention, access, or use of the person’s informa-
13 tion under this Act or pursuant to any other authority
14 of the executive branch of the Federal Government.

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

1 access, or use of information violates the Constitution or
2 laws of the United States.”.

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

“TITLE X—ADDITIONAL MATTERS

“Sec. 1001. Challenges to Government surveillance.”.

7 **SEC. 211. ACCOUNTABILITY PROCEDURES FOR VIOLATIONS**
8 **BY FEDERAL EMPLOYEES.**

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

13 **“SEC. 1002. ACCOUNTABILITY PROCEDURES FOR VIOLA-**
14 **TIONS BY FEDERAL EMPLOYEES.**

15 “(a) DEFINITIONS.—In this section:

16 “(1) APPROPRIATE COMMITTEES OF CON-
17 GRESS.—The term ‘appropriate committees of Con-
18 gress’ has the meaning given such term in section
19 101.

20 “(2) COVERED AGENCY.—The term ‘covered
21 agency’ means the Federal Bureau of Investigation,
22 the Central Intelligence Agency, the National Secu-
23 rity Agency, and the National Counterterrorism
24 Center.

1 “(3) COVERED VIOLATION.—The term ‘covered
2 violation’ means a violation of this Act or Executive
3 Order 12333 (50 U.S.C. 3001 note; relating to
4 United States intelligence activities), or successor
5 order, by an employee of a covered agency that re-
6 sults in the inappropriate collection, use, querying,
7 or dissemination of any communication, record, or
8 information of a United States person or a person
9 inside the United States.

10 “(4) PERSON, UNITED STATES, AND UNITED
11 STATES PERSON.—The terms ‘person’, ‘United
12 States’, and ‘United States person’ have the mean-
13 ings given such terms in section 101.

14 “(b) ACCOUNTABILITY PROCEDURES; DESIGNATED
15 INVESTIGATIVE ENTITY.—The head of each covered agen-
16 cy shall—

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

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

23 “(B) establish an internal process for the designated
24 entity to determine culpability for willful, knowing, reck-
25 less, and negligent covered violations.

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

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

6 “(2) Escalating consequences for willful, know-
7 ing, reckless, and negligent covered violations, in-
8 cluding—

9 “(A) consequences for an initial reckless or
10 negligent covered violation, including, at a min-
11 imum—

12 “(i) suspension of access to informa-
13 tion acquired under this Act or to the
14 dataset that gave rise to the violation for
15 not less than 90 days; and

16 “(ii) documentation of the incident in
17 the personnel file of each employee respon-
18 sible for the violation;

19 “(B) consequences for a second reckless or
20 negligent covered violation, including, at a min-
21 imum—

22 “(i) suspension of access to informa-
23 tion acquired under this Act or to the
24 dataset that gave rise to the violation for
25 not less than 180 days; and

1 “(ii) reassignment of each employee
2 responsible for the violation;

3 “(C) consequences for a third reckless or
4 negligent covered violation, including, at a min-
5 imum—

6 “(i) termination of security clearance;
7 and

8 “(ii) reassignment or termination of
9 each employee responsible for the violation;

10 “(D) consequences for an initial willful or
11 knowing covered violation, including, at a min-
12 imum—

13 “(i) suspension of access to informa-
14 tion acquired under this Act or to the
15 dataset that gave rise to the violation for
16 not less than 180 days; and

17 “(ii) reassignment of each employee
18 responsible for the violation; and

19 “(E) consequences for a second willful or
20 knowing covered violation, including, at a min-
21 imum—

22 “(i) termination of security clearance;
23 and

24 “(ii) reassignment or termination of
25 each employee responsible for the violation.

1 “(d) PRESUMPTION OF TERMINATION.—

2 “(1) IN GENERAL.—For purposes of subpara-
3 graphs (C)(ii) and (E)(ii) of subsection (c)(2), there
4 shall be a presumption in favor of termination of an
5 employee.

6 “(2) JUSTIFICATION.—If the head of a covered
7 agency determines not to terminate an employee for
8 a third reckless or negligent violation under subpara-
9 graph (C)(ii) of subsection (c)(2) or a second willful
10 or knowing violation under subparagraph (E)(ii) of
11 that subsection, the agency head shall submit to the
12 appropriate committees of Congress a written jus-
13 tification for the determination.

14 “(e) TIMING.—If a covered agency determines,
15 through an investigation, that an employee committed a
16 willful, knowing, reckless, or negligent covered violation,
17 the agency head shall determine what consequences to im-
18 pose on the employee under subsection (c)(2) not later
19 than 60 days after the conclusion of the investigation.”.

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

“Sec. 1002. Accountability procedures for violations by Federal employees.”.

23 (c) REPORT REQUIRED.—

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

1 of each covered agency, as defined in section 710 of
2 the Foreign Intelligence Surveillance Act of 1978 (as
3 added by subsection (a)), shall submit to the appro-
4 priate committees of Congress a report detailing—

5 (A) the procedures established under sec-
6 tion 710 of the Foreign Intelligence Surveil-
7 lance Act of 1978, as added by subsection (a);
8 and

9 (B) a description of any actions taken pur-
10 suant to such procedures.

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

15 **TITLE III—REFORMS RELATED**
16 **TO SURVEILLANCE CON-**
17 **DUCTED UNDER EXECUTIVE**
18 **ORDER 12333**

19 **SEC. 301. DEFINITIONS.**

20 In this title:

21 (1) INTELLIGENCE, INTELLIGENCE COMMU-
22 NITY, AND FOREIGN INTELLIGENCE.—The terms
23 “intelligence”, “intelligence community”, and “for-
24 eign intelligence” have the meanings given such

1 terms in section 3 of the National Security Act of
2 1947 (50 U.S.C. 3003).

3 (2) ELECTRONIC SURVEILLANCE, PERSON,
4 STATE, UNITED STATES, AND UNITED STATES PER-
5 SON.—The terms “electronic surveillance”, “per-
6 son”, “State”, “United States”, and “United States
7 person” have the meanings given such terms in sec-
8 tion 101 of the Foreign Intelligence Surveillance Act
9 of 1978 (50 U.S.C. 1801).

10 **SEC. 302. PROHIBITION ON WARRANTLESS QUERIES FOR**
11 **THE COMMUNICATIONS OF UNITED STATES**
12 **PERSONS AND PERSONS LOCATED IN THE**
13 **UNITED STATES.**

14 (a) IN GENERAL.—Except as provided in subsections
15 (b) and (c), no officer or employee of the Federal Govern-
16 ment may conduct a query of information acquired pursu-
17 ant to Executive Order 12333 (50 U.S.C. 3001 note; re-
18 lating to United States intelligence activities), or successor
19 order, in an effort to find communications or information
20 the compelled production of which would require a prob-
21 able cause warrant if sought for law enforcement purposes
22 in the United States of or about 1 or more United States
23 persons or persons reasonably believed to be located in the
24 United States at the time of the query or the time of the
25 communication or creation of the information.

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

3 (1) IN GENERAL.—Subsection (a) shall not
4 apply to a query relating to United States person or
5 persons reasonably believed to be located in the
6 United States at the time of the query or the time
7 of the communication or creation of the information
8 if—

9 (A) such persons or person are the subject
10 of an order or emergency authorization author-
11 izing electronic surveillance or physical search
12 under section 105 or 304 of the Foreign Intel-
13 ligence Surveillance Act of 1978 (50 U.S.C.
14 1805, 1824), or a warrant issued pursuant to
15 the Federal Rules of Criminal Procedure by a
16 court of competent jurisdiction covering the pe-
17 riod of the query;

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

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

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

1 graph (A) can, with due diligence, be ob-
2 tained; and

3 (ii) a description of the query is provided to the con-
4 gressional intelligence committees (as defined in section
5 3 of the National Security Act of 1947 (50 U.S.C. 3003))
6 in a timely manner;

7 (C) such persons or, if such person is in-
8 capable of providing consent, a third party le-
9 gally authorized to consent on behalf of the per-
10 son, has provided consent to the query on a
11 case-by-case basis; or

12 (D)(i) the query uses a known cybersecu-
13 rity threat signature as a query term;

14 (ii) the query is conducted, and the results of the
15 query are used, for the sole purpose of identifying targeted
16 recipients of malicious software and preventing or miti-
17 gating harm from such malicious software;

18 (iii) no additional contents of communications re-
19 trieved as a result of the query are accessed or reviewed;
20 and

21 (iv) all such queries are reported to the Foreign Intel-
22 ligence Surveillance Court.

23 (2) LIMITATIONS.—

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

1 trieved pursuant to a query authorized by para-
2 graph (1)(B) or evidence derived from such
3 query may be used, received in evidence, or oth-
4 erwise disseminated in any investigation, trial,
5 hearing, or other proceeding in or before any
6 court, grand jury, department, office, agency,
7 regulatory body, legislative committee, or other
8 authority of the United States, a State, or polit-
9 ical subdivision thereof, except in a proceeding
10 or investigation that arises from the threat that
11 prompted the query.

12 (B) ASSESSMENT OF COMPLIANCE.—Not
13 less frequently than annually, the Attorney
14 General shall assess compliance with the re-
15 quirements under subparagraphs (A).

16 (c) MATTERS RELATING TO EMERGENCY QUE-
17 RIES.—

18 (1) TREATMENT OF DENIALS.—In the event
19 that a query for communications or information the
20 compelled production of which would require a prob-
21 able cause warrant if sought for law enforcement
22 purposes in the United States relating to 1 or more
23 United States persons or persons reasonably believed
24 to be located in the United States at the time of the
25 query or the time of communication, or creation of

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

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

15 (B) no information concerning any United
16 States person or person reasonably believed to
17 be located in the United States at the time of
18 acquisition or the time of communication or
19 creation of the information acquired from such
20 query may subsequently be used or disclosed in
21 any other manner without the consent of such
22 person, except with the approval of the Attor-
23 ney General if the information indicates a
24 threat of death or serious bodily harm to any
25 person.

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

5 (d) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF
6 1978.—This section shall not apply to queries of commu-
7 nications and information collected pursuant to the For-
8 eign Intelligence Surveillance Act of 1978 (50 U.S.C.
9 1801 et seq.).

10 (e) FOREIGN INTELLIGENCE PURPOSE.—Except as
11 provided in subsection (b)(1), no officer or employee of
12 the United States may conduct a query of information ac-
13 quired pursuant to Executive Order 12333 (50 U.S.C.
14 3001 note; relating to United States intelligence activi-
15 ties), or successor order, in an effort to find information
16 of our about 1 or more United States persons or persons
17 reasonably believed to be located in the United States at
18 the time of the query or the time of communication or
19 creation of the information unless the query is reasonably
20 likely to retrieve foreign intelligence information.

21 (f) DOCUMENTATION.—No officer or employee of the
22 Federal Government may conduct a query of information
23 acquired pursuant to Executive Order 12333 (50 U.S.C.
24 3001 note; relating to United States intelligence activi-
25 ties), or successor order, in an effort to find information

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

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

10 (2) The date of the query.

11 (3) The identifier of the officer or employee.

12 (4) A statement of facts showing that the use
13 of each query term included under paragraph (1) is
14 reasonably likely to retrieve foreign intelligence in-
15 formation.

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

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

3 **SEC. 303. PROHIBITION ON REVERSE TARGETING OF**
4 **UNITED STATES PERSONS AND PERSONS LO-**
5 **CATED IN THE UNITED STATES.**

6 (a) PROHIBITION ON ACQUISITION.—

7 (1) PROHIBITION WITH EXCEPTIONS.—No offi-
8 cer or employee of the United States may inten-
9 tionally target, pursuant to Executive Order 12333
10 (50 U.S.C. 3001 note; relating to United States in-
11 telligence activities), or successor order, any person
12 if a significant purpose of the acquisition is to target
13 1 or more United States persons or persons reason-
14 ably believed to be located in the United States at
15 the time of acquisition, communication, or the cre-
16 ation of the information as prohibited by Section
17 703 of the Foreign Intelligence Surveillance Act of
18 1978, as added by section 201 of this Act, unless—

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

1 (ii) the information is sought for the pur-
2 pose of assisting that person; and

3 (iii) a description of the targeting is pro-
4 vided to the congressional intelligence commit-
5 tees (as defined in section 3 of the National Se-
6 curity Act of 1947 (50 U.S.C. 3003)) in a time-
7 ly manner; or

8 (B) the United States person or persons
9 reasonably believed to be located in the United
10 States at the time of acquisition, communica-
11 tion or creation of the information has provided
12 consent to the targeting, or if such person is in-
13 capable of providing consent, a third party le-
14 gally authorized to consent on behalf of such
15 person has provided consent.

16 (2) LIMITATION ON EXCEPTION.—No informa-
17 tion acquired pursuant to paragraph (1)(A) or evi-
18 dence derived from such targeting may be used, re-
19 ceived in evidence, or otherwise disseminated in any
20 investigation, trial, hearing, or other proceeding in
21 or before any court, grand jury, department, office,
22 agency, regulatory body, legislative committee, or
23 other authority of the United States, a State, or po-
24 litical subdivision thereof, except in proceedings or

1 investigations that arise from the threat that
2 prompted the targeting.

3 (b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF
4 1978 AND CRIMINAL WARRANTS.—This section shall not
5 apply to—

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

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

15 (3) an acquisition pursuant to a warrant issued
16 pursuant to the Federal Rules of Criminal Proce-
17 dure.

18 **SEC. 304. PROHIBITION ON INTELLIGENCE ACQUISITION**

19 **OF UNITED STATES PERSON DATA.**

20 (a) DEFINITIONS.—In this section:

21 (1) COVERED DATA.—The term “covered data”
22 means data, derived data, or any unique identifier
23 that—

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

1 (B) does not include data that—

2 (i) is lawfully available to the public
3 through Federal, State, or local govern-
4 ment records or through widely distributed
5 media;

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

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

12 (2) COVERED PERSON.—The term “covered
13 person” means an individual who—

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

17 (B) is a United States person.

18 (b) LIMITATION.—

19 (1) IN GENERAL.—Subject to paragraphs (2)
20 through (7), an element of the intelligence commu-
21 nity may not acquire a dataset that includes covered
22 data.

23 (2) AUTHORIZATION PURSUANT TO THE FOR-
24 EIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—
25 An element of the intelligence community may ac-

1 quire covered data if the data has been authorized
2 for collection pursuant to an order or emergency au-
3 thorization pursuant to the Foreign Intelligence Sur-
4 veillance Act of 1978 (50 U.S.C. 1801 et seq.) or
5 the Federal Rules of Criminal Procedure by a court
6 of competent jurisdiction covering the period of the
7 acquisition, subject to the use, dissemination,
8 querying, retention, and other minimization limita-
9 tions required by such authorization.

10 (3) AUTHORIZATION FOR EMPLOYMENT-RE-
11 LATED USE.—An element of the intelligence commu-
12 nity may acquire covered data about an employee of,
13 or applicant for employment by, an element of the
14 intelligence community for employment-related pur-
15 poses, provided that—

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

18 (B) the covered data is destroyed at such
19 time as it is no longer necessary for such pur-
20 poses.

21 (4) EXCEPTION FOR COMPLIANCE PURPOSES.—
22 An element of the intelligence community may ac-
23 quire covered data for the purpose of supporting
24 compliance with collection limitations and minimiza-
25 tion requirements imposed by statute, guidelines,

1 procedures, or the United States Constitution, pro-
2 vided that—

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

5 (B) the covered data is destroyed at such
6 time as it is no longer necessary for such pur-
7 pose.

8 (5) EXCEPTION FOR LIFE OR SAFETY.—An ele-
9 ment of the intelligence community may acquire cov-
10 ered data if—

11 (A) there is a reasonable belief that—

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

15 (ii) in order to prevent or mitigate
16 this threat, the acquisition must be con-
17 ducted before authorization pursuant to
18 paragraph (2) can, with due diligence, be
19 obtained;

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

22 (C) the covered data is destroyed at such
23 time as it is no longer necessary for such pur-
24 pose; and

1 (D) a description of the acquisition is pro-
2 vided to the congressional intelligence commit-
3 tees (as defined in section 3 of the National Se-
4 curity Act of 1947 (50 U.S.C. 3003)) in a time-
5 ly manner.

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

9 (A) each covered person linked or reason-
10 ably linked to the covered data, or, if such per-
11 son is incapable of providing consent, a third
12 party legally authorized to consent on behalf of
13 the person, has provided consent to the acquisi-
14 tion and use of the data on a case-by-case
15 basis;

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

19 (C) the covered data is destroyed at such
20 time as it is no longer necessary for such pur-
21 poses.

22 (7) EXCEPTION FOR NONSEGREGABLE DATA.—
23 An element of the intelligence community may ac-
24 quire a dataset that includes covered data if the cov-
25 ered data is not reasonably segregable prior to ac-

1 quisition, provided that the element of the intel-
2 ligence community complies with the minimization
3 procedures in subsection (c).

4 (c) MINIMIZATION PROCEDURES.—

5 (1) IN GENERAL.—The Attorney General shall
6 adopt specific procedures that are reasonably de-
7 signed to minimize the acquisition and retention of
8 covered data that is not subject to 1 or more of the
9 exceptions set forth in subsection (b).

10 (2) ACQUISITION AND RETENTION.—The proce-
11 dures adopted under paragraph (1) shall require ele-
12 ments of the intelligence community to exhaust all
13 reasonable means—

14 (A) to exclude covered data not subject to
15 1 or more exceptions set forth in subsection (b)
16 from datasets prior to acquisition; and

17 (B) to remove and delete covered data not
18 subject to 1 or more exceptions set forth in sub-
19 section (b) prior to the operational use of the
20 acquired dataset or the inclusion of the dataset
21 in a database intended for operational use.

22 (3) DESTRUCTION.—The procedures adopted
23 under paragraph (1) shall require that if an element
24 of the intelligence community identifies covered data

1 acquired in violation of subsection (b), such covered
2 data shall be promptly destroyed.

3 (d) PROHIBITION ON USE OF DATA OBTAINED IN
4 VIOLATION OF THIS SECTION.—Covered data acquired by
5 an element of the intelligence community in violation of
6 subsection (b), and any evidence derived therefrom, may
7 not be used, received in evidence, or otherwise dissemi-
8 nated in any investigation, trial, hearing, or other pro-
9 ceeding in or before any court, grand jury, department,
10 office, agency, regulatory body, legislative committee, or
11 other authority of the United States, a State, or political
12 subdivision thereof.

13 (e) REPORTING REQUIREMENT.—

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

22 (2) CONTENTS.—The report submitted pursu-
23 ant to paragraph (1) shall include the following:

24 (A) A description of the covered person in-
25 formation in each dataset.

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

3 (3) NOTIFICATIONS.—After submitting the re-
4 port required by paragraph (1), the Director shall,
5 in coordination with the Under Secretary, notify the
6 appropriate committees of Congress of any changes
7 to the information contained in such report.

8 (4) AVAILABILITY TO THE PUBLIC.—The Direc-
9 tor shall make available to the public on the website
10 of the Director—

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

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

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

20 **SEC. 305. PROHIBITION ON THE WARRANTLESS ACQUISI-**
21 **TION OF DOMESTIC COMMUNICATIONS.**

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

1 any communication as to which the sender and all in-
2 tended recipients are known to be located in the United
3 States at the time of acquisition or the time of commu-
4 nication except—

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

8 (2) if—

9 (A) there is a reasonable belief that—

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

13 (ii) in order to prevent or mitigate
14 this threat, the acquisition must be con-
15 ducted before an authorization pursuant to
16 the provisions of law cited in paragraph
17 (1) can, with due diligence, be obtained;
18 and

19 (B) a description of the acquisition is pro-
20 vided to the congressional intelligence commit-
21 tees (as defined in section 3 of the National Se-
22 curity Act of 1947 (50 U.S.C. 3003)) in a time-
23 ly manner.

24 (b) USE IN SUBSEQUENT PROCEEDINGS AND INVES-
25 TIGATIONS.—No information acquired pursuant to an

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

10 **SEC. 306. DATA RETENTION LIMITS.**

11 (a) PROCEDURES.—Each head of an element of the
12 Intelligence Community shall develop and implement pro-
13 cedures governing the retention of information collected
14 pursuant to Executive Order 12333 (50 U.S.C. 3001 note;
15 relating to United States intelligence activities), or suc-
16 cessor order.

17 (b) REQUIREMENTS.—

18 (1) COVERED INFORMATION DEFINED.—In this
19 subsection, the term “covered information” in-
20 cludes—

21 (A) any information, including an
22 encrypted communication, to, from, or per-
23 taining to a United States person or person
24 reasonably believed to be located in the United
25 States at the time of acquisition, communica-

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

4 (B) any unevaluated information, unless it
5 can reasonably be determined that the
6 unevaluated information does not contain com-
7 munications to or from, or information per-
8 taining to a United States person or person
9 reasonably believed to be located in the United
10 States at the time of acquisition, communica-
11 tion, or creation of the information.

12 (2) IN GENERAL.—The procedures developed
13 and implemented pursuant to subsection (a) shall
14 ensure, with respect to information described in such
15 subsection, that covered information shall be de-
16 stroyed within 5 years of collection unless the Attor-
17 ney General determines in writing that—

18 (A) the information is the subject of a
19 preservation obligation in pending administra-
20 tive, civil, or criminal litigation, in which case
21 the covered information shall be segregated, re-
22 tained, and used solely for that purpose and
23 shall be destroyed as soon as it is no longer re-
24 quired to be preserved for such litigation; or

1 (B) the information is being used in a pro-
2 ceeding or investigation in which the informa-
3 tion is directly related to and necessary to ad-
4 dress a specific threat identified in section
5 706(a)(2)(B) of the Foreign Intelligence Sur-
6 veillance Act of 1978 (50 U.S.C.
7 1881e(a)(2)(B)), as amended by section 102.

8 **SEC. 307. REPORTS ON VIOLATIONS OF LAW OR EXECUTIVE**
9 **ORDER.**

10 Section 511 of the National Security Act of 1947 (50
11 U.S.C. 3110) is amended by adding at the end the fol-
12 lowing:

13 “(c) PUBLIC AVAILABILITY.—The Director of Na-
14 tional Intelligence shall make each report submitted under
15 subsection (a) publicly available on an internet website,
16 with such redactions as may be necessary to protect
17 sources and methods.

18 “(d) DEPARTMENT OF JUSTICE REPORT.—The At-
19 torney General, in consultation with the Director of Na-
20 tional Intelligence, shall submit to the Committee on the
21 Judiciary of the Senate and the Committee on the Judici-
22 ary of the House of Representatives a version of the report
23 described in subsection (a) that only addresses violations
24 of the Foreign Intelligence Surveillance Act of 1978 (50
25 U.S.C. 1801 et seq.).”.

TITLE IV—INDEPENDENT OVERSIGHT

SEC. 401. INSPECTOR GENERAL OVERSIGHT OF ORDERS UNDER THE FOREIGN INTELLIGENCE SUR- VEILLANCE 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;

1 (ii) adequate safeguards are in place
2 to ensure that each application includes all
3 material information, including any infor-
4 mation that suggests that the court should
5 deny the application or that the court
6 should include one or more conditions in
7 an order, as required under section 901 of
8 the Foreign Intelligence Surveillance Act of
9 1978, as added by section 202(a); and

10 (iii) in the determination of the In-
11 spector General, there are any other areas
12 of potential risk or violation; and

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

16 (2) the Inspector General of the Department of
17 Justice shall assess the information provided by the
18 Department of Justice under section 903 and in-
19 clude a determination on the accuracy and complete-
20 ness of the information provided under that section.

21 (c) REPORT.—

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

1 findings and recommendations of the Inspector Gen-
2 eral and any remediations taken by the Department
3 or element, respectively.

4 (2) PERSONS SPECIFIED.—The persons speci-
5 fied in this paragraph are the following:

6 (A) The Attorney General.

7 (B) The Director of National Intelligence.

8 (C) The Privacy and Civil Liberties Over-
9 sight Board.

10 (D) The appropriate committees of Con-
11 gress.

12 (E) The Foreign Intelligence Surveillance
13 Court (as defined in section 601(e) of the For-
14 eign Intelligence Surveillance Act of 1978 (50
15 U.S.C. 1871(e))).

16 (F) Any amicus curiae appointed under
17 section 103(i)(2) of the Foreign Intelligence
18 Surveillance Act of 1978 (50 U.S.C.
19 1803(i)(2)).

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

1 (b)(2), subject to such procedures as are necessary to pro-
2 tect the national security of the United States.

3 (e) AVAILABILITY TO THE PUBLIC.—The Inspector
4 General of each element of the intelligence community
5 shall each make publicly available on a website of the rel-
6 evant element an unclassified version of any report sub-
7 mitted under subsection (c) by the respective Inspector
8 General.

9 **SEC. 402. DEPARTMENT OF JUSTICE INSPECTOR GENERAL**
10 **REVIEW OF HIGH INTENSITY DRUG TRAF-**
11 **FICKING AREA SURVEILLANCE PROGRAMS.**

12 (a) DEFINITION.—In this section:

13 (1) COVERED HIDTA SURVEILLANCE PRO-
14 GRAM.—The term “covered HIDTA surveillance pro-
15 gram” means a HIDTA surveillance program in
16 which a non-Federal government entity provides to
17 law enforcement agencies access to a database main-
18 tained by that entity containing information on more
19 than 1,000,000 United States persons or persons in
20 the United States.

21 (2) HIDTA SURVEILLANCE PROGRAM.—The
22 term “HIDTA surveillance program” means a pro-
23 gram that—

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

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

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

9 (3) UNITED STATES PERSON.—The term
10 “United States person” has the meaning given the
11 term in the Foreign Intelligence Surveillance Act of
12 1978 (50 U.S.C. 1801).

13 (b) REVIEW.—The Inspector General of the Depart-
14 ment of Justice shall—

15 (1) in the case of a HIDTA surveillance pro-
16 gram established before the date of the enactment of
17 this Act, conduct a review of such HIDTA surveil-
18 lance program—

19 (A) not later than 180 days after the ear-
20 lier of—

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

23 (ii) the date such HIDTA surveillance
24 program becomes a covered HIDTA sur-
25 veillance program; and

1 (B) not less frequently than once every 5
2 years for as long as such HIDTA surveillance
3 program is a covered HIDTA surveillance pro-
4 gram; and

5 (2) in the case of a HIDTA surveillance pro-
6 gram established after the date of the enactment of
7 this Act, conduct a review of such HIDTA surveil-
8 lance program—

9 (A) not later than 180 days after the
10 HIDTA surveillance program becomes a cov-
11 ered HIDTA surveillance program; and

12 (B) not less frequently than once every 5
13 years for as long as such HIDTA surveillance
14 program is a covered HIDTA surveillance pro-
15 gram.

16 **SEC. 403. INTELLIGENCE COMMUNITY PARITY AND COMMU-**
17 **NICATIONS WITH PRIVACY AND CIVIL LIB-**
18 **ERTIES OVERSIGHT BOARD.**

19 (a) WHISTLEBLOWER PROTECTIONS FOR MEMBERS
20 OF INTELLIGENCE COMMUNITY FOR COMMUNICATIONS
21 WITH PRIVACY AND CIVIL LIBERTIES OVERSIGHT
22 BOARD.—Section 1104 of the National Security Act of
23 1947 (50 U.S.C. 3234) is amended—

24 (1) in subsection (b)(1), in the matter before
25 subparagraph (A), by inserting “the Privacy and

1 Civil Liberties Oversight Board,” after “Inspector
2 General of the Intelligence Community,”; and

3 (2) in subsection (c)(1)(A), in the matter before
4 clause (i), by inserting “the Privacy and Civil Lib-
5 erties Oversight Board,” after “Inspector General of
6 the Intelligence Community,”.

7 (b) PARITY IN PAY FOR PRIVACY AND CIVIL LIB-
8 ERTIES OVERSIGHT BOARD STAFF AND THE INTEL-
9 LIGENCE COMMUNITY.—Section 1061(j)(1) of the Intel-
10 ligence Reform and Terrorism Prevention Act of 2004 (42
11 U.S.C. 2000ee(j)(1)) is amended by striking “except that”
12 and all that follows through the period at the end and
13 inserting “except that no rate of pay fixed under this sub-
14 section may exceed the highest amount paid by any ele-
15 ment of the intelligence community for a comparable posi-
16 tion, based on salary information provided to the chairman
17 of the Board by the Director of National Intelligence.”.

18 **SEC. 404. CONGRESSIONAL OVERSIGHT OF GRANTS OF IM-**
19 **MUNITY BY THE ATTORNEY GENERAL FOR**
20 **WARRANTLESS SURVEILLANCE ASSISTANCE.**

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

24 “(iv) Not later than 30 days after providing a certifi-
25 cation described in clause (B) of the first sentence of sub-

1 paragraph (ii) to a provider of wire or electronic commu-
2 nication service, an officer, employee, or agent thereof, a
3 landlord, a custodian, or another person, the person pro-
4 viding the certification shall submit the certification to the
5 appropriate committees of Congress, as defined in section
6 101 of the Foreign Intelligence Surveillance Act of 1978
7 (50 U.S.C. 1801).”.

8 (b) ONGOING PROGRAMS.—

9 (1) DEFINITIONS.—In this subsection—

10 (A) the term “appropriate committees of
11 Congress” has the meaning given that term in
12 section 101 of the Foreign Intelligence Surveil-
13 lance Act of 1978 (50 U.S.C. 1801), as amend-
14 ed by section 2 of this Act;

15 (B) the terms “electronic communication”,
16 “electronic communication service”, and “wire
17 communication” have the meanings given such
18 terms in section 2510 of title 18, United States
19 Code; and

20 (C) the term “ongoing certification” means
21 a certification described in clause (B) of the
22 first sentence of section 2511(2)(a)(ii) of title
23 18, United States Code, pursuant to which a
24 provider of wire or electronic communication
25 service, an officer, employee, or agent thereof,

1 a landlord, a custodian, or another person is
2 providing information, facilities, or technical as-
3 sistance on the date of enactment of this Act.

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

11 **TITLE V—REFORMS TO THE**
12 **ELECTRONIC COMMUNICA-**
13 **TIONS PRIVACY ACT OF 1986**

14 **SEC. 501. WARRANT PROTECTIONS FOR LOCATION INFOR-**
15 **MATION, WEB BROWSING RECORDS, AND**
16 **SEARCH QUERY RECORDS.**

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

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

21 (A) in subsection (a)—

22 (i) in the subsection heading, by strik-
23 ing “CONTENTS OF WIRE OR ELECTRONIC
24 COMMUNICATIONS” and inserting “LOCA-
25 TION INFORMATION, WEB BROWSING

1 RECORDS, SEARCH QUERY RECORDS, OR
2 CONTENTS OF WIRE OR ELECTRONIC
3 COMMUNICATIONS”; and

4 (ii) in the first sentence, by inserting
5 “location information, a web browsing
6 record, a search query record, or” before
7 “the contents of a wire”; and

8 (B) in subsection (c)(1), in the matter pre-
9 ceding subparagraph (A), by inserting “location
10 information, a web browsing record, a search
11 query record, or” before “the contents”.

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

14 (A) in the matter preceding paragraph (1),
15 by inserting “(a) IN GENERAL.—” before “As
16 used”;

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

18 (i) in paragraph (3)(C), by striking
19 “and” at the end;

20 (ii) in paragraph (4), by striking the
21 period at the end and inserting a semi-
22 colon; and

23 (iii) by adding at the end the fol-
24 lowing:

1 “(5) the term ‘location information’ means in-
2 formation derived or otherwise calculated from the
3 transmission or reception of a radio signal that re-
4 veals the approximate or actual geographic location
5 of a customer, subscriber, user, or device;

6 “(6) the term ‘web browsing record’—

7 “(A) means a record that reveals, in part
8 or in whole, the identity of a service provided
9 by an online service provider, or the identity of
10 a customer, subscriber, user, or device, for any
11 attempted or successful communication or
12 transmission between an online service provider
13 and such a customer, subscriber, user, or de-
14 vice;

15 “(B) includes a record that reveals, in part
16 or in whole—

17 “(i) the domain name, uniform re-
18 source locator, internet protocol address,
19 or other identifier for a service provided by
20 an online service provider with which a
21 customer, subscriber, user, or device has
22 exchanged or attempted to exchange a
23 communication or transmission; or

24 “(ii) the network traffic generated by
25 an attempted or successful communication

1 or transmission between a service provided
2 by an online service provider and a cus-
3 tomer, subscriber, user, or device; and

4 “(C) does not include a record that reveals
5 information about an attempted or successful
6 communication or transmission between a
7 known service and a particular, known cus-
8 tomer, subscriber, user, or device, if the record
9 is maintained by the known service and is lim-
10 ited to revealing additional identifying informa-
11 tion about the particular, known customer, sub-
12 scriber, user, or device;

13 “(7) the term ‘search query record’—

14 “(A) means a record that reveals a query
15 term or instruction submitted, in written,
16 verbal, or other format, by a customer, sub-
17 scriber, user, or device to any service provided
18 by an online service provider, including a search
19 engine, voice assistant, chat bot, or navigation
20 service; and

21 “(B) includes a record that reveals the re-
22 sponse provided by any service provided by an
23 online service provider to a query term or in-
24 struction by a customer, subscriber, user, or de-
25 vice;” and

1 (C) by adding at the end the following:

2 “(b) RULE OF CONSTRUCTION.—Nothing in this sec-
3 tion or section 2510 shall be construed to mean that a
4 record may not be more than 1 of the following types of
5 record:

6 “(1) The contents of a communication.

7 “(2) Location information.

8 “(3) A web browsing record.

9 “(4) A search query record.”.

10 (b) REAL-TIME SURVEILLANCE OF LOCATION INFOR-
11 MATION.—

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

14 (A) in the section heading, by striking
15 “**Mobile tracking devices**” and inserting
16 “**Tracking orders**”;

17 (B) by striking subsection (b);

18 (C) by redesignating subsection (a) as sub-
19 section (c);

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

22 “(a) IN GENERAL.—No officer or employee of a gov-
23 ernmental entity may install or direct the installation of
24 a tracking device, except pursuant to a warrant issued
25 using the procedures described in the Federal Rules of

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

8 “(b) EMERGENCIES.—

9 “(1) IN GENERAL.—Subject to paragraph (2),
10 the prohibition under subsection (a) does not apply
11 in a instance in which an investigative or law en-
12 forcement officer reasonably determines that—

13 “(A) a circumstance described in subpara-
14 graph (i), (ii), or (iii) of section 2518(7)(a) ex-
15 ists; and

16 “(B) there are grounds upon which a war-
17 rant could be issued to authorize the installa-
18 tion of the tracking device.

19 “(2) APPLICATION DEADLINE.—If a tracking
20 device is installed under the authority under para-
21 graph (1), an application for a warrant shall be
22 made within 48 hours after the installation.

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

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

4 “(4) LIMITATION.—In the event an application
5 for a warrant described in paragraph (2) is denied,
6 or in any other case where the use of a tracking de-
7 vice under the authority under paragraph (1) is ter-
8 minated without a warrant having been issued, the
9 information obtained shall be treated as having been
10 obtained in violation of this section, and an inven-
11 tory describing the installation and use of the track-
12 ing device shall be served on the person named in
13 the warrant application.”;

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

15 (i) in the subsection heading, by strik-
16 ing “IN GENERAL” and inserting “JURIS-
17 DICTION”;

18 (ii) by striking “or other order”;

19 (iii) by striking “mobile”;

20 (iv) by striking “such order” and in-
21 serting “such warrant”; and

22 (v) by adding at the end the following:

23 “For purposes of this subsection, the in-
24 stallation of a tracking device occurs with-
25 in the jurisdiction in which the device is

1 physically located when the installation is
2 complete.”; and

3 (F) by adding at the end the following:

4 “(d) DEFINITIONS.—As used in this section—

5 “(1) the term ‘computer’ has the meaning given
6 that term in section 1030(e);

7 “(2) the terms ‘court of competent jurisdiction’
8 and ‘governmental entity’ have the meanings given
9 such terms in section 2711;

10 “(3) the term ‘installation of a tracking device’
11 means, whether performed by an officer or employee
12 of a governmental entity or by a provider at the di-
13 rection of a governmental entity—

14 “(A) the physical placement of a tracking
15 device;

16 “(B) the remote activation of the tracking
17 software or functionality of a tracking device; or

18 “(C) the acquisition of a radio signal
19 transmitted by a tracking device; and

20 “(4) the term ‘tracking device’ means an elec-
21 tronic or mechanical device which permits the track-
22 ing of the movement of a person or object, including
23 a phone, wearable device, connected vehicle, or other
24 computer owned, used, or possessed by the target of
25 surveillance.”.

1 (2) CONFORMING AMENDMENTS.—

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

“3117. Tracking orders.”.

6 (B) Section 2510(12)(C) of title 18,
7 United States Code, is amended to read as fol-
8 lows:

9 “(C) a communication from a lawfully in-
10 stalled tracking device (as defined in section
11 3117 of this title), if—

12 “(i) the tracking device is physically
13 placed; or

14 “(ii) the tracking software or
15 functionality of the tracking device is re-
16 motely activated and the communication is
17 transmitted by the tracking software or
18 functionality as a result of the remote acti-
19 vation; or”.

20 (c) PROSPECTIVE SURVEILLANCE OF WEB BROWS-
21 ING RECORDS AND LOCATION INFORMATION.—Section
22 2703 of title 18, United States Code, is amended by add-
23 ing at the end the following:

24 “(i) PROSPECTIVE DISCLOSURE OF WEB BROWSING
25 RECORDS.—

1 “(1) IN GENERAL.—A governmental entity may
2 require the prospective disclosure by an online serv-
3 ice provider of a web browsing record only pursuant
4 to a warrant issued using the procedures described
5 in subsection (a).

6 “(2) TIME RESTRICTIONS.—A warrant requir-
7 ing the prospective disclosure by an online service
8 provider of web browsing records may require disclo-
9 sure of web browsing records for only a period as is
10 necessary to achieve the objective of the disclosure,
11 not to exceed 30 days from issuance of the warrant.
12 Extensions of such a warrant may be granted, but
13 only upon satisfaction of the showings necessary for
14 issuance of the warrant in the first instance.

15 “(j) PROSPECTIVE DISCLOSURE OF LOCATION
16 RECORDS.—A governmental entity may require the pro-
17 spective disclosure by an online service provider of location
18 information only pursuant to a warrant issued using the
19 procedures described in subsection (a), that satisfies the
20 restrictions imposed on warrants for tracking devices im-
21 posed by section 3117 of this title and rule 41 of the Fed-
22 eral Rules of Criminal Procedure.”.

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

3 Section 2703(c)(2)(C) of title 18, United States
4 Code, is amended by striking “local and long distance tele-
5 phone connection records, or”.

6 **SEC. 503. EMAIL PRIVACY ACT.**

7 (a) **SHORT TITLE.**—This section may be cited as the
8 “Email Privacy Act”.

9 (b) **VOLUNTARY DISCLOSURE CORRECTIONS.**—Sec-
10 tion 2702 of title 18, United States Code, is amended—

11 (1) in subsection (a)—

12 (A) in paragraph (1)—

13 (i) by striking “divulge” and inserting
14 “disclose”; and

15 (ii) by striking “while in electronic
16 storage by that service” and inserting
17 “that is in electronic storage with or other-
18 wise stored, held, or maintained by that
19 service”;

20 (B) in paragraph (2)—

21 (i) by striking “to the public”;

22 (ii) by striking “divulge” and insert-
23 ing “disclose”; and

24 (iii) by striking “which is carried or
25 maintained on that service” and inserting

1 “that is stored, held, or maintained by that
2 service”; and

3 (C) in paragraph (3)—

4 (i) by striking “divulge” and inserting
5 “disclose”; and

6 (ii) by striking “a provider of” and in-
7 serting “a person or entity providing”;

8 (2) in subsection (b)—

9 (A) in the matter preceding paragraph (1),
10 by inserting “wire or electronic” before “com-
11 munication”;

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

14 “(1) to an originator, addressee, or intended re-
15 cipient of such communication, to the subscriber or
16 customer on whose behalf the provider stores, holds,
17 or maintains such communication, or to an agent of
18 such addressee, intended recipient, subscriber, or
19 customer;”; and

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

22 “(3) with the lawful consent of the originator,
23 addressee, or intended recipient of such communica-
24 tion, or of the subscriber or customer on whose be-

1 half the provider stores, holds, or maintains such
2 communication;”;

3 (3) in subsection (c) by inserting “wire or elec-
4 tronic” before “communications”;

5 (4) in each of subsections (b) and (c), by strik-
6 ing “divulge” and inserting “disclose”; and

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

9 “(2) with the lawful consent of the subscriber
10 or customer;”.

11 (c) AMENDMENTS TO REQUIRED DISCLOSURE SEC-
12 TION.—Section 2703 of title 18, United States Code, as
13 amended by this Act, is amended—

14 (1) in subsection (a)—

15 (A) by striking “A governmental entity”
16 and inserting “Except as provided in sub-
17 sections (l) and (m), a governmental entity”;

18 (B) by striking “pursuant to” and insert-
19 ing “if the governmental entity obtains”; and

20 (C) by striking “by a court of competent
21 jurisdiction.” and inserting “that is issued by a
22 court of competent jurisdiction and that may
23 indicate the date by which the provider must
24 make the disclosure to the governmental entity.

25 In the absence of a date on the warrant indi-

1 eating the date by which the provider must
2 make disclosure to the governmental entity, the
3 provider shall promptly respond to the war-
4 rant.”;

5 (2) in subsection (c)—

6 (A) in paragraph (1)—

7 (i) in the matter preceding subpara-
8 graph (A)—

9 (I) by striking “A governmental
10 entity” and inserting “Except as pro-
11 vided in subsections (l) and (m), a
12 governmental entity”; and

13 (II) by striking “only when the
14 governmental entity—” and inserting
15 “only—”

16 (ii) in subparagraph (A)—

17 (I) by striking “obtains a war-
18 rant issued” and inserting “if the gov-
19 ernmental entity obtains a warrant”;

20 (II) by striking “by the Presi-
21 dent) by a court” and inserting the
22 following: “by the President) that—

23 “(i) is issued by a court”;

24 (III) by inserting “and” after
25 “jurisdiction;”; and

1 (IV) by adding at the end the fol-
2 lowing:

3 “(ii) may indicate the date by which the
4 online service provider must make the disclo-
5 sure to the governmental entity;”;

6 (iii) in subparagraph (B), by inserting
7 “if the governmental entity” before “ob-
8 tains”;

9 (iv) in subparagraph (C), by striking
10 “has the consent of the subscriber or cus-
11 tomer to such disclosure;” and inserting
12 “with the lawful consent of the subscriber
13 or customer; or”;

14 (v) by striking subparagraph (D);

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

17 (vii) in subparagraph (D), as so reded-
18 icated, by striking “seeks information”
19 and inserting “as otherwise authorized”;
20 and

21 (B) in paragraph (2)—

22 (i) in the matter preceding subpara-
23 graph (A), by inserting “, in response to
24 an administrative subpoena authorized by
25 Federal or State statute, a grand jury,

1 trial, or civil discovery subpoena, or any
2 means available under paragraph (1),”
3 after “shall”; and

4 (ii) in the matter following subpara-
5 graph (F), by striking “of a subscriber”
6 and all that follows and inserting “of a
7 subscriber or customer of such online serv-
8 ice provider.”;

9 (3) in subsection (d)—

10 (A) by striking “the contents of a wire or
11 electronic communication, or”;

12 (B) by striking “sought,” and inserting
13 “sought”; and

14 (C) by striking “section” and inserting
15 “subsection”; and

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

18 “(k) NOTICE.—Except as provided in section 2705,
19 an online service provider may notify a subscriber or cus-
20 tomer of a receipt of a warrant, court order, subpoena,
21 or request under subsection (a), (c), or (d) of this section.

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

1 State statute, a grand jury, trial, or civil discovery sub-
2 poena, or a warrant issued using the procedures described
3 in the Federal Rules of Criminal Procedure (or, in the
4 case of a State court, issued using State warrant proce-
5 dures) by a court of competent jurisdiction to—

6 “(1) require an originator, addressee, or in-
7 tended recipient of a wire or electronic communica-
8 tion that is not acting as an online service provider
9 with regard to that wire or electronic communication
10 to disclose a wire or electronic communication (in-
11 cluding the contents of that communication) to the
12 governmental entity;

13 “(2) require a person or entity that provides an
14 electronic communication service to the officers, di-
15 rectors, employees, or agents of the person or entity
16 (for the purpose of carrying out their duties) to dis-
17 close a wire or electronic communication (including
18 location information, a web browsing record, a
19 search query record, or the contents of that commu-
20 nication) to or from the person or entity itself or to
21 or from an officer, director, employee, or agent of
22 the entity to a governmental entity, if the wire or
23 electronic communication is stored, held, or main-
24 tained on an electronic communications system

1 owned, operated, or controlled by the person or enti-
2 ty; or

3 “(3) require an online service provider to dis-
4 close a wire or electronic communication (including
5 the contents of that communication) that advertises
6 or promotes a product or service and that has been
7 made readily accessible to the general public.

8 “(m) RULE OF CONSTRUCTION RELATED TO CON-
9 GRESSIONAL SUBPOENAS.—Nothing in this section or in
10 section 2702 shall limit the power of inquiry vested in the
11 Congress by article I of the Constitution of the United
12 States, including the authority to compel the production
13 of a wire or electronic communication (including location
14 information, a web browsing record, a search query record,
15 or the contents of a wire or electronic communication) that
16 is stored, held, or maintained by an online service pro-
17 vider.”.

18 (d) WARRANT REQUIREMENT FOR STORED COMMU-
19 NICATIONS CONTENT.—

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

22 (A) in subsection (a)—

23 (i) by striking “, that is in electronic
24 storage in an electronic communications

1 system for one hundred and eighty days or
2 less,”; and

3 (ii) by striking the last sentence;

4 (B) by striking subsection (b) and insert-
5 ing the following:

6 “(b) [Repealed].”; and

7 (C) in subsection (d) by striking “(b) or”.

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

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

12 (B) in section 2701(c)(3), by striking “,
13 2704”;

14 (C) by striking section 2704; and

15 (D) in section 2706(a), by striking “,
16 2703, or 2704” and inserting “or 2703”.

17 **SEC. 504. CONSISTENT PROTECTIONS FOR DEMANDS FOR**
18 **DATA HELD BY INTERACTIVE COMPUTING**
19 **SERVICES.**

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

24 “(8) the term ‘online service provider’ means a
25 provider of electronic communication service, a pro-

1 vider of remote computing service, or a provider of
2 an interactive computer service (as defined in section
3 230(f) of the Communications Act of 1934 (47
4 U.S.C. 230(f))); and”.

5 (b) REQUIRED DISCLOSURE.—Section 2703 of title
6 18, United States Code, is amended—

7 (1) in subsection (a), in the first sentence, by
8 striking “a provider of electronic communication
9 service” and inserting “an online service provider”;

10 (2) in subsection (c)—

11 (A) in paragraph (1), in the matter pre-
12 ceding subparagraph (A), by striking “a pro-
13 vider of electronic communication service or re-
14 mote computing service” and inserting “an on-
15 line service provider”; and

16 (B) in paragraph (2), in the matter pre-
17 ceding subparagraph (A), by striking “A pro-
18 vider of electronic communication service or re-
19 mote computing service” and inserting “An on-
20 line service provider”; and

21 (3) in subsection (g), by striking “a provider of
22 electronic communications service or remote com-
23 puting service” and inserting “an online service pro-
24 vider”.

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

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

5 (1) in section 3122(b)(2), by striking “that the
6 information likely to be obtained is relevant” and in-
7 serting “providing specific and articulable facts
8 showing there are reasonable grounds to believe that
9 the information likely to be obtained is relevant and
10 material”; and

11 (2) in section 3123(a)—

12 (A) in paragraph (1), in the first sen-
13 tence—

14 (i) by striking “the court shall enter”
15 and inserting “the court may enter”; and

16 (ii) by striking “certified to the court
17 that the information likely to be obtained
18 by such installation and use is relevant”
19 and inserting “submitted a certification
20 providing specific and articulable facts
21 showing there are reasonable grounds to
22 believe that the information likely to be ob-
23 tained by such installation and use is rel-
24 evant and material”; and

25 (B) in paragraph (2)—

1 (i) by striking “the court shall enter”
2 and inserting “the court may enter”; and
3 (ii) by striking “certified to the court
4 that the information likely to be obtained
5 by such installation and use is relevant”
6 and inserting “submitted a certification
7 providing specific and articulable facts
8 showing there are reasonable grounds to
9 believe that the information likely to be ob-
10 tained by such installation and use is rel-
11 evant and material”.

12 **SEC. 506. SUBPOENAS FOR CERTAIN SUBSCRIBER INFOR-**
13 **MATION.**

14 Section 2703(c)(2) of title 18, United States Code,
15 is amended, in the matter following subparagraph (F), as
16 amended by section 503(c) of this Act, by inserting “with
17 respect to whom the governmental entity identifies the
18 name, address, temporarily assigned network address, or
19 account identifier (such as a user name)” before the pe-
20 riod at the end.

21 **SEC. 507. MINIMIZATION STANDARDS FOR VOLUNTARY DIS-**
22 **CLOSURE OF CUSTOMER COMMUNICATIONS**
23 **OR RECORDS.**

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

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

6 (b) CONTENTS.—The procedures issued under sub-
7 section (a) shall include provisions to—

8 (1) limit, to the greatest extent possible, the ac-
9 quisition, use, and dissemination of the contents of
10 communication and records and other information to
11 that which is required for the specific purpose for
12 which the disclosure was intended;

13 (2) to the greatest extent possible, remove per-
14 sonally identifiable information prior to acquisition;

15 (3) to the extent personally identifiable infor-
16 mation cannot be removed prior to acquisition, mask
17 such information prior to its use or dissemination,
18 consistent with the purpose for which the disclosure
19 was intended; and

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

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

3 **SEC. 508. PROHIBITION ON LAW ENFORCEMENT PURCHASE**
4 **OF PERSONAL DATA FROM DATA BROKERS.**

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

7 “(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR
8 ANYTHING OF VALUE PERSONAL DATA BY LAW EN-
9 FORCEMENT AGENCIES.—

10 “(1) DEFINITIONS.—In this subsection and
11 subsection (f)—

12 “(A) the term ‘covered governmental enti-
13 ty’ means a law enforcement agency of a gov-
14 ernmental entity;

15 “(B) the term ‘covered organization’
16 means a person who—

17 “(i) is not a governmental entity; and

18 “(ii) is not an individual;

19 “(C) the term ‘covered person’ means an
20 individual who—

21 “(i) is reasonably believed to be lo-
22 cated inside the United States at the time
23 of the creation of the covered personal
24 data; or

1 “(ii) is a United States person, as de-
2 fined in section 101 of the Foreign Intel-
3 ligence Surveillance Act of 1978 (50
4 U.S.C. 1801);

5 “(D) the term ‘covered personal data’
6 means personal data relating to a covered per-
7 son;

8 “(E) the term ‘electronic device’ has the
9 meaning given the term ‘computer’ in section
10 1030(e);

11 “(F) the term ‘lawfully obtained public
12 data’ means personal data obtained by a par-
13 ticular covered organization that the covered or-
14 ganization—

15 “(i) reasonably understood to have
16 been voluntarily made available to the gen-
17 eral public by the covered person; and

18 “(ii) obtained in compliance with all
19 applicable laws, regulations, contracts, pri-
20 vacy policies, and terms of service;

21 “(G) the term ‘obtain in exchange for any-
22 thing of value’ means to obtain by purchasing,
23 to receive in connection with services being pro-
24 vided for monetary or nonmonetary consider-
25 ation, or to otherwise obtain in exchange for

1 consideration, including an access fee, service
2 fee, maintenance fee, or licensing fee; and

3 “(H) the term ‘personal data’—

4 “(i) means data, derived data, or any
5 unique identifier that is linked to, or is
6 reasonably linkable to, an individual or to
7 an electronic device that is linked to, or is
8 reasonably linkable to, 1 or more individ-
9 uals in a household;

10 “(ii) includes anonymized data that, if
11 combined with other data, can be linked to,
12 or is reasonably linkable to, an individual
13 or to an electronic device that identifies, is
14 linked to, or is reasonably linkable to 1 or
15 more individuals in a household; and

16 “(iii) does not include data that is
17 lawfully available through Federal, State,
18 or local government records or through
19 widely distributed media.

20 “(2) LIMITATION.—

21 “(A) IN GENERAL.—

22 “(i) PROHIBITION.—Subject to
23 clauses (ii) through (vii), a covered govern-
24 mental entity may not obtain in exchange

1 for anything of value covered personal data
2 if—

3 “(I) the covered personal data is
4 directly or indirectly obtained from a
5 covered organization; or

6 “(II) the covered personal data is
7 derived from covered personal data
8 that was directly or indirectly ob-
9 tained from a covered organization.

10 “(ii) EXCEPTION FOR CERTAIN COM-
11 PILATIONS OF DATA.—A covered govern-
12 mental entity may obtain in exchange for
13 something of value covered personal data
14 as part of a larger compilation of data
15 which includes personal data about persons
16 who are not covered persons, if—

17 “(I) the covered governmental
18 entity is unable through reasonable
19 means to exclude covered personal
20 data from the larger compilation ob-
21 tained; and

22 “(II) the covered governmental
23 entity minimizes any covered personal
24 data from the larger compilation, in
25 accordance with subsection (f).

1 “(iii) EXCEPTION FOR WHISTLE-
2 BLOWER DISCLOSURES TO LAW ENFORCE-
3 MENT.—Clause (i) shall not apply to cov-
4 ered personal data that is obtained by a
5 covered governmental entity under a pro-
6 gram established by an Act of Congress
7 under which a portion of a penalty or a
8 similar payment or bounty is paid to an in-
9 dividual who discloses information about
10 an unlawful activity to the Government,
11 such as the program authorized under sec-
12 tion 7623 of the Internal Revenue Code of
13 1986 (relating to awards to whistleblowers
14 in cases of underpayments or fraud).

15 “(iv) EXCEPTION FOR COST REIM-
16 BURSEMENT UNDER COMPULSORY LEGAL
17 PROCESS.—Clause (i) shall not apply to
18 covered personal data that is obtained by
19 a covered governmental entity from a cov-
20 ered organization in accordance with com-
21 pulsory legal process that—

22 “(I) is established by a Federal
23 or State statute; and

24 “(II) provides for the reimburse-
25 ment of costs of the covered organiza-

1 tion that are incurred in connection
2 with providing the record or informa-
3 tion to the covered governmental enti-
4 ty, such as the reimbursement of costs
5 under section 2706.

6 “(v) EXCEPTION FOR EMPLOYMENT-
7 RELATED USE.—Clause (i) shall not apply
8 to covered personal data about an em-
9 ployee of, or applicant for employment by,
10 a covered governmental entity that is—

11 “(I) obtained by the covered gov-
12 ernmental entity for employment-re-
13 lated purposes;

14 “(II) accessed and used by the
15 covered governmental entity only for
16 employment-related purposes; and

17 “(III) destroyed at such time as
18 the covered personal data is no longer
19 needed for employment-related pur-
20 poses.

21 “(vi) EXCEPTION FOR USE IN BACK-
22 GROUND CHECKS.—Clause (i) shall not
23 apply to covered personal data about a cov-
24 ered person that is—

1 “(I) obtained by a covered gov-
2 ernmental entity for purposes of con-
3 ducting a background check of the
4 covered person with the written con-
5 sent of the covered person;

6 “(II) accessed and used by the
7 covered governmental entity only for
8 background check-related purposes;
9 and

10 “(III) destroyed at such time as
11 the covered personal data is no longer
12 needed for background check-related
13 purposes.

14 “(vii) EXCEPTION FOR LAWFULLY OB-
15 TAINED PUBLIC DATA.—Clause (i) shall
16 not apply to covered personal data that is
17 obtained by a covered governmental entity
18 if—

19 “(I) the covered personal data is
20 lawfully obtained public data; or

21 “(II) the covered personal data is
22 derived from covered personal data
23 that solely consists of lawfully ob-
24 tained public data.

1 “(B) INDIRECTLY ACQUIRED RECORDS
2 AND INFORMATION.—The limitation under sub-
3 paragraph (A) shall apply without regard to
4 whether the covered organization possessing the
5 covered personal data is the covered organiza-
6 tion that initially obtained or collected, or is the
7 covered organization that initially received the
8 disclosure of, the covered personal data.

9 “(3) LIMIT ON SHARING BETWEEN AGEN-
10 CIES.—An agency of a governmental entity that is
11 not a covered governmental entity may not provide
12 to a covered governmental entity covered personal
13 data that was obtained in a manner that would vio-
14 late paragraph (2) if the agency of a governmental
15 entity were a covered governmental entity.

16 “(4) PROHIBITION ON USE AS EVIDENCE BY
17 COVERED GOVERNMENTAL ENTITIES.—

18 “(A) IN GENERAL.—Covered personal data
19 obtained by or provided to a covered govern-
20 mental entity in violation of paragraph (2) or
21 (3), and any evidence derived therefrom, may
22 not be used, received in evidence, or otherwise
23 disseminated by, on behalf of, or upon a motion
24 or other action by a covered governmental enti-
25 ty in any investigation, trial, hearing, or other

1 proceeding by, in, or before any court, grand
2 jury, department, officer, agency, regulatory
3 body, legislative committee, or other authority
4 of the United States, a State, or a political sub-
5 division thereof.

6 “(B) USE BY AGGRIEVED PARTIES.—Noth-
7 ing in subparagraph (A) shall be construed to
8 limit the use of covered personal data by a cov-
9 ered person aggrieved of a violation of para-
10 graph (2) or (3) in connection with any action
11 relating to such a violation.

12 “(f) MINIMIZATION PROCEDURES.—

13 “(1) IN GENERAL.—The Attorney General shall
14 adopt specific procedures that are reasonably de-
15 signed to minimize the acquisition and retention,
16 and to restrict the querying, of covered personal
17 data, and prohibit the dissemination of information
18 derived from covered personal data.

19 “(2) ACQUISITION AND RETENTION.—The pro-
20 cedures adopted under paragraph (1) shall require
21 covered governmental entities to exhaust all reason-
22 able means—

23 “(A) to exclude covered personal data that
24 is not subject to 1 or more of the exceptions set

1 forth in clauses (iii) through (vii) of subsection
2 (e)(2)(A) from the data obtained; and

3 “(B) to remove and delete covered personal
4 data described in subparagraph (A) after a
5 compilation is obtained and before operational
6 use of the compilation or inclusion of the com-
7 pilation in a dataset intended for operational
8 use.

9 “(3) DESTRUCTION.—The procedures adopted
10 under paragraph (1) shall require that, if a covered
11 governmental entity identifies covered personal data
12 in a compilation described in paragraph (2)(B), the
13 covered governmental entity shall promptly destroy
14 the covered personal data and any dissemination of
15 information derived from the covered personal data
16 shall be prohibited.

17 “(4) QUERYING.—

18 “(A) IN GENERAL.—Except as provided in
19 subparagraphs (B) and (C), no officer or em-
20 ployee of a covered governmental entity may
21 conduct a query of personal data, including per-
22 sonal data already subjected to minimization, in
23 an effort to find records of or about a par-
24 ticular covered person.

1 “(B) EXCEPTIONS.—Subparagraph (A)
2 shall not apply to a query related to a par-
3 ticular covered person if—

4 “(i) such covered person is the subject
5 of a court order issued under this title that
6 would authorize the covered governmental
7 entity to compel the production of the cov-
8 ered personal data, during the effective pe-
9 riod of that order;

10 “(ii) the officer or employee of a cov-
11 ered governmental entity carrying out the
12 query has a reasonable belief that the life
13 or safety of such covered person is threat-
14 ened and the information is sought for the
15 purpose of assisting that person, in which
16 case information resulting from the query
17 may be accessed or used solely for that
18 purpose and shall be destroyed at such
19 time as it is no longer necessary for such
20 purpose; or

21 “(iii) such covered person has con-
22 sented to the query.

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

1 “(i) each query shall be reasonably de-
2 signed to exclude personal data of covered
3 persons; and

4 “(ii) any personal data of covered per-
5 sons returned pursuant to a query shall
6 not be reviewed and shall immediately be
7 destroyed.”.

8 **SEC. 509. CONSISTENT PRIVACY PROTECTIONS FOR DATA**
9 **HELD BY DATA BROKERS.**

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

13 “(n) COVERED PERSONAL DATA.—

14 “(1) DEFINITIONS.—In this subsection, the
15 terms ‘covered personal data’ and ‘covered organiza-
16 tion’ have the meanings given such terms in section
17 2702(e).

18 “(2) LIMITATION.—Unless a governmental enti-
19 ty obtains an order in accordance with paragraph
20 (3), the governmental entity may not require a cov-
21 ered organization that is not an online service pro-
22 vider to disclose covered personal data if a court
23 order would be required for the governmental entity
24 to require an online service provider to disclose such

1 covered personal data that is a record of a customer
2 or subscriber of the online service provider.

3 “(3) ORDERS.—

4 “(A) IN GENERAL.—A court may only
5 issue an order requiring a covered organization
6 that is not an online service provider to disclose
7 covered personal data on the same basis and
8 subject to the same limitations as would apply
9 to a court order to require disclosure by an on-
10 line service provider.

11 “(B) STANDARD.—For purposes of sub-
12 paragraph (A), a court shall apply the most
13 stringent standard under Federal statute or the
14 Constitution of the United States that would be
15 applicable to a request for a court order to re-
16 quire a comparable disclosure by an online serv-
17 ice provider of a customer or subscriber of the
18 online service provider.”.

19 **SEC. 510. PROTECTION OF DATA ENTRUSTED TO INTER-**
20 **MEDIARY OR ANCILLARY SERVICE PRO-**
21 **VIDERS.**

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

1 “(9) the term ‘intermediary or ancillary service
2 provider’ means an entity or facilities owner or oper-
3 ator that directly or indirectly delivers, transmits,
4 stores, or processes communications or any other
5 covered personal data (as defined in section 2702(e)
6 of this title) for, or on behalf of, an online service
7 provider.”.

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

10 (1) in paragraph (1), by striking “and” at the
11 end;

12 (2) in paragraph (2)(B), by striking “and” at
13 the end;

14 (3) in paragraph (3), by striking the period at
15 the end and inserting “; and”; and

16 (4) by adding at the end the following:

17 “(4) an intermediary or ancillary service pro-
18 vider may not knowingly disclose—

19 “(A) to any person or entity the contents
20 of a communication while in electronic storage
21 by that intermediary or ancillary service pro-
22 vider; or

23 “(B) to any governmental entity a record
24 or other information pertaining to a subscriber
25 to or customer of, a recipient of a communica-

1 tion from a subscriber to or customer of, or the
2 sender of a communication to a subscriber to or
3 customer of, the online service provider for, or
4 on behalf of, which the intermediary or ancil-
5 lary service provider directly or indirectly deliv-
6 ers, transmits, stores, or processes communica-
7 tions or any other covered personal data (as de-
8 fined in subsection (e)).”.

9 **SEC. 511. MODERNIZING CRIMINAL SURVEILLANCE RE-**
10 **PORTS.**

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

13 (1) IN GENERAL.—Section 2703 of title 18,
14 United States Code, as amended by section 509 of
15 this Act, is amended by adding at the end the fol-
16 lowing:

17 “(o) REPORTS CONCERNING ACCESS TO CUSTOMER
18 COMMUNICATIONS OR RECORDS.—

19 “(1) IN GENERAL.—In January of each year,
20 any judge who has issued an order under this sec-
21 tion or a warrant to obtain records described in this
22 section, or who has denied approval of an application
23 under this section during the preceding year, shall
24 report to the Administrative Office of the United
25 States Courts—

1 “(A) the fact that the order or warrant
2 was applied for;

3 “(B) the type of records sought in the
4 order or warrant;

5 “(C) whether the order or warrant was—

6 “(i) granted as applied for;

7 “(ii) granted as modified; or

8 “(iii) denied;

9 “(D) the subsection of this section under
10 which the application for the order or warrant
11 was filed;

12 “(E) the nature of the offense or criminal
13 investigation that was the basis for the applica-
14 tion for the order or warrant;

15 “(F) the name of each provider of elec-
16 tronic communication service or remote com-
17 puting service served with the order or warrant,
18 if so granted; and

19 “(G) the investigative or law enforcement
20 agency that submitted the application.

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

1 Courts and include in the report required under sec-
2 tion 2519(3)—

3 “(A) a full and complete report concerning
4 the number of applications for orders or war-
5 rants requiring the disclosure of, during the
6 preceding calendar year—

7 “(i) the contents of wire or electronic
8 communications in electronic storage under
9 subsection (a); and

10 “(ii) records concerning electronic
11 communication service or remote computer
12 service under subsection (c);

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

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

20 “(3) FORMAT.—Not later than 180 days after
21 the date of enactment of the Government Surveil-
22 lance Reform Act of 2023, the Director of the Ad-
23 ministrative Office of the United States Courts shall,
24 in consultation with the National Institute of Stand-
25 ards and Technology, the Administrator of General

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

8 “(4) REGULATIONS.—The Director of the Ad-
9 ministrative Office of the United States Courts may
10 issue binding regulations with respect to the content
11 and form of the reports required under paragraph
12 (1).”.

13 (2) TECHNICAL AND CONFORMING AMEND-
14 MENT.—Section 2519(3) of title 18, United States
15 Code, is amended, in the first sentence, by inserting
16 “publish on the website of the Administrative Office
17 of the United States Courts and” before “transmit”.

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

21 **“§ 3126. Reports concerning pen registers and trap**
22 **and trace devices**

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

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

5 “(1) the fact that an order or extension was ap-
6 plied for;

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

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

10 “(4) the period of installation and use of a pen
11 register or trap and trace device authorized by the
12 order, and the number and duration of any exten-
13 sions of the order;

14 “(5) the offense specified in the order or appli-
15 cation, or extension of an order;

16 “(6) the precise nature of the facilities affected
17 and the precise nature of the information sought;
18 and

19 “(7) the investigative or law enforcement agen-
20 cy that submitted the application.

21 “(b) PUBLIC REPORT.—In June of each year, the Di-
22 rector of the Administrative Office of the United States
23 Courts shall publish on the website of the Administrative
24 Office of the United States Courts and include in the re-
25 port required under section 2519(3)—

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

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

6 “(B) the number of orders and extensions
7 granted or denied pursuant to this chapter dur-
8 ing the preceding calendar year; and

9 “(2) a detailed summary and analysis of each
10 category of data required to be reported under sub-
11 section (a).

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

22 “(d) **REGULATIONS.**—The Director of the Adminis-
23 trative Office of the United States Courts may issue bind-
24 ing regulations with respect to the content and form of
25 the reports required under subsection (a).”.

1 (c) REPORTING OF VOLUNTARY DISCLOSURES.—Sec-
2 tion 2702(d) of title 18, United States Code, is amended—

3 (1) in the heading, by striking “EMERGENCY”
4 and inserting “VOLUNTARY”;

5 (2) in the matter preceding paragraph (1), by
6 inserting “and publish on the website of the Depart-
7 ment of Justice” after “Senate”; and

8 (3) in paragraph (1)—

9 (A) by striking “the Department of Jus-
10 tice” and inserting “each Federal agency”; and

11 (B) by striking “subsection (b)(8)” and in-
12 serting “paragraph (5) or (8) of subsection (b)
13 or paragraph (3) or (4) of subsection (c), bro-
14 ken down by each such paragraph”;

15 (4) in paragraph (2)(A)—

16 (A) by striking “Department of Justice”
17 and inserting “Federal agency”; and

18 (B) by striking “subsection (b)(8)” and in-
19 serting “paragraph (5) or (8) of subsection (b)
20 or paragraph (3) or (4) of subsection (c)”; and
21 (5) by striking paragraph (3).

1 **TITLE VI—REGULATION OF GOV-**
2 **ERNMENT SURVEILLANCE**
3 **USING CELL SITE SIMULA-**
4 **TORS, GENERAL PROHIBI-**
5 **TION ON PRIVATE, NON-RE-**
6 **SEARCH USE**

7 **SEC. 601. CELL SITE SIMULATORS.**

8 (a) PROHIBITION.—Chapter 205 of title 18, United
9 States Code, is amended by adding at the end the fol-
10 lowing:

11 **“§ 3119. Cell-site simulators**

12 “(a) GENERAL PROHIBITION OF USE.—

13 “(1) IN GENERAL.—Except as provided in sub-
14 section (d), it shall be unlawful—

15 “(A) for any individual or entity to know-
16 ingly use a cell-site simulator in the United
17 States; or

18 “(B) for an element of the intelligence
19 community to use a cell-site simulator outside
20 the United States if the subject of the surveil-
21 lance is a United States person.

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

1 “(b) PENALTY.—Any individual or entity that vio-
2 lates subsection (a)(1) shall be fined not more than
3 \$250,000.

4 “(c) PROHIBITION OF USE AS EVIDENCE.—

5 “(1) IN GENERAL.—Except as provided in para-
6 graph (2), no information acquired through the use
7 of a cell-site simulator in violation of subsection
8 (a)(1), and no evidence derived therefrom, may be
9 used, received in evidence, or otherwise disseminated
10 in any investigation, trial, hearing, or other pro-
11 ceeding by, in, or before any court, grand jury, de-
12 partment, officer, agency, regulatory body, legislative
13 committee, or other authority of the United States,
14 a State, or a political subdivision thereof.

15 “(2) EXCEPTION FOR ENFORCEMENT.—Infor-
16 mation acquired through the use of a cell-site simu-
17 lator in violation of subsection (a)(1) by a person,
18 and evidence derived therefrom, may be used, re-
19 ceived in evidence, or otherwise disseminated in any
20 investigation trial, hearing, or other proceeding de-
21 scribed in paragraph (1) of this subsection relating
22 to the alleged violation of subsection (a)(1) in con-
23 nection with such use.

24 “(d) EXCEPTIONS.—

25 “(1) IN GENERAL.—

1 “(A) WARRANT.—

2 “(i) IN GENERAL.—Subsection (a)(1)
3 shall not apply to the use of a cell-site sim-
4 ulator by a law enforcement agency of a
5 governmental entity under a warrant
6 issued—

7 “(I) in accordance with this sub-
8 paragraph; and

9 “(II) using the procedures de-
10 scribed in, and in accordance with the
11 requirements for executing and re-
12 turning a warrant under, the Federal
13 Rules of Criminal Procedure (or, in
14 the case of a State court, issued using
15 State warrant and execution and re-
16 turn procedures and, in the case of a
17 court-martial or other proceeding
18 under chapter 47 of title 10 (the Uni-
19 form Code of Military Justice), issued
20 under section 846 of that title and in
21 accordance with the requirements for
22 executing and returning such a war-
23 rant, in accordance with regulations
24 prescribed by the President) by a
25 court of competent jurisdiction.

1 “(ii) REQUIREMENTS.—A court may
2 issue a warrant described in clause (i) (ex-
3 cept, with respect to a State court, to the
4 extent use of a cell-site simulator by a law
5 enforcement agency of a governmental en-
6 tity is prohibited by the law of the State)
7 only if the law enforcement agency—

8 “(I) demonstrates that other in-
9 vestigative procedures, including elec-
10 tronic location tracking methods that
11 solely collect records of the investiga-
12 tive target—

13 “(aa) have been tried and
14 have failed; or

15 “(bb) reasonably appear to
16 be—

17 “(AA) unlikely to suc-
18 ceed if tried; or

19 “(BB) too dangerous;

20 “(II) specifies the likely area of
21 effect of the cell-site simulator to be
22 used and the time that the cell-site
23 simulator will be in operation;

24 “(III) certifies that the requested
25 area of effect and time of operation

1 are the narrowest reasonably possible
2 to obtain the necessary information;
3 and

4 “(IV) demonstrates that the re-
5 quested use of a cell-site simulator
6 would be in compliance with applica-
7 ble provisions of the Communications
8 Act of 1934 (47 U.S.C. 151 et seq.)
9 and the rules of the Federal Commu-
10 nications Commission.

11 “(iii) CONSIDERATIONS.—In consid-
12 ering an application for a warrant de-
13 scribed in clause (i), the court shall—

14 “(I) consider—

15 “(aa) the number of individ-
16 uals impacted;

17 “(bb) the nature of any
18 communications to be obtained;
19 and

20 “(cc) the type of activities in
21 which users of an electronic de-
22 vice are engaged;

23 “(II) direct the law enforcement
24 agency of the governmental entity to
25 take steps to ensure heightened pro-

1 tections for constitutionally protected
2 activities and to minimize the collec-
3 tion of information relating to individ-
4 uals who are not the subject of the
5 warrant;

6 “(III) weigh the need of the gov-
7 ernment to enforce the law and appre-
8 hend criminals against the likelihood
9 and impact of any potential negative
10 side effects, including those disclosed
11 by the government under subpara-
12 graph (C); and

13 “(IV) not grant a request for a
14 warrant that would put public safety
15 at risk or unreasonably inconvenience
16 the community.

17 “(iv) PERIOD OF INITIAL AUTHORIZA-
18 TION.—No warrant described in clause (i)
19 may authorize the use of a cell site simu-
20 lator for any period longer than is nec-
21 essary to achieve the objective of the au-
22 thorization, nor in any event for longer
23 than 30 days.

24 “(v) EXTENSIONS.—

1 “(I) IN GENERAL.—A court may
2 grant extensions of a warrant de-
3 scribed in clause (i), but only upon
4 application for an extension made in
5 accordance with clause (i) and the
6 court considering the factors described
7 in clause (iii) and determining the re-
8 quirements under clause (ii) are met.

9 “(II) PERIOD OF EXTENSION.—
10 The period of an extension of a war-
11 rant shall be no longer than the au-
12 thorizing judge determines necessary
13 to achieve the purposes for which the
14 extension was granted, nor in any
15 event for longer than 30 days.

16 “(vi) TERMINATION PROVISION.—
17 Each warrant described in clause (i), and
18 each extension thereof, shall contain a pro-
19 vision that the authorization to use the cell
20 site simulator shall be executed as soon as
21 practicable and shall terminate upon at-
22 tainment of the authorized objective, or in
23 any event in 30 days.

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

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

3 “(I) the date on which a law en-
4 forcement agency first begins to use
5 the cell site simulator as authorized
6 by the warrant, or extension thereof;
7 or

8 “(II) the date that is 10 days
9 after the warrant, or extension there-
10 of, is issued.

11 “(B) EMERGENCY.—

12 “(i) IN GENERAL.—Subject to clause
13 (ii), subsection (a)(1) shall not apply to the
14 use of a cell-site simulator by a law en-
15 forcement agency of a governmental entity,
16 or use of a cell-site simulator as part of as-
17 sistance provided by a component of the
18 Department of Defense or an Armed Force
19 to such a law enforcement agency, if—

20 “(I) the governmental entity rea-
21 sonably determines an emergency ex-
22 ists that—

23 “(aa) involves—

1 “(AA) immediate dan-
2 ger of death or serious phys-
3 ical injury to any person;

4 “(BB) conspiratorial
5 activities characteristic of
6 organized crime; or

7 “(CC) an immediate
8 threat to a national security
9 interest; and

10 “(bb) requires use of a cell-
11 site simulator before a warrant
12 described in subparagraph (A)
13 can, with due diligence, be ob-
14 tained; and

15 “(II) except in an instance in
16 which the governmental entity is try-
17 ing to locate a lost or missing person,
18 locate someone believed to have been
19 abducted or kidnaped, or find victims,
20 dead or alive, in an area where a nat-
21 ural disaster, terrorist attack, or other
22 mass casualty event has taken place—

23 “(aa) there are grounds
24 upon which a warrant described

1 in subparagraph (A) could be en-
2 tered to authorize such use; and

3 “(bb) the governmental enti-
4 ty applies for a warrant described
5 in subparagraph (A) approving
6 such use not later than 48 hours
7 after such use begins, and takes
8 such steps to expedite the consid-
9 eration of such application as
10 may be possible.

11 “(ii) TERMINATION OF EMERGENCY
12 USE.—

13 “(I) IN GENERAL.—A law en-
14 forcement agency of a governmental
15 entity shall immediately terminate use
16 of a cell-site simulator under clause
17 (i) of this subparagraph at the earlier
18 of the time the information sought is
19 obtained or the time the application
20 for a warrant described in subpara-
21 graph (A) is denied.

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

1 “(aa) any information or
2 evidence derived from use of the
3 cell-site simulator shall be subject
4 to subsection (c);

5 “(bb) the attorney for the
6 governmental entity submitting
7 the application shall—

8 “(AA) retain, until the
9 date that is 1 year after the
10 date of the denial, a single
11 copy of any information or
12 evidence derived from use of
13 the cell-site simulator for po-
14 tential use by a person
15 about whose electronic de-
16 vice the government ob-
17 tained information with the
18 cell site simulator, which
19 may not be used for any
20 other purpose; and

21 “(BB) promptly destroy
22 any other copies of such in-
23 formation or evidence; and

24 “(cc) the applicable law en-
25 forcement agency shall serve no-

1 tice in accordance with subpara-
2 graph (D).

3 “(C) DISCLOSURES REQUIRED IN APPLICA-
4 TION.—In any application for a warrant au-
5 thorizing the use of a cell-site simulator under
6 subparagraph (A) or (B), the governmental en-
7 tity shall include the following:

8 “(i) A disclosure of any potential dis-
9 ruption of the ability of the subject of the
10 surveillance or bystanders to use commer-
11 cial mobile radio services or private mobile
12 services, including using advanced commu-
13 nications services, to make or receive, as
14 applicable—

15 “(I) emergency calls (including
16 9–1–1 calls);

17 “(II) calls to the universal tele-
18 phone number within the United
19 States for the purpose of the national
20 suicide prevention and mental health
21 crisis hotline system under designated
22 under paragraph (4) of section 251(e)
23 of the Communications Act of 1934
24 (47 U.S.C. 251(e));

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

6 “(IV) calls using telecommuni-
7 cations relay services; or

8 “(V) any other communications
9 or transmissions.

10 “(ii) A certification that the specific
11 model of the cell-site simulator to be used
12 has been inspected by a third party that is
13 an accredited testing laboratory recognized
14 by the Federal Communications Commis-
15 sion to verify the accuracy of the disclosure
16 under clause (i).

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

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

23 “(II) any user-defined limit on
24 the transmission range of the cell-site
25 simulator.

1 “(iv) A disclosure as to whether the
2 cell-site simulator will be used in an area
3 or at a gathering where constitutionally
4 protected activity, including speech or reli-
5 gious observance, will occur.

6 “(v) A disclosure as to whether sen-
7 sitive matters, such as attorney-client com-
8 munications, political campaign or political
9 party deliberations, medical information, or
10 communications among elected political
11 representatives of a State or the Federal
12 Government, will be implicated.

13 “(vi) A disclosure as to the estimated
14 number of individuals whose communica-
15 tions, electronic device, or location infor-
16 mation will be implicated.

17 “(D) NOTICE.—

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

21 “(I) the fact of the entry of the
22 warrant or the application;

23 “(II) the date of the entry and
24 the period of authorized, approved or

1 disapproved use of a cell-site simu-
2 lator, or the denial of the application;

3 “(III) whether, during the pe-
4 riod—

5 “(aa) information about
6 their electronic device was, or
7 was not, obtained by the govern-
8 ment;

9 “(bb) their location was, or
10 was not, tracked; and

11 “(cc) their communications
12 were, or were not, intercepted;
13 and

14 “(IV) confirmation that all infor-
15 mation unrelated to the individual to-
16 wards whom the warrant was directed
17 has been destroyed.

18 “(ii) PROVISION OF NOTICE TO OTHER
19 PARTIES.—The court issuing a warrant au-
20 thorizing the use of a cell-site simulator
21 may also require that notice be provided to
22 other persons not named in the applica-
23 tion, whose electronic devices the govern-
24 mental entity obtained information with
25 the cell site simulator.

1 “(2) FOREIGN INTELLIGENCE SURVEIL-
2 LANCE.—Use of a cell-site simulator by an element
3 of the intelligence community shall not be subject to
4 subsection (a)(1) if it is conducted in a manner that
5 is in accordance with title I of the Foreign Intel-
6 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et
7 seq.) (including testing or training authorized under
8 paragraph (1) or (3) of section 105(g) of such Act
9 (50 U.S.C. 1805(g)) (including such testing or train-
10 ing conducted in conjunction with a component of
11 the Department of Defense or an Armed Force), if
12 any information obtained during such testing or
13 training (including metadata) is destroyed after its
14 use for such testing or training).

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

19 “(A) a law enforcement agency of a gov-
20 ernmental entity;

21 “(B) an element of the intelligence commu-
22 nity; or

23 “(C) acting as an agent thereof.

24 “(4) PROTECTIVE SERVICES.—

1 “(A) IN GENERAL.—Subsection (a)(1)
2 shall not apply to the use of a cell-site simu-
3 lator in the performance of protective duties
4 pursuant to section 3056 of this title or as oth-
5 erwise authorized by law.

6 “(B) PROHIBITION ON USE AS EVI-
7 DENCE.—No information acquired through the
8 use of a cell-site simulator under the authority
9 under subparagraph (A), and no evidence de-
10 rived therefrom, may be used, received in evi-
11 dence, or otherwise disseminated in any inves-
12 tigation, trial, hearing, or other proceeding by,
13 in, or before any court, grand jury, department,
14 officer, agency, regulatory body, legislative com-
15 mittee, or other authority of the United States,
16 a State, or a political subdivision thereof.

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

23 “(5) CONTRABAND INTERDICTION BY CORREC-
24 TIONAL FACILITIES.—Subsection (a)(1) shall not
25 apply to the use of a contraband interdiction system

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

4 “(A) has—

5 “(i) taken reasonable steps to restrict
6 transmissions by the contraband interdic-
7 tion system to cellular devices physically lo-
8 cated within the property of the correc-
9 tional facility;

10 “(ii) posted signs around the correc-
11 tional facility informing visitors and staff
12 that the correctional facility employs such
13 a contraband interdiction system; and

14 “(iii) complied with any relevant regu-
15 lations promulgated by the Federal Com-
16 munications Commission and, as applica-
17 ble, policies issued by the National Tele-
18 communications and Information Adminis-
19 tration;

20 “(B) annually tests and evaluates compli-
21 ance with subparagraph (A) in accordance with
22 best practices, which shall be issued by the Fed-
23 eral Communications Commission; and

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

1 contraband interdiction system, whether in the
2 course of normal business operations or con-
3 ducting testing and evaluation, submits to the
4 Federal Communications Commission a report
5 describing the issues identified and the steps
6 taken to address the issues.

7 “(6) TESTING AND TRAINING BY LAW EN-
8 FORCEMENT.—Subsection (a)(1) shall not apply to
9 the use of a cell-site simulator by a law enforcement
10 agency of a governmental entity in the normal
11 course of official duties that is not targeted against
12 the communications of any particular person or per-
13 sons, under procedures approved by the Attorney
14 General, solely to—

15 “(A) test the capability of electronic equip-
16 ment, if—

17 “(i) it is not reasonable to obtain the
18 consent of the persons incidentally sub-
19 jected to the surveillance;

20 “(ii) the test is limited in extent and
21 duration to that necessary to determine to
22 capability of the equipment;

23 “(iii) any information obtained during
24 such testing (including metadata) is re-
25 tained and used only for the purpose of de-

1 termining the capability of the equipment,
2 is disclosed only to test personnel, and is
3 destroyed before or immediately upon com-
4 pletion of the test; and

5 “(iv) the test is for a period of not
6 longer than 90 days, unless the law en-
7 forcement agency obtains the prior ap-
8 proval of the Attorney General; or

9 “(B) train law enforcement personnel in
10 the use of electronic surveillance equipment,
11 if—

12 “(i) it is not reasonable to—

13 “(I) obtain the consent of the
14 persons incidentally subjected to the
15 surveillance;

16 “(II) train persons in the course
17 of otherwise authorized law enforce-
18 ment activities; or

19 “(III) train persons in the use of
20 such equipment without engaging in
21 surveillance;

22 “(ii) such surveillance is limited in ex-
23 tent and duration to that necessary to
24 train the personnel in the use of the equip-
25 ment; and

1 “(iii) any information obtained during
2 such training (including metadata) is de-
3 stroyed after its use for such training.

4 “(7) FCC TESTING.—Subsection (a)(1) shall
5 not apply to the use of a cell-site simulator by the
6 Federal Communications Commission, or an accred-
7 ited testing laboratory recognized by the Federal
8 Communications Commission, in order to test the
9 cell-site simulator.

10 “(8) RULE OF CONSTRUCTION.—Nothing in
11 this subsection shall be construed to exempt a State
12 or local government from complying with regulations
13 promulgated by the Federal Communications Com-
14 mission, including the requirement to obtain author-
15 ization to transmit on spectrum regulated by the
16 Federal Communications Commission.

17 “(e) LIMIT ON CERTAIN USE NOT CONDUCTED PUR-
18 SUANT TO WARRANTS AND ORDERS.—The use of a cell-
19 site simulator under subsection (d)(1)(B) of this section
20 (which shall not include such a use by a component of
21 the Department of Defense or an Armed Force providing
22 assistance to a law enforcement agency of a governmental
23 entity under such subsection (d)(1)(B)), under section
24 105(e) of the Foreign Intelligence Surveillance Act of
25 1978 (50 U.S.C. 1805(e)), or under clause (i) or (ii) of

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

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

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

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

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

22 “(f) MINIMIZATION.—

23 “(1) IN GENERAL.—The Attorney General shall
24 adopt specific procedures that are reasonably de-
25 signed to minimize the acquisition and retention,

1 provide for the destruction, and prohibit the dissemi-
2 nation, of information obtained through the use of
3 a cell-site simulator under an exception under para-
4 graph (1) or (2) of subsection (d) that pertains to
5 any person who is not an authorized subject of the
6 use.

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

11 “(3) USE BY AGENCIES.—If a law enforcement
12 agency of a governmental entity or element of the
13 intelligence community acquires information per-
14 taining to a person who is not an authorized subject
15 of the use of a cell-site simulator under an exception
16 under paragraph (1) or (2) of subsection (d), the
17 law enforcement agency or element of the intel-
18 ligence community shall—

19 “(A) minimize the acquisition and reten-
20 tion, and prohibit the dissemination, of the in-
21 formation in accordance with the procedures
22 adopted under paragraph (1); and

23 “(B) destroy the information (including
24 metadata) at the earliest possible opportunity.

1 “(g) DISCLOSURE TO DEFENDANT.—Any informa-
2 tion acquired through the operation of a cell-site simu-
3 lator, or derived from such information, including the fact
4 that the information was obtained or derived, as the case
5 may be, from a cell-site simulator, shall be disclosed to
6 the defendant in any action in which the information is
7 introduced into evidence.

8 “(h) SCOPE OF COLLECTION.—

9 “(1) AUTHORIZED USE.—Information collected
10 under this section may only include information
11 identifying nearby electronic devices communicating
12 with the cell-site simulator and the strength and di-
13 rection of transmissions from those electronic de-
14 vices.

15 “(2) COMPLIANCE WITH WIRETAPPING RE-
16 QUIREMENTS TO OBTAIN CONTENTS.—In the case of
17 any interception of a wire or electronic communica-
18 tion by the cell-site simulator—

19 “(A) with respect to an interception by a
20 law enforcement agency of a governmental enti-
21 ty, the provisions of chapter 119 shall apply in
22 addition to the provisions of this section; and

23 “(B) with respect to an interception by an
24 element of the intelligence community targeted
25 against a United States person or person lo-

1 cated in the United States, the element of the
2 intelligence community may only conduct the
3 surveillance using the cell-site simulator in ac-
4 cordance with an order authorizing the use
5 issued in accordance with title I of the Foreign
6 Intelligence Surveillance Act of 1978 (50
7 U.S.C. 1801 et seq.), in addition to complying
8 with the provisions of this section.

9 “(3) COMPLIANCE WITH TRACKING DEVICE RE-
10 QUIREMENTS.—

11 “(A) IN GENERAL.—If a cell-site simulator
12 is to be used by a law enforcement agency of
13 a governmental entity to locate or track the
14 movement of a person or object, the provisions
15 of section 3117 and rule 41 of the Federal
16 Rules of Criminal Procedure shall apply in ad-
17 dition to the provisions of this section.

18 “(B) COURT.—For purposes of applying
19 section 3117 and rule 41 of the Federal Rules
20 of Criminal Procedure to the use of a cell-site
21 simulator, a Federal court may authorize such
22 use within the jurisdiction of the court, and
23 outside that jurisdiction if—

24 “(i) the use commences within that
25 jurisdiction; or

1 “(ii) at the time the application is
2 presented to the court, the governmental
3 entity certifies that it has probable cause
4 to believe that the target is physically lo-
5 cated within that jurisdiction.

6 “(i) CIVIL ACTION.—Any person subject to an unlaw-
7 ful operation of a cell-site simulator may bring a civil ac-
8 tion for appropriate relief (including declaratory and in-
9 junctive relief, actual damages, statutory damages of not
10 more than \$500 for each violation, and attorney fees)
11 against the person, including a governmental entity, that
12 conducted that unlawful operation.

13 “(j) ADMINISTRATIVE DISCIPLINE.—If a court or ap-
14 propriate department or agency determines that the
15 United States or any of its departments or agencies has
16 violated any provision of this section, and the court or ap-
17 propriate department or agency finds that the cir-
18 cumstances surrounding the violation raise serious ques-
19 tions about whether or not an officer or employee of the
20 United States acted willfully or intentionally with respect
21 to the violation, the department or agency shall, upon re-
22 ceipt of a true and correct copy of the decision and find-
23 ings of the court or appropriate department or agency
24 promptly initiate a proceeding to determine whether dis-
25 ciplinary action against the officer or employee is war-

1 ranted. If the head of the department or agency involved
2 determines that disciplinary action is not warranted, he
3 or she shall notify the Inspector General with jurisdiction
4 over the department or agency concerned and shall provide
5 the Inspector General with the reasons for such deter-
6 mination.

7 “(k) DEFINITIONS.—As used in this section—

8 “(1) the terms defined in section 2711 have, re-
9 spectively, the definitions given such terms in that
10 section;

11 “(2) the term ‘advanced communications serv-
12 ices’ has the meaning given that term in section 3
13 of the Communications Act of 1934 (47 U.S.C.
14 153);

15 “(3) the term ‘cell-site simulator’ means any
16 device that functions as or simulates a base station
17 for commercial mobile services or private mobile
18 services in order to identify, locate, or intercept
19 transmissions from cellular devices for purposes
20 other than providing ordinary commercial mobile
21 services or private mobile services;

22 “(4) the term ‘commercial mobile radio service’
23 has the meaning given that term in section 20.3 of
24 title 47, Code of Federal Regulations, or any suc-
25 cessor thereto;

1 “(5) the term ‘contraband interdiction system’
2 means any device that functions as or simulates a
3 base station for commercial mobile services or pri-
4 vate mobile services for purposes of identifying, lo-
5 cating, or intercepting transmissions from contra-
6 band cellular devices in correctional facilities;

7 “(6) the term ‘derived’ means, with respect to
8 information or evidence, that the government would
9 not have originally possessed the information or evi-
10 dence but for the use of a cell-site simulator, and re-
11 gardless of any claim that the information or evi-
12 dence is attenuated from the surveillance would in-
13 evitably have been discovered, or was subsequently
14 reobtained through other means;

15 “(7) the term ‘electronic communication’ has
16 the meaning given that term in section 2510;

17 “(8) the term ‘electronic device’ has the mean-
18 ing given the term ‘computer’ in section 1030(e);

19 “(9) the term ‘emergency call’ has the meaning
20 given that term in section 6001 of the Middle Class
21 Tax Relief and Job Creation Act of 2012 (47 U.S.C.
22 1401));

23 “(10) the term ‘intelligence community’ has the
24 meaning given that term in section 3 of the National
25 Security Act of 1947 (50 U.S.C. 3003);

1 “(11) the term ‘mitigation’ means the deletion
2 of all information collected about a person who is
3 not the subject of the warrant or investigation;

4 “(12) the term ‘private mobile service’ has the
5 meaning given that term in section 332 of the Com-
6 munications Act of 1934 (47 U.S.C. 332);

7 “(13) the term ‘telecommunications relay serv-
8 ice’ has the meaning given that term in section 225
9 of the Communications Act of 1934 (47 U.S.C.
10 225); and

11 “(14) the term ‘United States person’ has the
12 meaning given that term in section 101 of the For-
13 eign Intelligence Surveillance Act of 1978 (50
14 U.S.C. 1801).”.

15 (b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF
16 1978 REQUIREMENTS.—The Foreign Intelligence Surveil-
17 lance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

18 (1) in section 101 (50 U.S.C. 1801), as amend-
19 ed by section 203 of this Act, by adding at the end
20 the following:

21 “(r) ‘Cell-site simulator’ has the meaning given that
22 term in section 3119 of title 18, United States Code.”;

23 (2) in section 102(a) (50 U.S.C. 1802(a)), by
24 adding at the end the following:

1 “(5) The Government may only use a cell-site simu-
2 lator pursuant to the authority under clause (i) or (ii) of
3 paragraph (1)(A) without obtaining an order under this
4 title authorizing such use if the Government has imple-
5 mented measures that are reasonably likely to limit the
6 collection activities to—

7 “(A) means of communications used exclusively
8 between or among foreign powers, as defined in
9 paragraph (1), (2), or (3) of section 101(a); or

10 “(B) property or premises under the open and
11 exclusive control of a foreign power, as defined in
12 paragraph (1), (2), or (3) of section 101(a).”; and

13 (3) in section 105 (50 U.S.C. 1805), by adding
14 at the end the following:

15 “(k)(1) A judge having jurisdiction under section 103
16 may issue an order under this section that authorizes the
17 use of a cell-site simulator only if the applicant—

18 “(A) demonstrates that other investigative pro-
19 cedures, including electronic location tracking meth-
20 ods that solely collect records of the investigative
21 target—

22 “(i) have been tried and have failed; or

23 “(ii) reasonably appear to be—

24 “(I) unlikely to succeed if tried; or

25 “(II) too dangerous;

1 “(B) specifies the likely area of effect of the
2 cell-site simulator to be used and the time that the
3 cell-site simulator will be in operation;

4 “(C) certifies that the requested area of effect
5 and time of operation are the narrowest reasonably
6 possible to obtain the necessary information;

7 “(D) specifies the procedures in place to ensure
8 that information unrelated to the target of the appli-
9 cation will be promptly destroyed; and

10 “(E) demonstrates that the requested use of a
11 cell-site simulator would be in compliance with appli-
12 cable provisions of the Communications Act of 1934
13 (47 U.S.C. 151 et seq.) and the rules of the Federal
14 Communications Commission.

15 “(2) In any application for an order under this sec-
16 tion authorizing the use of a cell-site simulator, the appli-
17 cant shall include the following:

18 “(A) A disclosure of any potential disruption of the
19 ability of the subject of the surveillance or bystanders to
20 use commercial mobile radio services or private mobile
21 services, including using advanced communications serv-
22 ices, to make or receive, as applicable—

23 “(i) emergency calls (including 9–1–1 calls);

24 “(ii) calls to the universal telephone number within
25 the United States for the purpose of the national suicide

1 prevention and mental health crisis hotline system under
2 designated under paragraph (4) of section 251(e) of the
3 Communications Act of 1934 (47 U.S.C. 251(e));

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

7 “(iv) calls using telecommunications relay services; or

8 “(v) any other communications or transmissions.

9 “(B) A certification that the specific model of the
10 cell-site simulator to be used has been inspected by a third
11 party that is an accredited testing laboratory recognized
12 by the Federal Communications Commission to verify the
13 accuracy of the disclosure under paragraph (1).

14 “(C) A disclosure of the methods and precautions
15 that will be used to minimize disruption, including—

16 “(i) any limit on the length of time the cell-site simu-
17 lator can be in continuous operation; and

18 “(ii) any user-defined limit on the transmission range
19 of the cell-site simulator.

20 “(D) A disclosure as to whether the cell-site simu-
21 lator will be used in an area or at a gathering where con-
22 stitutionally protected activity, including speech or reli-
23 gious observation, will occur.

24 “(E) A disclosure as to whether sensitive matters,
25 such as attorney-client communications, political cam-

1 paign or political party deliberations, medical information,
2 or communications among elected political representatives
3 of a State or the Federal Government, will be implicated.

4 “(F) A disclosure as to the estimated number of indi-
5 viduals whose communications, devices, or location infor-
6 mation will be implicated.

7 “(3) In considering an application for an order under
8 this section that authorizes the use of a cell-site simulator,
9 the court shall—

10 “(A) consider—

11 “(i) the number of individuals impacted;

12 “(ii) the nature of any communications to be ob-
13 tained; and

14 “(iii) the type of activities in which users of an elec-
15 tronic device (as defined in section 3119(k) of title 18,
16 United States Code) are engaged;

17 “(B) direct the Government to take steps to ensure
18 heightened protections for constitutionally protected ac-
19 tivities and to minimize the collection of any information
20 relating to individuals for whom the Government has not
21 established probable cause as to their status as a foreign
22 power or an agent of a foreign power;

23 “(C) weigh the need of the Government to obtain the
24 information sought against the likelihood and impact of

1 any potential negative side effects, including those dis-
2 closed by the Government under paragraph (2); and
3 “(D) not grant a request for an order that would put
4 public safety at risk or unreasonably inconvenience the
5 community.”.

6 (c) CONFORMING AMENDMENT.—Section 3127 of
7 title 18, United States Code, is amended—

8 (1) in paragraph (3) by striking “but such term
9 does not include any” and inserting “except such
10 term does not include any cell-site simulator, as that
11 term is defined in section 3119, or”; and

12 (2) in paragraph (4) by striking “of any com-
13 munication” and inserting “of any communication,
14 except such term does not include any cell-site simu-
15 lator, as that term is defined in section 3119”.

16 (d) INSPECTOR GENERAL REPORTS.—

17 (1) DEFINITION.—In this subsection, the term
18 “covered Federal entity” means—

19 (A) a law enforcement agency of a depart-
20 ment or agency of the Federal Government; and

21 (B) an element of the intelligence commu-
22 nity (as defined in section 3 of the National Se-
23 curity Act of 1947 (50 U.S.C. 3003)).

24 (2) REPORTS.—The Inspector General of the
25 Department of Justice, the Inspector General of the

1 Department of Homeland Security, the Inspector
2 General of the Department of Defense, and the In-
3 spector General of the Intelligence Community shall
4 annually submit to Congress a joint report, and pub-
5 lish an unclassified version of the report on the
6 website of each such inspector general, on—

7 (A) the overall compliance of covered Fed-
8 eral entities with this title and the amendments
9 made by this title;

10 (B) the number of applications by covered
11 Federal entities for use of a cell-site simulator
12 that were applied for and the number that were
13 granted;

14 (C) the number of emergency uses of a
15 cell-site simulator under section 3119(d)(1)(B)
16 of title 18, United States Code, as added by
17 this title;

18 (D) the number of such emergency uses
19 for which a court subsequently issued a warrant
20 authorizing the use and the number of such
21 emergency uses in which an application for a
22 warrant was denied;

23 (E) the number of devices that were tar-
24 geted with a cell-site simulator, which shall be
25 provided separately for targeting conducted

1 pursuant to a warrant or court order and tar-
2 geting conducted pursuant to an authority to
3 use a cell-site simulator without a warrant or
4 order;

5 (F) the number of devices that were not
6 the target of the use of a cell-site simulator
7 about which information was obtained with the
8 cell-site simulator, which shall—

9 (i) be provided separately for use con-
10 ducted pursuant to a warrant or court
11 order and use conducted pursuant to an
12 authority to use a cell-site simulator with-
13 out a warrant or order; and

14 (ii) include the number of such de-
15 vices about which the information was not
16 destroyed as a result of the minimization
17 requirements under section 3119(f) of title
18 18, United States Code, as added by this
19 section, which shall be provided separately
20 for use conducted pursuant to a warrant or
21 court order and use conducted pursuant to
22 an authority to use a cell-site simulator
23 without a warrant or order;

24 (G) which components of a law enforce-
25 ment agency of a department or agency of the

1 Federal Government are using cell-site simula-
2 tors and how many are available to that compo-
3 nent; and

4 (H) instances in which a law enforcement
5 agency of a department or agency of the Fed-
6 eral Government made cell-site simulators avail-
7 able to a State or unit of local government.

8 (3) FORM OF REPORTS.—Each report sub-
9 mitted under paragraph (2) shall be submitted in
10 unclassified form, but may include a classified
11 annex.

12 (e) FCC REGULATIONS.—

13 (1) IN GENERAL.—Not later than 180 days
14 after the date of enactment of this Act, the Federal
15 Communications Commission shall initiate any pro-
16 ceeding that may be necessary to promulgate or
17 modify regulations promulgated by the Federal Com-
18 munications Commission to implement this title and
19 the amendments made by this title.

20 (2) CONSTRUCTION.—Nothing in this title or
21 an amendment made by this title shall be construed
22 to expand or contract the authority of the Federal
23 Communications Commission.

24 (f) EFFECTIVE DATE.—

1 (1) IN GENERAL.—Except as provided in para-
2 graph (2), subsections (a), (b), (c), and (d) of this
3 section, and the amendments made by such sub-
4 sections, shall apply on and after the date that is 2
5 years after the date of enactment of this Act.

6 (2) EXCEPTIONS.—

7 (A) DEFINITION.—In this paragraph, the
8 term “cell-site simulator” has the meaning
9 given that term in section 3119 of title 18,
10 United States Code, as added by subsection (a).

11 (B) EXTENSION FOR EXISTING CELL-SITE
12 SIMULATORS.—For any model of a cell-site sim-
13 ulator in use before the date of enactment of
14 this Act, including such use in a contraband
15 interdiction system at a correctional facility, if
16 the Attorney General certifies that additional
17 time is necessary to obtain independent tests of
18 the model of cell-site simulator, subsections (a),
19 (b), (c), and (d) of this section, and the amend-
20 ments made by such subsections, shall apply to
21 the use of the model of cell-site simulator on
22 and after the date that is 3 years after the date
23 of enactment of this Act.

1 **TITLE VII—PROTECTION OF CAR**
2 **DATA FROM WARRANTLESS**
3 **SEARCHES**

4 **SEC. 701. PROTECTION OF CAR DATA FROM WARRANTLESS**
5 **SEARCHES.**

6 (a) IN GENERAL.—Part I of title 18, United States
7 Code, is amended by adding at the end the following:

8 **“CHAPTER 124—ACCESSING VEHICLE**
9 **DATA.**

“Sec.

“2730. Definitions.

“2731. Prohibition on access to vehicle data.

“2732. Prohibition on use of acquired information as evidence.

10 **“§ 2730. Definitions**

11 “In this chapter:

12 “(1) ACCESS.—The term ‘access’—

13 “(A) means any retrieval of covered vehicle
14 data, regardless of—

15 “(i) whether the data is obtained as
16 the information is being produced or from
17 digital storage; and

18 “(ii) where the vehicle data is stored
19 or transmitted, including by wire or radio;
20 and

21 “(B) does not include data covered by
22 chapter 119 of this title or section 104 of the

1 Foreign Intelligence Surveillance Act of 1978
2 (50 U.S.C. 1804).

3 “(2) CONSENT.—The term ‘consent’—

4 “(A) means an affirmative, express, and
5 voluntary agreement that—

6 “(i) states that the person providing
7 the consent is providing consent to a gov-
8 ernment official to access the digital con-
9 tents, access credential, or online account
10 information, or other information being
11 sought;

12 “(ii) specifies the type of content, ac-
13 cess credential, or online account informa-
14 tion the person is providing access to;

15 “(iii) specifies the time period of the
16 covered vehicle data to be accessed;

17 “(iv) informs the person providing
18 consent that consent is optional and that
19 the government official attempting to ob-
20 tain consent must otherwise acquire a war-
21 rant if consent is not obtained;

22 “(v) does not involve sanctions or the
23 threat of sanctions for withholding consent;
24 and

1 “(vi) uses clear, simple, and com-
2 prehensible language that is presented in a
3 way that is accessible to the person pro-
4 viding consent; and

5 “(B) does not include consent obtained
6 through agreement to a generic privacy policy.

7 “(3) COVERED VEHICLE DATA.—The term ‘cov-
8 ered vehicle data’—

9 “(A) means all onboard and telematics
10 data generated by, processed by, or stored on a
11 noncommercial vehicle using computing, storage
12 and communication systems installed, attached
13 to, or carried in the vehicle, including diagnostic
14 data, entertainment system data, navigation
15 data, images or data captured by onboard sen-
16 sors, or cameras, including images or data used
17 to support automated features or autonomous
18 driving, internet access, and communication to
19 and from vehicle occupants;

20 “(B) includes data gathered by event data
21 recorders; and

22 “(C) does not include—

23 “(i) automotive software installed by
24 the manufacturer, as defined by applicable
25 industry standards or regulations;

1 “(ii) any data subject to chapter 119
2 of this title or section 104 of the Foreign
3 Intelligence Surveillance Act of 1978 (50
4 U.S.C. 1804); or

5 “(iii) data that is collected from out-
6 side the vehicle, including speed data and
7 geolocation data, for purposes of traffic,
8 law enforcement, or toll collection.

9 “(4) EVENT DATA RECORDER.—The term
10 ‘event data recorder’ has the meaning given the term
11 in section 563.5 of title 49, Code of Federal Regula-
12 tions (as in effect on March 5, 2019).

13 “(5) INVESTIGATIVE OR LAW ENFORCEMENT
14 OFFICER.—The term ‘investigative or law enforce-
15 ment officer’ means any officer of the United States
16 or of a State or political subdivision thereof and any
17 Tribal justice official, who is empowered by law to
18 execute searches, to seize evidence, or to make ar-
19 rests for a violation of Federal or State law.

20 “(6) NONCOMMERCIAL VEHICLE.—The term
21 ‘noncommercial vehicle’ has the meaning given the
22 term ‘non-CMV’ in section 383.5 of title 49, Code of
23 Federal Regulations.

1 “(7) STATE.—The term ‘State’ means any
2 State of the United States, the District of Columbia,
3 and any territory or possession of the United States.

4 “(8) VEHICLE OPERATOR.—The term ‘vehicle
5 operator’ means—

6 “(A) a person who controls the operation
7 of a vehicle at the time consent is sought; and

8 “(B) with respect to a vehicle that is not
9 classified as a highly autonomous vehicle by the
10 Secretary of Transportation, the driver of the
11 vehicle.

12 **“§ 2731. Prohibition on access to vehicle data**

13 “(a) IN GENERAL.—Except as provided in subsection
14 (b), an investigative or law enforcement officer may not
15 access covered vehicle data unless pursuant to a warrant
16 issued in accordance with the procedures described in rule
17 41 of the Federal Rules of Criminal Procedure (or, in the
18 case of a State court, issued using State warrant proce-
19 dures) by a court of competent jurisdiction, or as other-
20 wise provided in this chapter or sections 104 and 303 of
21 the Foreign Intelligence Surveillance Act of 1978 (50
22 U.S.C. 1804, 1823).

23 “(b) EXCEPTIONS.—

24 “(1) CONSENT.—

1 “(A) IN GENERAL.—An investigative or
2 law enforcement officer may access covered ve-
3 hicle data if—

4 “(i) the vehicle operator provides prior
5 consent to such access; and

6 “(ii) no passenger 14 years of age or
7 older objects to the access.

8 “(B) VEHICLE OWNER.—If the vehicle op-
9 erator cannot be located with reasonable effort,
10 the vehicle owner or, in the case of a leased ve-
11 hicle, the lessee, may provide consent under this
12 paragraph.

13 “(C) UNLAWFUL POSSESSION.—No indi-
14 vidual may provide or withhold consent under
15 this paragraph or object to another individual
16 accessing covered vehicle data if the indi-
17 vidual—

18 “(i) is the vehicle operator who is in
19 unlawful possession of the vehicle; or

20 “(ii) is a passenger who unlawfully
21 obtained access to the vehicle.

22 “(D) ORAL CONSENT.—Consent provided
23 under this paragraph shall be in writing un-
24 less—

1 “(i) the person providing the consent
2 requests that the consent be made orally;
3 and

4 “(ii) the request for consent and the
5 consent are recorded.

6 “(E) CONSENT OF VEHICLE OPERATOR.—

7 If the vehicle operator is not the owner of the
8 vehicle and provides consent under this para-
9 graph, the consent is valid only with respect to
10 covered vehicle data generated during the lawful
11 possession and use of the vehicle by the vehicle
12 operator.

13 “(2) EMERGENCY.—

14 “(A) IN GENERAL.—An investigative or
15 law enforcement officer, the Attorney General,
16 the Deputy Attorney General, the Associate At-
17 torney General, or the principal prosecuting at-
18 torney of any State or subdivision thereof act-
19 ing pursuant to a statute of that State, may ac-
20 cess covered vehicle data if—

21 “(i) such officer reasonably deter-
22 mines that an emergency situation exists
23 that—

1 “(I) involves immediate danger of
2 death or serious physical injury to any
3 person; and

4 “(II) requires access to covered
5 vehicle data before such officer can,
6 with due diligence, obtain a warrant;

7 “(ii) there are grounds upon which a
8 warrant could be granted to authorize such
9 access; and

10 “(iii) an application for a warrant ap-
11 proving such access is submitted to a court
12 within 48 hours after the access has oc-
13 curred or begins to occur.

14 “(B) DENIAL.—If an application for a
15 warrant submitted pursuant to subparagraph
16 (A)(iii) is denied, any covered vehicle data
17 accessed under this paragraph shall be treated
18 as having been obtained in violation of this
19 chapter.

20 “(3) EVENT DATA RECORDER FOR MOTOR VE-
21 HICLE SAFETY.—In addition to the exceptions in
22 paragraphs (1) and (2), data recorded or trans-
23 mitted by an event data recorder may be accessed
24 from a noncommercial vehicle if authorized by para-

1 graph (3), (4), or (5) of section 24302(b) of the
2 Driver Privacy Act of 2015 (49 U.S.C. 30101 note).

3 “(4) RULE OF CONSTRUCTION.—Nothing in
4 this section shall be interpreted to require the trans-
5 mission or storage of data that is not otherwise
6 transmitted or stored, or the retrieval of data that
7 is not generally retrievable.

8 **“§ 2732. Prohibition on use of acquired information**
9 **as evidence**

10 “(a) IN GENERAL.—If any covered vehicle data has
11 been acquired in violation of this chapter, no part of such
12 information and no evidence derived therefrom may be
13 used, received in evidence, or otherwise disseminated in
14 any investigation, trial, hearing, or other proceeding by,
15 in, or before any court, grand jury, department, officer,
16 agency, regulatory body, legislative committee, or other
17 authority of the United States, a State, or a political sub-
18 division thereof.

19 “(b) PROBABLE CAUSE.—No data described in sec-
20 tion 2731(b)(3) may be used to establish probable cause.”.

21 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

22 (1) DRIVER PRIVACY ACT OF 2015.—Section
23 24302 of the Driver Privacy Act of 2015 (49 U.S.C.
24 30101 note) is amended—

1 (A) in subsection (b), in the matter pre-
 2 ceding paragraph (1), by striking “Data” and
 3 inserting “Except as provided in subsection (c),
 4 data”; and

5 (B) by adding at the end the following:

6 “(c) INVESTIGATIVE OR LAW ENFORCEMENT OFFI-
 7 CERS.—An investigative or law enforcement officer may
 8 only access or retrieve data recorded or transmitted by an
 9 event data recorder described in subsection (a) in accord-
 10 ance with chapter 124 of title 18, United States Code.”.

11 (2) TABLE OF CHAPTERS.—The table of chap-
 12 ters for part 1 of title 18, United States Code, is
 13 amended by adding at the end the following:

“124. Accessing vehicle data 2730”.

14 **TITLE VIII—INTELLIGENCE** 15 **TRANSPARENCY**

16 **SEC. 801. ENHANCED ANNUAL REPORTS BY DIRECTOR OF** 17 **THE ADMINISTRATIVE OFFICE OF THE** 18 **UNITED STATES COURTS.**

19 Section 603(a)(1) of the Foreign Intelligence Surveil-
 20 lance Act of 1978 (50 U.S.C. 1873(a)(1)) is amended—

21 (1) in subparagraph (E), by striking “; and”
 22 and inserting a semicolon;

23 (2) in subparagraph (F), by striking the period
 24 at the end and inserting a semicolon; and

25 (3) by adding at the end the following:

1 “(G) the number of certifications by the
2 Foreign Intelligence Surveillance Court pursu-
3 ant to section 103(j);

4 “(H) the number of petitions to certify a
5 question made by an amicus curiae pursuant to
6 section 103(i)(7)(A);

7 “(I) the number of hearings or rehearings
8 by the Foreign Intelligence Surveillance Court
9 en banc pursuant to section 103(a)(2),
10 disaggregated by hearings or rehearings by
11 such court en banc pursuant to clause (i) or (ii)
12 of such section; and

13 “(J) the number of times amici curiae
14 have been appointed pursuant to section
15 103(i)(2).”.

16 **SEC. 802. ENHANCED ANNUAL REPORTS BY DIRECTOR OF**
17 **NATIONAL INTELLIGENCE.**

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

21 (1) in paragraph (2)(C), by striking the semi-
22 colon and inserting “; and”;

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

1 (3) by inserting after paragraph (2) the fol-
2 lowing:

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

5 “(4) statistics revealing the number of persons
6 and identifiers targeted under section 702(a),
7 disaggregated by certification under which the per-
8 son or identifier was targeted;

9 “(5) the total number of directives issued pur-
10 suant to section 702(i)(1), disaggregated by each
11 type of electronic communication service provider de-
12 scribed in subparagraphs (A) through (E) of section
13 701(b)(4);” and

14 (4) by adding at the end the following:

15 “(11)(A) the total number of disseminated in-
16 telligence reports derived from collection pursuant to
17 section 702 containing the identities of United
18 States persons regardless of whether the identities of
19 the United States persons were openly included or
20 masked;

21 “(B) the total number of disseminated intelligence re-
22 ports derived from collection not authorized by this Act
23 containing the identities of United States persons regard-
24 less of whether the identities of the United States persons
25 were openly included or masked;

1 “(C) the total number of disseminated intelligence re-
2 ports derived from collection pursuant to section 702 con-
3 taining the identities of United States persons in which
4 the identities of the United States persons were masked;

5 “(D) the total number of disseminated intelligence re-
6 ports derived from collection not authorized by this Act
7 containing the identities of United States persons in which
8 the identities of the United States persons were masked;

9 “(E) the total number of disseminated intelligence re-
10 ports derived from collection pursuant to section 702 con-
11 taining the identities of United States persons in which
12 the identities of the United States persons were openly in-
13 cluded; and

14 “(F) the total number of disseminated intelligence re-
15 ports derived from collection not authorized by this Act
16 containing the identities of United States persons in which
17 the identities of the United States persons were openly in-
18 cluded;

19 “(12)(A) the number of queries conducted in an
20 effort to find communications or information of or
21 about 1 or more United States persons or persons
22 reasonably believed to be located in the United
23 States at the time of the query or the time of the
24 communication or creation of the information that
25 required a warrant pursuant to section 302; and

1 “(B) the number of queries conducted in an effort
2 to find communications or information of or about 1 or
3 more United States persons or persons reasonably believed
4 to be located in the United States at the time of the query
5 or the time of the communication or creation of the infor-
6 mation that did not require a warrant pursuant to section
7 302; and

8 “(13) the number of criminal proceedings in
9 which the Federal Government or a government of
10 a State or political subdivision thereof entered into
11 evidence or otherwise used or disclosed in a criminal
12 proceeding any information obtained or derived from
13 an acquisition conducted pursuant to Executive
14 Order 12333 (50 U.S.C. 3001 note; relating to
15 United States intelligence activities), or successor
16 order, outside the authorities provided by this Act.”.

17 (b) REPEAL OF NONAPPLICABILITY TO FEDERAL
18 BUREAU OF INVESTIGATION OF CERTAIN REQUIRE-
19 MENTS.—Subsection (d) of such section is amended—

20 (1) by striking paragraph (2); and

21 (2) by redesignating paragraph (3) as para-
22 graph (2).

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

1 **SEC. 803. ANNUAL REPORTING ON ACCURACY AND COM-**
2 **PLETENESS OF APPLICATIONS.**

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

5 (1) by redesignating subsection (e) as sub-
6 section (f); and

7 (2) by inserting after subsection (d) the fol-
8 lowing:

9 “(e) ANNUAL REPORT BY ATTORNEY GENERAL ON
10 ACCURACY AND COMPLETENESS OF APPLICATIONS.—

11 “(1) REPORT REQUIRED.—In April each year,
12 the Attorney General shall submit to the appropriate
13 committees of Congress and publish on the website
14 of the Department of Justice, subject to a declas-
15 sification review, a report setting forth, with respect
16 to the preceding calendar year, the following:

17 “(A) A summary of all accuracy or com-
18 pleteness reviews of applications for court or-
19 ders submitted to the Foreign Intelligence Sur-
20 veillance Court by the Federal Bureau of Inves-
21 tigation under this Act.

22 “(B) The total number of such applica-
23 tions reviewed for accuracy or completeness.

24 “(C) The total number of material errors
25 or omissions identified during such reviews.

1 “(D) The total number of nonmaterial er-
2 rors or omissions identified during such reviews.

3 “(E) The total number of instances in
4 which facts contained in an application were
5 not supported by documentation that existed in
6 the applicable file being reviewed at the time of
7 the review.

8 “(F) An explanation for any increase or
9 decrease in the number of errors identified
10 under subparagraphs (C) and (D), and in the
11 event of an increase in the number of errors, a
12 description of any action taken by the Depart-
13 ment to improve compliance and accuracy.

14 “(2) INSPECTOR GENERAL RISK ASSESS-
15 MENT.—In addition to conducting audits under sec-
16 tion 401 of the Government Surveillance Reform Act
17 of 2023, the Inspector General of the Department of
18 Justice shall—

19 “(A) periodically assess the reports re-
20 quired by paragraph (1); and

21 “(B) as determined by the Inspector Gen-
22 eral, report any risks identified through such
23 assessments to the appropriate committees of
24 Congress.

1 “(3) DEFINITION OF APPROPRIATE COMMIT-
2 TEES OF CONGRESS.—In this subsection, the term
3 ‘appropriate committees of Congress’ has the mean-
4 ing given that term in section 101.”.

5 **SEC. 804. ALLOWING MORE GRANULAR AGGREGATE RE-**
6 **PORTING BY RECIPIENTS OF FOREIGN INTEL-**
7 **LIGENCE SURVEILLANCE ORDERS.**

8 (a) MODIFICATION OF AGGREGATION BANDING.—
9 Subsection (a) of section 604 of the Foreign Intelligence
10 Surveillance Act of 1978 (50 U.S.C. 1874) is amended—

11 (1) by striking paragraphs (1) through (3) and
12 inserting the following:

13 “(1) A semiannual report that aggregates the
14 number of orders, directives, or national security let-
15 ters with which the person was required to comply
16 into separate categories of—

17 “(A) the number of national security let-
18 ters received, reported—

19 “(i) for the first 1000 national secu-
20 rity letters received, in bands of 200 start-
21 ing with 1–200; and

22 “(ii) for more than 1000 national se-
23 curity letters received, the precise number
24 of national security letters received;

1 “(B) the number of customer selectors tar-
2 geted by national security letters, reported—

3 “(i) for the first 1000 customer selec-
4 tors targeted, in bands of 200 starting
5 with 1–200; and

6 “(ii) for more than 1000 customer se-
7 lectors targeted, the precise number of cus-
8 tomer selectors targeted;

9 “(C) the number of orders or directives re-
10 ceived, combined, under this Act for contents—

11 “(i) reported—

12 “(I) for the first 1000 orders and
13 directives received, in bands of 200
14 starting with 1–200; and

15 “(II) for more than 1000 orders
16 and directives received, the precise
17 number of orders received; and

18 “(ii) disaggregated by whether the
19 order or directive was issued under section
20 105, 402, or 702;

21 “(D) the number of customer selectors tar-
22 geted under orders or directives received, com-
23 bined, under this Act for contents—

24 “(i) reported—

200

1 “(I) for the first 1000 customer
2 selectors targeted, in bands of 200
3 starting with 1–200; and

4 “(II) for more than 1000 cus-
5 tomer selectors targeted, the precise
6 number of customer selectors tar-
7 geted; and

8 “(ii) disaggregated by whether the
9 order or directive was issued under section
10 105, 402, or 702;

11 “(E) the number of orders or directives re-
12 ceived under this Act for noncontents—

13 “(i) reported—

14 “(I) for the first 1000 orders or
15 directives received, in bands of 200
16 starting with 1–200; and

17 “(II) for more than 1000 orders
18 or directives received, the precise
19 number of orders received; and

20 “(ii) disaggregated by whether the
21 order or directive was issued under section
22 105, 402, or 702; and

23 “(F) the number of customer selectors tar-
24 geted under orders or directives under this Act
25 for noncontents—

1 “(i) reported—

2 “(I) for the first 1000 customer
3 selectors targeted, in bands of 200
4 starting with 1–200; and

5 “(II) for more than 1000 cus-
6 tomer selectors targeted, the precise
7 number of customer selectors tar-
8 geted; and

9 “(ii) disaggregated by whether the
10 order or directive was issued under section
11 105, 402, or 702.”; and

12 (2) by redesignating paragraph (4) as para-
13 graph (2).

14 (b) ADDITIONAL DISCLOSURES.—Such section is
15 amended—

16 (1) by redesignating subsections (b) through (d)
17 as subsections (c) through (e), respectively; and

18 (2) by inserting after subsection (a) the fol-
19 lowing:

20 “(b) ADDITIONAL DISCLOSURES.—A person who
21 publicly reports information under subsection (a) may also
22 publicly report, using a semiannual report, information re-
23 lating to the previous 180 days that indicates whether the
24 person was or was not required to comply with an order,
25 directive, or national security letter issued under each of

1 sections 105, 402, and 702 and the provisions listed in
2 section 603(f)(3).”.

3 (c) CONFORMING AMENDMENTS.—Subsection (c) of
4 such section, as redesignated by subsection (b)(1) of this
5 section, is amended—

6 (1) in paragraph (1), by striking “or (2)”;

7 (2) by striking paragraph (2);

8 (3) by redesignating paragraph (3) as para-
9 graph (2); and

10 (4) in paragraph (2), as so redesignated, by
11 striking “(4)” and inserting “(2)”.

12 **SEC. 805. REPORT ON USE OF FOREIGN INTELLIGENCE**
13 **SURVEILLANCE AUTHORITIES REGARDING**
14 **PROTECTED ACTIVITIES AND PROTECTED**
15 **CLASSES.**

16 (a) REPORT.—Not later than 1 year after the date
17 of the enactment of this Act, the Privacy and Civil Lib-
18 erties Oversight Board shall make publicly available and
19 submit to the appropriate committees of Congress a report
20 on the use of activities and protected classes described in
21 subsection (b) in—

22 (1) applications for orders made by the United
23 States Government under the Foreign Intelligence
24 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.);
25 and

1 (2) investigations for which such orders are
2 sought.

3 (b) ACTIVITIES AND PROTECTED CLASSES DE-
4 SCRIBED.—The activities and protected classes described
5 in this subsection are the following:

6 (1) Activities and expression protected by the
7 First Amendment to the Constitution of the United
8 States.

9 (2) Race, ethnicity, national origin, and reli-
10 gious affiliation.

11 (c) FORM.—In addition to the report made publicly
12 available and submitted under subsection (a), the Board
13 may submit to the appropriate committees of Congress a
14 classified annex.

15 **SEC. 806. PUBLICATION OF ESTIMATES REGARDING COM-**
16 **MUNICATIONS COLLECTED UNDER CERTAIN**
17 **PROVISIONS OF FOREIGN INTELLIGENCE**
18 **SURVEILLANCE ACT OF 1978.**

19 Not later than 90 days after the date of the enact-
20 ment of this Act, the Director of National Intelligence
21 shall publish a good faith estimate of—

22 (1) the number of United States persons whose
23 communications are collected under section 702 of
24 the Foreign Intelligence Surveillance Act of 1978
25 (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.

5 SEC. 807. ENHANCED REPORTING OF ASSESSMENTS OF
6 COMPLIANCE WITH EMERGENCY ORDER RE-
7 QUIREMENTS UNDER CERTAIN PROVISIONS
8 OF THE FOREIGN INTELLIGENCE SURVEIL-
9 LANCE ACT OF 1978.

10 (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—

19 (A) in subparagraph (C), by striking “;
20 and” and inserting a semicolon;

(B) in subparagraph (D), by striking “section 301(e).” and inserting “section 304(e); and”; and

24 (C) by adding at the end the following:

1 “(E) the annual assessment conducted
2 pursuant to section 105(e)(6).”.

3 (b) PHYSICAL SEARCHES.—

4 (1) ANNUAL ASSESSMENT.—Section 304(e)(6)
5 of the Foreign Intelligence Surveillance Act of 1978
6 (50 U.S.C. 1824(e)(6)) is amended by striking
7 “shall assess compliance” and inserting “shall not
8 less frequently than annually assess compliance”.

9 (2) REPORTING.—Section 306 of the Foreign
10 Intelligence Surveillance Act of 1978 (50 U.S.C.
11 1826) is amended—

12 (A) in paragraph (3), by striking “; and”
13 and inserting a semicolon;

14 (B) in paragraph (4), by striking the pe-
15 riod and inserting “; and”; and

16 (C) by adding at the end the following:

17 “(5) the annual assessment conducted pursuant
18 to section 304(e)(6).”.

19 **TITLE IX—SEVERABILITY AND**
20 **LIMITED DELAYS IN IMPLE-**
21 **MENTATION**

22 **SEC. 901. SEVERABILITY.**

23 If any provision of this Act, an amendment made by
24 this Act, or the application of such a provision or amend-
25 ment 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.