

119TH CONGRESS  
2D SESSION

# H. R. 7901

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

---

## IN THE HOUSE OF REPRESENTATIVES

MARCH 12, 2026

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

---

## 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 2026”.

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

Sec. 1. Short title; table of contents.

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. Protections related to 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. Prohibition on reverse targeting of United States persons and persons located in the United States.
- Sec. 104. Data retention limits for information collected under section 702 of the Foreign Intelligence Surveillance Act of 1978.
- Sec. 105. 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. 106. Prohibition on warrantless acquisition of domestic communications pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978.
- Sec. 107. Requirement of primary foreign intelligence purpose.
- Sec. 108. Reports to Congress on sensitive queries.
- Sec. 109. Repeal of expanded definition of electronic communication service provider.
- Sec. 110. Repeal of expanded querying requirements for persons traveling to the United States.
- Sec. 111. Four-year extension of section 702 of the Foreign Intelligence Surveillance Act of 1978.

**TITLE II—FOURTH AMENDMENT IS NOT FOR SALE ACT**

- Sec. 201. Prohibition on Federal law enforcement purchase of personal data from data brokers.

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

- Sec. 301. Court supervision of collection targeting United States persons and persons located inside the United States.
- Sec. 302. Consistent disclosures of relevant information in title V and other FISA applications.
- Sec. 303. Strengthening accuracy procedures.
- Sec. 304. Clarification regarding treatment of information and evidence acquired under the Foreign Intelligence Surveillance Act of 1978.
- Sec. 305. Sunset on grandfather clause of section 215 of the USA PATRIOT Act.
- Sec. 306. Written record of Department of Justice interactions with Foreign Intelligence Surveillance court.
- Sec. 307. Appointment of amici curiae and access to information.
- Sec. 308. Declassification of significant decisions, orders, and opinions.

- Sec. 309. Clarification of Foreign Intelligence Surveillance Court jurisdiction over records of the court and other ancillary matters.
- Sec. 310. 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. 311. Accountability procedures for violations by Federal employees.
- Sec. 312. Reforms to the exclusive means limitations under the Foreign Intelligence Surveillance Act of 1978.

#### TITLE IV—REFORMS RELATED TO SURVEILLANCE CONDUCTED FOR FOREIGN INTELLIGENCE PURPOSES OTHER THAN UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

- Sec. 401. Definitions.
- Sec. 402. Protections related to warrantless queries for the communications of United States persons and persons located in the United States.
- Sec. 403. Prohibition on reverse targeting of United States persons and persons located in the United States.
- Sec. 404. Prohibition on intelligence acquisition of United States person data.
- Sec. 405. Prohibition on the warrantless acquisition of domestic communications.
- Sec. 406. Data retention limits.
- Sec. 407. Reports on violations of law or Executive order.

#### TITLE V—INDEPENDENT OVERSIGHT

- Sec. 501. Inspector General oversight of orders under the Foreign Intelligence Surveillance Act of 1978.
- Sec. 502. Intelligence community parity and communications with Privacy and Civil Liberties Oversight Board.
- Sec. 503. Congressional oversight of grants of immunity by the Attorney General for warrantless surveillance assistance.

#### TITLE VI—REFORMS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

- Sec. 601. Warrant protections for location information, web browsing records, and search query records.
- Sec. 602. Consistent protections for phone and app-based call and texting records.
- Sec. 603. Email Privacy Act.
- Sec. 604. Consistent protections for demands for data held by interactive computing services.
- Sec. 605. Consistent protections from Federal law enforcement for real-time and historical metadata.
- Sec. 606. Subpoenas for certain subscriber information.
- Sec. 607. Minimization standards for voluntary disclosure of customer communications or records.
- Sec. 608. Consistent privacy protections for data held by data brokers.
- Sec. 609. Protection of data entrusted to intermediary or ancillary service providers.
- Sec. 610. Modernizing criminal surveillance reports.
- Sec. 611. Limitation of amendments to Federal departments and agencies.

#### TITLE VII—PROTECTION OF CAR DATA FROM FEDERAL WARRANTLESS SEARCHES

Sec. 701. Protection of car data from Federal 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 the 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. Rule of construction with respect to State and local law enforcement authorities.

Sec. 902. Severability.

Sec. 903. Limited delays in implementation.

### 1 **SEC. 2. DEFINITIONS.**

#### 2 (a) AMENDMENTS TO THE FOREIGN INTELLIGENCE 3 SURVEILLANCE 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) TITLE VII.—Section 701(b) of such title (50  
9 U.S.C. 1881) is amended by adding at the end the  
10 following new paragraph:

11 “(6) COVERED PERSON.—The term ‘covered  
12 person’ means, with respect to a query, a commu-  
13 nication, an acquisition, or creation of information,  
14 a person who is—

15 “(A) a United States person; or

16 “(B) a person known or believed to be lo-  
17 cated in the United States—

18 “(i) at the time of the applicable  
19 query; or

20 “(ii) at the time of the acquisition,  
21 communication, or creation of the informa-  
22 tion subject to the applicable query.”.

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

1 (A) in section 102(a)(3) (50 U.S.C.  
2 1802(a)(3)), by striking “the court established  
3 under section 103(a)” and inserting “the For-  
4 eign Intelligence Surveillance Court”;

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

6 (i) in subsection (a)—

7 (I) in paragraph (2)(A), by strik-  
8 ing “The court established under this  
9 subsection” and inserting “The For-  
10 eign Intelligence Surveillance Court”;  
11 and

12 (II) by striking “the court estab-  
13 lished under this subsection” each  
14 place it appears and inserting “the  
15 Foreign Intelligence Surveillance  
16 Court”;

17 (ii) in subsection (g)—

18 (I) in paragraph (2)—

19 (aa) in subparagraph (A),  
20 by striking “the court established  
21 pursuant to subsection (a)” and  
22 inserting “the Foreign Intel-  
23 ligence Surveillance Court”; and

24 (bb) in subparagraph (B),  
25 by striking “the court of review

1                   established pursuant to sub-  
2                   section (b)” and inserting “the  
3                   Foreign Intelligence Surveillance  
4                   Court of Review”; and  
5                   (II) in paragraph (1), by striking  
6                   “The courts established pursuant to  
7                   subsections (a) and (b)” and inserting  
8                   “The Foreign Intelligence Surveillance  
9                   Court and the Foreign Intelligence  
10                  Surveillance Court of Review”;  
11                  (iii) in subsection (h), by striking “a  
12                  court established under this section” and  
13                  inserting “the Foreign Intelligence Surveil-  
14                  lance Court or the Foreign Intelligence  
15                  Surveillance Court of Review”;  
16                  (iv) in subsection (i)—  
17                  (I) in paragraph (1), by striking  
18                  “the courts established under sub-  
19                  sections (a) and (b)” and inserting  
20                  “the Foreign Intelligence Surveillance  
21                  Court and the Foreign Intelligence  
22                  Surveillance Court of Review”;  
23                  (II) in paragraph (3)(B), in the  
24                  first sentence, by striking “the  
25                  courts” and inserting “the Foreign

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

4 (III) in paragraph (5), by strik-  
5 ing “the court” and inserting “the  
6 Foreign Intelligence Surveillance  
7 Court or the Foreign Intelligence Sur-  
8 veillance Court of Review, as the case  
9 may be,”;

10 (IV) in paragraph (6), by strik-  
11 ing “the court” each place it appears  
12 and inserting “the Foreign Intel-  
13 ligence Surveillance Court or the For-  
14 eign Intelligence Surveillance Court of  
15 Review”;

16 (V) by striking “a court estab-  
17 lished under subsection (a) or (b)”  
18 each place it appears and inserting  
19 “the Foreign Intelligence Surveillance  
20 Court or the Foreign Intelligence Sur-  
21 veillance Court of Review”; and

22 (VI) by striking “A court estab-  
23 lished under subsection (a) or (b)”  
24 each place it appears and inserting  
25 “The Foreign Intelligence Surveillance



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

3 (v) in subsection (j)—

4 (I) by striking “a court estab-  
5 lished under subsection (a)” and in-  
6 serting “the Foreign Intelligence Sur-  
7 veillance Court”; and

8 (II) by striking “the court deter-  
9 mines” and inserting “the Foreign In-  
10 telligence Surveillance Court deter-  
11 mines”;

12 (vi) by striking “the court established  
13 under subsection (a)” each place it appears  
14 and inserting “the Foreign Intelligence  
15 Surveillance Court”; and

16 (vii) by striking “the court established  
17 under subsection (b)” each place it appears  
18 and inserting “the Foreign Intelligence  
19 Surveillance Court of Review”;

20 (C) in section 105(c)(3) (50 U.S.C.  
21 1805(c)(3)), by striking “the court” each place  
22 it appears and inserting “the Foreign Intel-  
23 ligence Surveillance Court”;

24 (D) in section 401(1) (50 U.S.C. 1841(1)),  
25 by striking “, and ‘State’” and inserting

1 “‘State’, ‘Foreign Intelligence Surveillance  
2 Court’, and ‘Foreign Intelligence Surveillance  
3 Court of Review’ ”;

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

5 (i) in subsection (b)(1), by striking  
6 “the court established by section 103(a) of  
7 this Act” and inserting “the Foreign Intel-  
8 ligence Surveillance Court”; and

9 (ii) in subsection (h)(2), by striking  
10 “the court established under section  
11 103(a)” and inserting “the Foreign Intel-  
12 ligence Surveillance Court”;

13 (F) in section 502(b)(1)(A), by striking  
14 “the court established by section 103(a) of this  
15 Act” and inserting “the Foreign Intelligence  
16 Surveillance Court (as defined by section 101)”;

17 (G) in section 801 (50 U.S.C. 1885)—

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

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

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

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

3 (H) 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—

8 (1) the terms “appropriate committees of Con-  
9 gress”, “Foreign Intelligence Surveillance Court”,  
10 and “Foreign Intelligence Surveillance Court of Re-  
11 view” have the meanings given such terms in section  
12 101 of the Foreign Intelligence Surveillance Act of  
13 1978 (50 U.S.C. 1801), as amended by subsection  
14 (a)(1); and

15 (2) the term “covered person” has the meaning  
16 given such term in section 701 of such Act (50  
17 U.S.C. 1881), as amended by subsection (a)(2).

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. PROTECTIONS RELATED TO WARRANTLESS QUE-**  
9 **RIES FOR THE COMMUNICATIONS OF UNITED**  
10 **STATES PERSONS AND PERSONS LOCATED IN**  
11 **THE UNITED STATES.**

12 (a) IN GENERAL.—Section 702(f) of the Foreign In-  
13 telligence Surveillance Act of 1978 (50 U.S.C. 1881a(f))  
14 is amended—

15 (1) in paragraph (1)(A), by inserting “and the  
16 limitations and requirements in this subsection”  
17 after “Constitution of the United States”;

18 (2) in paragraph (5)—

19 (A) in subparagraph (B), by striking  
20 “means” and all that follows through the period  
21 and inserting the following: “means the use of  
22 1 or more terms, whether conducted through  
23 manual or automated means, to retrieve any in-  
24 formation acquired under this section, including  
25 retrieval from a subset of such information,

1 whether that subset was created by retrieval  
2 through a query or other means.”;

3 (B) by redesignating subparagraph (B) as  
4 subparagraph (D); and

5 (C) by inserting after subparagraph (A)  
6 the following:

7 “(B) The term ‘covered information’  
8 means—

9 “(i) communications content; and

10 “(ii) information, the compelled dis-  
11 closure of which would require a probable  
12 cause warrant if sought for law enforce-  
13 ment purposes inside the United States.

14 “(C) The term ‘covered query’ means a  
15 query that is conducted—

16 “(i) using a term associated with 1 or  
17 more covered persons; or

18 “(ii) for a significant purpose of re-  
19 trieval information of or concerning 1 or  
20 more covered persons.”; and

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

22 “(7) PROHIBITION ON WARRANTLESS QUERIES  
23 FOR THE COMMUNICATIONS AND OTHER INFORMA-  
24 TION OF UNITED STATES PERSONS AND PERSONS  
25 LOCATED IN THE UNITED STATES.—

1           “(A) IN GENERAL.—Except as provided in  
2           subparagraphs (B) and (C), no officer or em-  
3           ployee of the Federal Government may access  
4           covered information returned in response to a  
5           covered query.

6           “(B) EXCEPTIONS FOR CONCURRENT AU-  
7           THORIZATION, CONSENT, EMERGENCY SITUA-  
8           TIONS, AND CERTAIN DEFENSIVE CYBERSECU-  
9           RITY QUERIES.—Subparagraph (A) shall not  
10          apply if—

11               “(i) the covered person to whom the  
12               covered query relates is the subject of an  
13               order or emergency authorization author-  
14               izing electronic surveillance or physical  
15               search under section 105 or 304 of this  
16               Act, or a warrant issued pursuant to the  
17               Federal Rules of Criminal Procedure by a  
18               court of competent jurisdiction, if—

19                       “(I) such order, authorization, or  
20                       warrant covers the period of the cov-  
21                       ered query; and

22                       “(II) the covered query is con-  
23                       ducted and covered information is  
24                       accessed in compliance with all use,  
25                       dissemination, querying, retention,

1 and other minimization limitations re-  
2 quired by the order, authorization, or  
3 warrant;

4 “(ii)(I) the officer or employee access-  
5 ing the covered information has a reason-  
6 able belief that—

7 “(aa) an emergency exists involv-  
8 ing an imminent threat of death or se-  
9 rious bodily harm; and

10 “(bb) in order to prevent or miti-  
11 gate the threat described in item (aa),  
12 the covered information must be  
13 accessed before authorization de-  
14 scribed in clause (i) can, with due dili-  
15 gence, be obtained; and

16 “(II) not later than 14 days after the  
17 covered information is accessed, a descrip-  
18 tion of the circumstances justifying the ac-  
19 cessing of the covered information is pro-  
20 vided to the Foreign Intelligence Surveil-  
21 lance Court and the appropriate commit-  
22 tees of Congress;

23 “(iii) the covered person to whom the  
24 covered query relates or, if such person is  
25 incapable of providing consent, a third

1 party legally authorized to consent on be-  
2 half of such person, has provided consent  
3 for the access on a case-by-case basis; or

4 “(iv)(I) the covered information is  
5 accessed and used for defensive cybersecu-  
6 rity purposes, including the protection of a  
7 covered person from cybersecurity attack;

8 “(II) other than for such defensive cy-  
9 bersecurity purposes, no covered informa-  
10 tion is accessed or reviewed; and

11 “(III) not later than 14 days after the  
12 covered information is accessed, a descrip-  
13 tion of the circumstances justifying the ac-  
14 cessing of the covered information is pro-  
15 vided to the Foreign Intelligence Surveil-  
16 lance Court and the appropriate commit-  
17 tees of Congress.

18 “(C) MATTERS RELATING TO EMERGENCY  
19 QUERIES.—

20 “(i) TREATMENT OF DENIALS.—If  
21 covered information is accessed pursuant  
22 to an emergency authorization described in  
23 subparagraph (B)(i) and the subsequent  
24 application to authorize electronic surveil-  
25 lance, a physical search, or an acquisition



1           pursuant to section 105(e) or section  
2           304(e) of this Act is denied, or in any  
3           other case in which covered information is  
4           accessed in violation of this paragraph—

5                   “(I) no covered information  
6                   accessed, or information or evidence  
7                   derived from such access may be used,  
8                   received in evidence, or otherwise dis-  
9                   seminated in any investigation, trial,  
10                  hearing, or other proceeding in or be-  
11                  fore any court, grand jury, depart-  
12                  ment, office, agency, regulatory body,  
13                  legislative committee, or other author-  
14                  ity of the United States, a State, or  
15                  political subdivision thereof; and

16                   “(II) no covered information  
17                   accessed may subsequently be used or  
18                   disclosed in any other manner without  
19                   the consent of such person, except if  
20                   the Attorney General personally ap-  
21                   proves the use or disclosure of such  
22                   information in order to prevent the  
23                   death of or serious bodily harm to any  
24                   person and not later than 14 days of  
25                   such approval, a description of the cir-

1           cumstances justifying the approval is  
2           provided to the Foreign Intelligence  
3           Surveillance Court and the appro-  
4           priate committees of Congress.

5           “(ii) ASSESSMENT OF COMPLIANCE.—

6           Not less frequently than once each year,  
7           the Attorney General shall assess compli-  
8           ance with the requirements under clause  
9           (i).

10          “(D) FOREIGN INTELLIGENCE PURPOSE  
11          REQUIRED FOR QUERIES.—

12          “(i) IN GENERAL.—Except as pro-  
13          vided in clause (ii), no officer or employee  
14          of the Federal Government may conduct a  
15          query unless the query is—

16                  “(I) reasonably likely to retrieve  
17                  foreign intelligence information; and

18                  “(II) is made with a significant  
19                  foreign intelligence purpose.

20          “(ii) EXCEPTIONS.—An officer or em-  
21          ployee of the Federal Government is per-  
22          mitted to conduct a query if an exception  
23          described in clauses (i) and (ii) of para-  
24          graph (2)(B) applies.

1           “(E) DOCUMENTATION.—No officer or em-  
2           ployee of the Federal Government may conduct  
3           a query, or access covered information returned  
4           in response to a covered query, unless an elec-  
5           tronic record is created that includes—

6                   “(i) for each query—

7                           “(I) each term used for the con-  
8                           duct of the query;

9                           “(II) the date of the query;

10                          “(III) the identifier of the officer  
11                          or employee who conducted the query;  
12                          and

13                          “(IV) a statement of facts justi-  
14                          fying that the query is reasonably  
15                          likely to retrieve foreign intelligence  
16                          information and the significant for-  
17                          eign intelligence purpose for the query  
18                          or, if an exception under subpara-  
19                          graph (D)(ii) applies, a description of  
20                          the basis for such exception; and

21                          “(ii) for each access—

22                           “(I) the date of the access;

23                           “(II) the identifier of the officer  
24                           or employee who did the particular ac-  
25                           cess; and

1                   “(III) a statement of facts show-  
2                   ing that an access is authorized by an  
3                   exception under subparagraph (B).

4                   “(F) QUERY RECORD SYSTEM.—Each head  
5                   of an agency who is authorized to conduct a  
6                   covered query shall ensure that a system, mech-  
7                   anism, or business practice is in place to main-  
8                   tain the records described in subparagraph (E),  
9                   including ensuring that any queries or accesses  
10                  to covered information returned in response to  
11                  covered queries, that are conducted by auto-  
12                  mated means are attributed to the officer or  
13                  employee who was the proximate cause of such  
14                  query or access.”.

15               (b) REPORT ON COMPLIANCE WITH QUERY RECORD  
16               SYSTEM REQUIREMENT.—Not later than 90 days after  
17               the date of enactment of this Act, each head of a Federal  
18               agency described in section 702(f)(7)(F) of such Act, as  
19               added by subsection (a), shall submit to the appropriate  
20               committees of Congress a report on the compliance of the  
21               Federal agency with the requirement of such section.

22               (c) CONFORMING AMENDMENTS.—Section 702(f) of  
23               such Act, as amended by subsection (a), is further amend-  
24               ed—

1 (1) in the headings for subparagraph (B) of  
 2 paragraph (1), subparagraph (A) of paragraph (2),  
 3 and subparagraph (A) of paragraph (3), by striking  
 4 “UNITED STATES PERSON” each place it appears  
 5 and inserting “COVERED PERSON”;

6 (2) in paragraph (6)—

7 (A) in the heading, by striking “NON-  
 8 UNITED STATES PERSONS” and inserting “NON-  
 9 COVERED PERSONS”; and

10 (B) by striking “non-United States per-  
 11 sons” and inserting “noncovered persons”; and

12 (3) in paragraphs (1) through (6), by striking  
 13 “United States person” each place it appears and  
 14 inserting “covered person”.

15 **SEC. 102. LIMITATION ON USE OF INFORMATION OBTAINED**  
 16 **UNDER SECTION 702 OF THE FOREIGN INTEL-**  
 17 **LIGENCE SURVEILLANCE ACT OF 1978 RELAT-**  
 18 **ING TO UNITED STATES PERSONS AND PER-**  
 19 **SONS LOCATED IN THE UNITED STATES IN**  
 20 **CRIMINAL, CIVIL, AND ADMINISTRATIVE AC-**  
 21 **TIONS.**

22 Paragraph (2) of section 706(a) of the Foreign Intel-  
 23 ligence Surveillance Act of 1978 (50 U.S.C. 1881e(a)) is  
 24 amended—

1 (1) in the paragraph heading, by striking  
2 “UNITED STATES PERSONS” and inserting “COV-  
3 ERED PERSONS”; and

4 (2) in subparagraph (A)—

5 (A) by striking “United States person”  
6 both places it appears and inserting “covered  
7 person”;

8 (B) in the matter before clause (i), by  
9 striking “in any criminal proceeding” and in-  
10 serting “in any criminal, civil, or administrative  
11 proceeding”; and

12 (C) in clause (ii), by striking “the criminal  
13 proceeding” both places it appears and insert-  
14 ing “the proceeding”.

15 **SEC. 103. PROHIBITION ON REVERSE TARGETING OF**  
16 **UNITED STATES PERSONS AND PERSONS LO-**  
17 **CATED IN THE UNITED STATES.**

18 Section 702 of the Foreign Intelligence Surveillance  
19 Act of 1978 (50 U.S.C. 1881a), as amended by section  
20 101, is further amended—

21 (1) in subsection (b)—

22 (A) by redesignating paragraph (6) as  
23 paragraph (7); and

24 (B) by inserting after paragraph (5) the  
25 following:

1           “(6) may not intentionally target a person rea-  
2           sonably believed to be located outside the United  
3           States if a significant purpose of such acquisition is  
4           to acquire the information of one or more particular,  
5           known covered persons, unless—

6                   “(A)(i) there is a reasonable belief that an  
7                   emergency exists involving an imminent threat  
8                   of death or serious bodily harm to such covered  
9                   persons;

10                   “(ii) the information is sought for the pur-  
11                   pose of assisting that covered persons; and

12                   “(iii) not later than 14 days after the tar-  
13                   geting, a description of the targeting is pro-  
14                   vided to the Foreign Intelligence Surveillance  
15                   Court and the appropriate committees of Con-  
16                   gress; or

17                   “(B) the covered persons have provided  
18                   consent to the targeting, or if such persons are  
19                   incapable of providing consent, a third party le-  
20                   gally authorized to consent on behalf of such  
21                   covered person has provided consent;”;

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

24                   “(A) ensure that—

1 “(i) any acquisition authorized under  
2 subsection (a) is limited to targeting per-  
3 sons reasonably believed to be non-United  
4 States persons located outside the United  
5 States; and

6 “(ii) except as provided in subsection  
7 (b)(6), it is not a significant purpose of an  
8 acquisition to acquire the information of  
9 one or more particular, known covered per-  
10 sons; and”;

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

13 “(I) ensure that—

14 “(aa) an acquisition author-  
15 ized under subsection (a) is lim-  
16 ited to targeting persons reason-  
17 ably believed to be non-United  
18 States persons located outside  
19 the United States; and

20 “(bb) except as provided in  
21 subsection (b)(6), it is not a sig-  
22 nificant purpose of an acquisition  
23 to acquire the information of one  
24 or more particular, known cov-  
25 ered persons; and”;



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

3 “(i) ensure that—

4 “(I) an acquisition authorized  
 5 under subsection (a) is limited to tar-  
 6 geting persons reasonably believed to  
 7 be non-United States persons located  
 8 outside the United States; and

9 “(II) except as provided in sub-  
 10 section (b)(6), it is not a significant  
 11 purpose of an acquisition to acquire  
 12 the information of one or more par-  
 13 ticular, known covered persons; and”.

14 **SEC. 104. DATA RETENTION LIMITS FOR INFORMATION**  
 15 **COLLECTED UNDER SECTION 702 OF THE**  
 16 **FOREIGN INTELLIGENCE SURVEILLANCE ACT**  
 17 **OF 1978.**

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

21 **“SEC. 710. DATA RETENTION LIMITS.**

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

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

3               “(1) any information or communication per-  
4 taining to a covered person, including an encrypted  
5 communication to or from a covered person, that has  
6 been evaluated and is not specifically known to con-  
7 tain foreign intelligence information; and

8               “(2) any unevaluated information, unless it can  
9 reasonably be determined that the unevaluated infor-  
10 mation does not contain—

11                       “(A) any information pertaining to a cov-  
12 ered person; or

13                       “(B) any communication to or from a cov-  
14 ered person, regardless of whether such commu-  
15 nication is encrypted.

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

22               “(1) the information is the subject of a preser-  
23 vation obligation in pending administrative, civil, or  
24 criminal litigation, in which case the information  
25 shall be segregated, retained, and used solely for

1 that purpose and shall be destroyed as soon as it is  
 2 no longer required to be preserved for such litigation;  
 3 or

4 “(2) the information is being used in a proceeding or investigation consistent with section  
 5 706(a).”.

7 (b) CLERICAL AMENDMENT.—The table of contents  
 8 for such Act is amended by inserting after the item relating to section 709 the following:

“Sec. 710. Data retention limits.”.

10 **SEC. 105. FOREIGN INTELLIGENCE SURVEILLANCE COURT**  
 11 **SUPERVISION OF DEMANDS FOR TECHNICAL**  
 12 **ASSISTANCE FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE**  
 13 **SURVEILLANCE ACT OF 1978.**

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

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

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

24 “(A) IN GENERAL.—Subject to subparagraph (B), in carrying out”; and  
 25

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

2 “(B) LIMITATIONS.—Neither the Attorney  
3 General nor the Director of National Intel-  
4 ligence may direct technical assistance from an  
5 electronic communication service provider under  
6 subparagraph (A) without demonstrating that  
7 the assistance sought—

8 “(i) is necessary;

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

11 “(iii) would not pose an undue burden  
12 on the electronic communication service  
13 provider or its customers who are not in-  
14 tended targets of the surveillance.

15 “(C) COMPLIANCE.—An electronic commu-  
16 nication service provider is not obligated to  
17 comply with a directive to provide technical as-  
18 sistance under this paragraph unless—

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

22 “(ii) the Court issues an order, which  
23 has been delivered to the provider, explic-  
24 itly describing the assistance to be fur-

1           nished by the provider that has been ap-  
2           proved by the Court.”.

3 **SEC. 106. PROHIBITION ON WARRANTLESS ACQUISITION OF**  
4 **DOMESTIC COMMUNICATIONS PURSUANT TO**  
5 **SECTION 702 OF THE FOREIGN INTEL-**  
6 **LIGENCE SURVEILLANCE ACT OF 1978.**

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

9           (1) in subsection (b)(4), by striking “known at  
10       the time of the acquisition” and inserting “known or  
11       believed at the time of acquisition or communica-  
12       tion”;

13          (2) in subsection (d)(1)(B), by striking “known  
14       at the time of the acquisition” and inserting “known  
15       or believed at the time of acquisition or communica-  
16       tion”;

17          (3) in subsection (h)(2)(A)(i)(II), by striking  
18       “known at the time of the acquisition” and inserting  
19       “known or believed at the time of acquisition or  
20       communication”; and

21          (4) in subsection (j)(2)(B)(ii), by striking  
22       “known at the time of the acquisition” and inserting  
23       “known or believed at the time of acquisition or  
24       communication”.

1 **SEC. 107. REQUIREMENT OF PRIMARY FOREIGN INTEL-**  
 2 **LIGENCE PURPOSE.**

3 Section 702(h)(2)(A)(v) of the Foreign Intelligence  
 4 Surveillance Act of 1978 (50 U.S.C. 1881a(h)(2)(A)(v))  
 5 is amended by striking “a significant” and inserting “the  
 6 primary”.

7 **SEC. 108. REPORTS TO CONGRESS ON SENSITIVE QUERIES.**

8 Section 702(f)(3)(D) of the Foreign Intelligence Sur-  
 9 veillance Act of 1978 (50 U.S.C. 1881a(f)(3)(D)) is  
 10 amended by adding at the end the following:

11 “(vii) REPORTS TO CONGRESS.—Not  
 12 less frequently than once each year, the  
 13 Attorney General shall submit to the ap-  
 14 propriate committees of Congress an an-  
 15 nual report on the number of sensitive que-  
 16 ries made in the year covered by the re-  
 17 port, disaggregated by the subclause of  
 18 clause (ii) under which the queries were  
 19 approved.”.

20 **SEC. 109. REPEAL OF EXPANDED DEFINITION OF ELEC-**  
 21 **TRONIC COMMUNICATION SERVICE PRO-**  
 22 **VIDER.**

23 (a) DEFINITION WITH RESPECT TO ADDITIONAL  
 24 PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE  
 25 THE UNITED STATES.—Section 701(b)(4) of the Foreign

1 Intelligence Surveillance Act of 1978 (50 U.S.C.  
2 1881(b)(4)) is amended—

3 (1) in subparagraph (F)—

4 (A) by striking “custodian,”; and

5 (B) by striking “(D), or (E)” and insert-  
6 ing “or (D)”;

7 (2) by striking subparagraph (E);

8 (3) in subparagraph (D), by striking the semi-  
9 colon and inserting “; or”; and

10 (4) by redesignating subparagraph (F) as sub-  
11 paragraph (E).

12 (b) DEFINITION WITH RESPECT TO PROTECTION OF  
13 PERSONS ASSISTING THE GOVERNMENT.—Section 801(6)  
14 of such Act (50 U.S.C. 1885(6)) is amended—

15 (1) in subparagraph (G)—

16 (A) by striking “custodian,”; and

17 (B) by striking “(E), or (F)” and inserting  
18 “or (E)”;

19 (2) by striking subparagraph (E);

20 (3) in subparagraph (F), by striking the semi-  
21 colon and inserting “; or”; and

22 (4) by redesignating subparagraphs (F) and  
23 (G) as subparagraphs (E) and (F), respectively.

24 (c) TREATMENT OF CERTAIN SECTION 702 DIREC-  
25 TIVES.—Any directive issued pursuant to section 702(i)

1 of such Act (50 U.S.C. 1881a(i)) to a person who was  
 2 considered an electronic communication service provider  
 3 pursuant to section 701(b)(4) of such Act (50 U.S.C.  
 4 1881(b)(4)) as such section was in effect during the period  
 5 beginning on April 20, 2024, and ending on the date of  
 6 the enactment of this Act, but is not an electronic commu-  
 7 nication service provider pursuant to such section as in  
 8 effect after the date of the enactment of this Act, shall  
 9 be considered null and void.

10 **SEC. 110. REPEAL OF EXPANDED QUERYING REQUIRE-**  
 11 **MENTS FOR PERSONS TRAVELING TO THE**  
 12 **UNITED STATES.**

13 Section 702(f) of the Foreign Intelligence Surveil-  
 14 lance Act of 1978 (50 U.S.C. 1881a(f)), as amended by  
 15 section 101, is further amended—

16 (1) by striking paragraph (6); and

17 (2) by redesignating paragraph (7), as added by  
 18 section 101, as paragraph (6).

19 **SEC. 111. FOUR-YEAR EXTENSION OF SECTION 702 OF THE**  
 20 **FOREIGN INTELLIGENCE SURVEILLANCE ACT**  
 21 **OF 1978.**

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



1 (1) in paragraph (1) (50 U.S.C. 1881–1881g  
2 note)—

3 (A) by striking “effective two years after  
4 the date of enactment of the Reforming Intel-  
5 ligence and Securing America Act” and insert-  
6 ing “effective April 20, 2030”; and

7 (B) by striking “and the Reforming Intel-  
8 ligence and Securing America Act” and insert-  
9 ing “, the Reforming Intelligence and Securing  
10 America Act, and the Government Surveillance  
11 Reform Act of 2026”; and

12 (2) in paragraph (2) (18 U.S.C. 2511 note), in  
13 the matter preceding subparagraph (A), by striking  
14 “two years after the date of enactment of the Re-  
15 forming Intelligence and Securing America Act” and  
16 inserting “April 20, 2030”.

17 (b) CONFORMING AMENDMENTS.—Section 404(b) of  
18 the FISA Amendments Act of 2008 (Public Law 110–261;  
19 50 U.S.C. 1801 note) is amended—

20 (1) in paragraph (1)—

21 (A) in the paragraph heading, by striking  
22 “TWO YEARS AFTER THE DATE OF ENACTMENT  
23 OF THE REFORMING INTELLIGENCE AND SE-  
24 CURING AMERICA ACT” and inserting “APRIL  
25 20, 2030”; and

1 (B) by striking “and the Reforming Intel-  
 2 ligence and Securing America Act” and insert-  
 3 ing “, the Reforming Intelligence and Securing  
 4 America Act, and the Government Surveillance  
 5 Reform Act of 2026”; and

6 (2) in paragraph (2), in the matter before sub-  
 7 paragraph (A), by striking “and the Reforming In-  
 8 telligence and Securing America Act” and inserting  
 9 “, the Reforming Intelligence and Securing America  
 10 Act, and the Government Surveillance Reform Act of  
 11 2026”.

## 12 **TITLE II—FOURTH AMENDMENT** 13 **IS NOT FOR SALE ACT**

### 14 **SEC. 201. PROHIBITION ON FEDERAL LAW ENFORCEMENT** 15 **PURCHASE OF PERSONAL DATA FROM DATA** 16 **BROKERS.**

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

19 “(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR  
 20 ANYTHING OF VALUE PERSONAL DATA BY FEDERAL LAW  
 21 ENFORCEMENT AGENCIES.—

22 “(1) DEFINITIONS.—In this subsection and  
 23 subsections (f) and (g)—

24 “(A) the term ‘biometric information’—

1 “(i) means any covered personal data  
2 that allows or confirms the unique identi-  
3 fication or verification of an individual and  
4 is generated from the measurement or  
5 processing of unique biological, physical, or  
6 physiological characteristics, including—

7 “(I) fingerprints;

8 “(II) voice prints;

9 “(III) iris or retina imagery  
10 scans;

11 “(IV) facial or hand mapping,  
12 geometry, or templates; and

13 “(V) gait; and

14 “(ii) does not include—

15 “(I) a digital or physical photo-  
16 graph;

17 “(II) an audio or video recording;

18 or

19 “(III) data derived from a digital  
20 or physical photograph or an audio or  
21 video recording that cannot be used to  
22 identify or authenticate a specific in-  
23 dividual;

24 “(B) the term ‘covered organization’  
25 means a person who—

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

2 “(ii) is not an individual, unless such  
3 individual is an agent of, or otherwise act-  
4 ing on behalf of, a person who is not a  
5 governmental entity and is not an indi-  
6 vidual;

7 “(C) the term ‘covered person’ means an  
8 individual who—

9 “(i) is reasonably believed to be lo-  
10 cated inside the United States at the time  
11 of the creation of the covered personal  
12 data; or

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

17 “(D) the term ‘covered personal data’  
18 means personal data relating to a covered per-  
19 son;

20 “(E) the term ‘electronic device’ has the  
21 meaning given the term ‘computer’ in section  
22 1030(e);

23 “(F) the term ‘Federal law enforcement  
24 agency’ means a law enforcement agency of a  
25 department or agency of the United States;

1           “(G) the term ‘lawfully obtained public  
2 data’ means covered personal data obtained by  
3 a particular covered organization—

4           “(i) that the covered organization rea-  
5 sonably understood to have been volun-  
6 tarily made available to the general public  
7 by the covered person;

8           “(ii) that the covered organization ob-  
9 tained in compliance with all applicable  
10 laws and regulations; and

11           “(iii) if the covered organization did  
12 not initially obtain the covered personal  
13 data after the covered personal data was  
14 made available to the general public—

15           “(I) that the covered organiza-  
16 tion reasonably understood to have  
17 been obtained in compliance with all  
18 applicable laws and regulations by—

19           “(aa) the person that ini-  
20 tially obtained the covered per-  
21 sonal data; and

22           “(bb) if the covered organi-  
23 zation did not obtain the covered  
24 personal data from the person  
25 described in item (aa), each other

1 person in the sequence of trans-  
2 fers of the covered personal data  
3 leading up to the obtaining of the  
4 covered personal data by the cov-  
5 ered organization; and

6 “(II) with respect to which the  
7 covered organization receives an attes-  
8 tation under penalty of perjury—

9 “(aa) by the person that ini-  
10 tially obtained the covered per-  
11 sonal data indicating that the  
12 covered personal data was volun-  
13 tarily made available to the gen-  
14 eral public by the covered person  
15 and was obtained in compliance  
16 with all applicable laws and regu-  
17 lations; and

18 “(bb) if the covered organi-  
19 zation did not obtain the covered  
20 personal data from the person  
21 described in item (aa), by each  
22 other person in the sequence of  
23 transfers of the covered personal  
24 data leading up to the obtaining  
25 of the covered personal data by

1 the covered organization indi-  
2 cating that such person reason-  
3 ably understood the data to have  
4 been lawfully obtained public  
5 data;

6 “(H) the term ‘obtain in exchange for any-  
7 thing of value’ means to obtain by purchasing,  
8 to receive in connection with services being pro-  
9 vided for monetary or nonmonetary consider-  
10 ation, or to otherwise obtain in exchange for  
11 consideration, including an access fee, service  
12 fee, maintenance fee, or licensing fee;

13 “(I) the term ‘personal data’—

14 “(i) means data, derived data, or any  
15 unique identifier that is linked to, or is  
16 reasonably linkable to, an individual or to  
17 an electronic device that is linked to, or is  
18 reasonably linkable to, 1 or more individ-  
19 uals in a household;

20 “(ii) includes anonymized data that, if  
21 combined with other data, can be linked to,  
22 or is reasonably linkable to, an individual  
23 or to an electronic device that identifies, is  
24 linked to, or is reasonably linkable to 1 or  
25 more individuals in a household; and

1 “(iii) does not include data that is  
2 lawfully available through Federal, State,  
3 or local government records or through  
4 widely distributed media; and

5 “(J) the term ‘State or local law enforce-  
6 ment agency’ means a law enforcement depart-  
7 ment or agency of a State, or a political sub-  
8 division of a State.

9 “(2) LIMITATION.—

10 “(A) IN GENERAL.—

11 “(i) PROHIBITION.—Subject to  
12 clauses (ii) through (vii), a Federal law en-  
13 forcement agency may not obtain in ex-  
14 change for anything of value covered per-  
15 sonal data if—

16 “(I) the covered personal data is  
17 directly or indirectly obtained from a  
18 covered organization; or

19 “(II) the covered personal data is  
20 derived from covered personal data  
21 that was directly or indirectly ob-  
22 tained from a covered organization.

23 “(ii) EXCEPTION FOR CERTAIN COM-  
24 PILATIONS OF DATA.—A Federal law en-  
25 forcement agency may obtain in exchange



1           for something of value covered personal  
2           data as part of a larger compilation of  
3           data which includes personal data about  
4           persons who are not covered persons, if—

5                   “(I) the Federal law enforcement  
6                   agency is unable through reasonable  
7                   means to exclude covered personal  
8                   data from the larger compilation ob-  
9                   tained; and

10                   “(II) the Federal law enforce-  
11                   ment agency minimizes any covered  
12                   personal data from the larger compila-  
13                   tion, in accordance with the require-  
14                   ments described in, and the proce-  
15                   dures established under, subsection  
16                   (f).

17                   “(iii) EXCEPTION FOR WHISTLE-  
18                   BLOWER DISCLOSURES TO LAW ENFORCE-  
19                   MENT.—Clause (i) shall not apply to cov-  
20                   ered personal data that is obtained by a  
21                   Federal law enforcement agency under a  
22                   program established by an Act of Congress  
23                   under which a portion of a penalty or a  
24                   similar payment or bounty is paid to an in-  
25                   dividual who discloses information about

1 an unlawful activity to the Government,  
2 such as the program authorized under sec-  
3 tion 7623 of the Internal Revenue Code of  
4 1986 (relating to awards to whistleblowers  
5 in cases of underpayments or fraud).

6 “(iv) EXCEPTION FOR COST REIM-  
7 BURSEMENT UNDER COMPULSORY LEGAL  
8 PROCESS.—Clause (i) shall not apply to  
9 covered personal data that is obtained by  
10 a Federal law enforcement agency from a  
11 covered organization in accordance with  
12 compulsory legal process that—

13 “(I) is established by statute; and

14 “(II) provides for the reimburse-  
15 ment of costs of the covered organiza-  
16 tion that are incurred in connection  
17 with providing the record or informa-  
18 tion to the Federal law enforcement  
19 agency, such as the reimbursement of  
20 costs under section 2706.

21 “(v) EXCEPTION FOR EMPLOYMENT-  
22 RELATED USE.—Clause (i) shall not apply  
23 to covered personal data about an em-  
24 ployee of, or applicant for employment by,

1 a Federal law enforcement agency that  
2 is—

3 “(I) obtained by the Federal law  
4 enforcement agency for lawful employ-  
5 ment-related purposes;

6 “(II) accessed and used by the  
7 Federal law enforcement agency only  
8 for such employment-related purposes;  
9 and

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

14 “(vi) EXCEPTION FOR USE IN BACK-  
15 GROUND CHECKS.—Clause (i) shall not  
16 apply to covered personal data about a cov-  
17 ered person that is—

18 “(I) obtained by a Federal law  
19 enforcement agency for purposes of  
20 conducting a background check of the  
21 covered person with the written con-  
22 sent of the covered person;

23 “(II) accessed and used by the  
24 Federal law enforcement agency only

1 for background check-related pur-  
2 poses; and

3 “(III) destroyed at such time as  
4 the covered personal data is no longer  
5 needed for background check-related  
6 purposes.

7 “(vii) EXCEPTION FOR LAWFULLY OB-  
8 TAINED PUBLIC DATA.—

9 “(I) IN GENERAL.—Except as  
10 provided in subclause (II) or (III) of  
11 this clause, clause (i) shall not apply  
12 to covered personal data that is ob-  
13 tained by a Federal law enforcement  
14 agency if—

15 “(aa) the Federal law en-  
16 forcement agency reasonably be-  
17 lieves that—

18 “(AA) the covered per-  
19 sonal data is lawfully ob-  
20 tained public data; or

21 “(BB) the covered per-  
22 sonal data is derived from  
23 covered personal data that  
24 solely consists of lawfully ob-  
25 tained public data; and

1 “(bb) the Federal law en-  
2 forcement agency receives—

3 “(AA) an attestation  
4 under penalty of perjury  
5 from the person providing  
6 the covered personal data  
7 that the covered personal  
8 data is lawfully obtained  
9 public data or is derived  
10 from covered personal data  
11 that solely consists of law-  
12 fully obtained public data;  
13 and

14 “(BB) each attestation  
15 described in paragraph  
16 (1)(G)(iii) with respect to  
17 the lawfully obtained public  
18 data.

19 “(II) EXCEPTION FOR BIOMET-  
20 RIC INFORMATION.—The exception  
21 under subclause (I) shall not apply to  
22 biometric information.

23 “(III) EXCEPTION FOR LOCATION  
24 INFORMATION.—The exception under

1                   subclause (I) shall not apply to loca-  
2                   tion information.

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

10                  “(3) LIMIT ON SHARING BETWEEN AGEN-  
11                  CIES.—

12                  “(A) IN GENERAL.—A Federal law en-  
13                  forcement agency may not acquire, receive,  
14                  query, or otherwise obtain or access covered  
15                  personal data from any governmental entity  
16                  (without regard to whether the governmental  
17                  entity is a Federal entity), if the covered per-  
18                  sonal data was obtained by that governmental  
19                  entity in a manner that would violate paragraph  
20                  (2) if the Federal law enforcement agency di-  
21                  rectly obtained the covered personal data in a  
22                  like manner.

23                  “(B) CAUSATION NOT REQUIRED.—The  
24                  prohibition in subparagraph (A) shall apply  
25                  without regard to whether the Federal law en-

1           enforcement agency caused the governmental enti-  
2           ty to obtain the covered personal data.

3           “(C) ATTESTATION REQUIRED.—A Fed-  
4           eral law enforcement agency may only acquire,  
5           receive, query, or otherwise obtain or access  
6           covered personal data from another govern-  
7           mental entity (without regard to whether the  
8           governmental entity is a Federal entity), if the  
9           Federal law enforcement agency obtains an at-  
10          testation that the covered personal data was not  
11          obtained by that governmental entity in a man-  
12          ner that would violate paragraph (2) if the Fed-  
13          eral law enforcement agency directly obtained  
14          the covered personal data in a like manner.

15          “(D) DESTRUCTION UPON ACQUISITION OF  
16          KNOWLEDGE.—If a Federal law enforcement  
17          agency learns that the Federal law enforcement  
18          agency previously acquired, received, queried, or  
19          otherwise obtained or accessed covered personal  
20          data from any governmental entity (without re-  
21          gard to whether the governmental entity is a  
22          Federal entity) that the governmental entity ob-  
23          tained in a manner described in subparagraph  
24          (A), the Federal law enforcement agency may  
25          not use or disseminate the covered personal

1 data or any information derived from the cov-  
2 ered personal data, and shall promptly destroy  
3 any such covered personal data that is still re-  
4 tained.

5 “(4) PROHIBITION ON USE AS EVIDENCE BY  
6 FEDERAL LAW ENFORCEMENT AGENCIES.—

7 “(A) IN GENERAL.—Covered personal data  
8 acquired, received, queried, or otherwise ob-  
9 tained or accessed by a Federal law enforce-  
10 ment agency in violation of paragraph (2) or  
11 (3), and any evidence derived therefrom, may  
12 not be used, received in evidence, or otherwise  
13 disseminated by, on behalf of, or upon a motion  
14 or other action by a Federal law enforcement  
15 agency in any investigation, trial, hearing, or  
16 other proceeding by, in, or before any court,  
17 grand jury, department, officer, agency, regu-  
18 latory body, legislative committee, or other au-  
19 thority of the United States, a State, or a polit-  
20 ical subdivision thereof.

21 “(B) USE BY AGGRIEVED PARTIES.—Noth-  
22 ing in subparagraph (A) shall be construed to  
23 limit the use of covered personal data by a cov-  
24 ered person aggrieved of a violation of para-



1 graph (2) or (3) in connection with any action  
2 relating to such a violation.

3 “(f) MINIMIZATION PROCEDURES.—

4 “(1) ADOPTION.—

5 “(A) IN GENERAL.—The Attorney General  
6 shall adopt specific procedures that are reason-  
7 ably designed to minimize the acquisition and  
8 retention, and to restrict the querying, of cov-  
9 ered personal data, and prohibit the dissemina-  
10 tion of information derived from covered per-  
11 sonal data, which shall include procedures to  
12 enforce the requirements of paragraphs (2), (3),  
13 and (4).

14 “(B) PERIODIC REVIEW.—Not later than 3  
15 years after the date of enactment of the Gov-  
16 ernment Surveillance Reform Act of 2026, and  
17 every 3 years thereafter, the Attorney General  
18 shall—

19 “(i) review the procedures adopted  
20 under subparagraph (A);

21 “(ii) publish a determination regard-  
22 ing whether the procedures need to be re-  
23 vised, in light of new technologies or viola-  
24 tions of the procedures; and

1 “(iii) adopt any necessary revisions to  
2 the procedures.

3 “(2) ACQUISITION AND RETENTION.—Each  
4 Federal law enforcement agency shall—

5 “(A) exhaust all reasonable means—

6 “(i) to exclude covered personal data  
7 that is not subject to 1 or more of the ex-  
8 ceptions set forth in clauses (iii) through  
9 (vii) of subsection (e)(2)(A) from the data  
10 obtained; and

11 “(ii) to remove and delete covered per-  
12 sonal data described in clause (i) after a  
13 compilation is obtained and before oper-  
14 ational use of the compilation or inclusion  
15 of the compilation in a dataset intended  
16 for operational use; and

17 “(B) audit the acquisition and retention of  
18 covered personal data by the Federal law en-  
19 forcement agency on an ongoing and continuous  
20 basis, to evaluate compliance with the proce-  
21 dures adopted under paragraph (1).

22 “(3) DESTRUCTION.—If a Federal law enforce-  
23 ment agency identifies covered personal data in a  
24 compilation described in paragraph (2)(A)(ii), the  
25 Federal law enforcement agency shall promptly de-

1       stroy the covered personal data and any dissemina-  
2       tion of information derived from the covered per-  
3       sonal data shall be prohibited.

4               “(4) QUERYING.—

5               “(A) IN GENERAL.—Except as provided in  
6       subparagraphs (B) and (C), no officer or em-  
7       ployee of a Federal law enforcement agency  
8       may conduct a query of personal data, including  
9       personal data already subjected to minimiza-  
10      tion, in an effort to find records of or about 1  
11      or more particular covered persons.

12              “(B) EXCEPTIONS.—Subparagraph (A)  
13      shall not apply to a query related to 1 or more  
14      particular covered persons if—

15              “(i) such covered persons are the sub-  
16      ject of a court order issued under this title  
17      or the Foreign Intelligence Surveillance  
18      Act of 1978 (50 U.S.C. 1801 et seq.) that  
19      would authorize the Federal law enforce-  
20      ment agency to compel the production of  
21      the covered personal data, during the effec-  
22      tive period of that order;

23              “(ii) the officer or employee of a Fed-  
24      eral law enforcement agency carrying out  
25      the query has a reasonable belief that the

1 life or safety of such covered persons are  
2 threatened and the information is sought  
3 for the purpose of assisting such covered  
4 persons, in which case information result-  
5 ing from the query may be accessed or  
6 used solely for that purpose and shall be  
7 destroyed at such time as it is no longer  
8 necessary for such purpose; or

9 “(iii) such covered persons have con-  
10 sented to the query.

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

14 “(i) each query shall be reasonably de-  
15 signed to exclude personal data of covered  
16 persons; and

17 “(ii) any personal data of covered per-  
18 sons returned pursuant to a query shall  
19 not be reviewed and shall immediately be  
20 destroyed.

21 “(g) TRANSPARENCY REQUIREMENTS.—

22 “(1) DEFINITION OF COVERED FEDERAL  
23 FUNDS.—In this subsection, the term ‘covered Fed-  
24 eral funds’ means—

1           “(A) funds provided under the Edward  
2           Byrne Memorial Justice Assistance Grant Pro-  
3           gram under subpart 1 of part E of title I of the  
4           Omnibus Crime Control and Safe Streets Act of  
5           1968 (34 U.S.C. 10151 et seq.);

6           “(B) funds provided through the Office of  
7           Community Oriented Policing Services;

8           “(C) funds received under an in-kind grant  
9           made under section 2576 of title 10;

10          “(D) funds received under an in-kind grant  
11          made via a transfer made under section 981 of  
12          this title; or

13          “(E) funds received under any other Fed-  
14          eral program that offers assistance to a law en-  
15          forcement agency similar to the assistance  
16          under the programs described in subparagraphs  
17          (A) through (D).

18          “(2) REPORTING.—If a State or local law en-  
19          forcement agency, using any means or facility of  
20          interstate or foreign commerce, through activities in  
21          or affecting interstate or foreign commerce, or by  
22          using covered Federal funds, obtains covered per-  
23          sonal data in a manner that would violate subsection  
24          (e)(2) if obtained by a Federal law enforcement  
25          agency in a like manner, the State or local law en-

1 enforcement agency shall publicly report, not less fre-  
2 quently than once per year—

3 “(A) the total amount in dollars of any-  
4 thing of value exchanged for such covered per-  
5 sonal data during the preceding year, which  
6 shall be disaggregated into money directly ex-  
7 changed and the estimated value of the other  
8 things of value that were exchanged;

9 “(B) the categories of covered personal  
10 data obtained in such a manner in the pre-  
11 ceding year, including whether the agency ob-  
12 tained location information, biometric informa-  
13 tion, web browsing data, or metadata of com-  
14 munications; and

15 “(C) an estimate of the total number of  
16 covered persons whose covered data was ob-  
17 tained in such a manner in the preceding  
18 year.”.

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

6 **SEC. 301. 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. 1881 et seq.)  
11 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 Federal Government may intentionally target  
21 a covered person for the purpose of acquiring foreign intel-  
22 ligence information, where such acquisition would be of  
23 communications content, location information, web brows-  
24 ing history, or internet search history of the covered per-  
25 son, or the acquisition would occur under circumstances

1 in which the person has a reasonable expectation of pri-  
2 vacy, or a warrant would be required for the acquisition  
3 of such information if the officer or employee sought to  
4 compel production of the information inside the United  
5 States for law enforcement purposes, unless such person  
6 is the subject of—

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

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

19           “(b) PEN REGISTER OR TRAP AND TRACE.—No offi-  
20      cer or employee of the Federal Government may inten-  
21      tionally target a covered person for the purpose of col-  
22      lecting foreign intelligence information through the instal-  
23      lation and use of a pen register or trap and trace device,  
24      or to acquire information the compelled production of  
25      which would require a pen register or trap and trace device



1 order if conducted inside the United States, unless such  
2 person is the subject of—

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

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

12 “(c) MATTERS RELATING TO EMERGENCY ACQUI-  
13 TION.—If an acquisition is conducted pursuant to an  
14 emergency authorization described in subsection (a)(1) or  
15 (b)(1) and the subsequent application to authorize elec-  
16 tronic surveillance, a physical search, an acquisition, or  
17 the installation and use of a pen register or trap and trace  
18 device pursuant to section 105(e), 304(e), or 403(a) of  
19 this Act is denied, or in any other case in which the acqui-  
20 sition has been conducted and no order is issued approving  
21 the acquisition—

22 “(1) no information obtained or evidence de-  
23 rived from such acquisition may be used, received in  
24 evidence, or otherwise disseminated in any investiga-  
25 tion, trial, hearing, or other proceeding in or before

1 any court, grand jury, department, office, agency,  
2 regulatory body, legislative committee, or other au-  
3 thority of the United States, a State, or political  
4 subdivision thereof; and

5 “(2) no information obtained or evidence de-  
6 rived from such acquisition concerning a covered  
7 person may subsequently be used or disclosed in any  
8 other manner without the consent of such person,  
9 except with the approval of the Attorney General, if  
10 the information indicates a threat of death or seri-  
11 ous bodily harm to any person.

12 “(d) RULE OF CONSTRUCTION.—Subsections (a),  
13 (b), and (c) shall apply regardless of the location of the  
14 acquisition.”.

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

18 (1) in section 601(a)(1) (50 U.S.C.  
19 1871(a)(1))—

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

22 (B) in subparagraph (B), by striking the  
23 semicolon and inserting “; and”;

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

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

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

8           (1) by striking the items relating to sections  
9       703, 704, and 705; and

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

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

12       **SEC. 302. CONSISTENT DISCLOSURES OF RELEVANT INFOR-**  
13                               **MATION IN TITLE V AND OTHER FISA APPLI-**  
14                               **CATIONS.**

15       (a) CONSISTENT PROCEDURES FOR TITLE V AND  
16       OTHER FISA APPLICATIONS.—The Foreign Intelligence  
17       Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is  
18       amended in section 104(a)(12), in the matter before sub-  
19       paragraph (A), section 303(a)(10), in the matter before  
20       subparagraph (A), and section 402(c)(4), in the matter  
21       before subparagraph (A), are amended by inserting “, and  
22       that the application fairly reflects all information,” after  
23       “apprised of all information” each place it appears.

1 (b) TECHNICAL CORRECTIONS.—Such Act is further  
2 amended—

3 (1) in section 104(a)—

4 (A) in paragraph (9), by striking “; and”  
5 and inserting a semicolon;

6 (B) in paragraph (11), by striking “; and”  
7 and inserting a semicolon; and

8 (C) in paragraph (12)(B), by striking the  
9 period at the end and inserting “; and”;  
10 (2) in section 303(a)—

11 (A) in paragraph (9), by striking “; and”  
12 and inserting a semicolon; and

13 (B) in paragraph (10)(B), by striking the  
14 period at the end and inserting “; and”; and

15 (3) in section 502(b)(2), by redesignating sub-  
16 paragraphs (E) and (F) as subparagraphs (C) and  
17 (D), respectively.

18 **SEC. 303. STRENGTHENING ACCURACY PROCEDURES.**

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

1 **“TITLE IX—REQUIRED DISCLO-**  
2 **SURE OF RELEVANT INFOR-**  
3 **MATION**

4 **“SEC. 901. CERTIFICATION REGARDING ACCURACY PROCE-**  
5 **DURES.**

6 “(a) DEFINITION OF ACCURACY PROCEDURES.—In  
7 this section, the term ‘accuracy procedures’ means specific  
8 procedures, adopted by the Attorney General, to ensure  
9 that an application for a court order under this Act, in-  
10 cluding any application for renewal of an existing order,  
11 is accurate and complete, including procedures that en-  
12 sure, at a minimum, that—

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

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

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

1           “(4) the applicant coordinates with the appro-  
2           priate elements of the intelligence community (as de-  
3           fined in section 3 of the National Security Act of  
4           1947 (50 U.S.C. 3003)), concerning any prior or ex-  
5           isting relationship with the target of any surveil-  
6           lance, search, or other means of investigation, and  
7           discloses any such relationship in the application;

8           “(5) before any application targeting a United  
9           States person is made, the applicant Federal officer  
10          or employee documents that the officer or employee  
11          has collected and reviewed for accuracy and com-  
12          pleteness supporting documentation for each factual  
13          assertion in the application; and

14          “(6) the applicant Federal agency establishes  
15          compliance and auditing mechanisms on an annual  
16          basis to assess the efficacy of the accuracy proce-  
17          dures that have been adopted and reports such find-  
18          ings to the Attorney General.

19          “(b) STATEMENT AND CERTIFICATION OF ACCURACY  
20          PROCEDURES.—Any Federal officer or employee making  
21          an application for a court order under this Act shall in-  
22          clude with the application—

23                 “(1) a description of the accuracy procedures  
24                 employed by the officer or employee, or their des-  
25                 ignee; and

1           “(2) a certification that the officer or employee,  
2           or their designee, has collected and reviewed for ac-  
3           curacy and completeness—

4                   “(A) supporting documentation for each  
5           factual assertion contained in the application;

6                   “(B) all information that might reasonably  
7           call into question the accuracy of the informa-  
8           tion or the reasonableness of any assessment in  
9           the application, or otherwise raises doubts  
10          about the requested findings; and

11                   “(C) all material information that might  
12          reasonably call into question the reliability and  
13          reporting of any information from any confiden-  
14          tial human source that is used in the applica-  
15          tion.

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

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

“TITLE IX—REQUIRED DISCLOSURE OF RELEVANT  
INFORMATION

“901. Certification regarding accuracy procedures.”.

1       (c) TIMELINE TO ADOPT NEW ACCURACY PROCE-  
2 DURES.—

3           (1) IN GENERAL.—Not later than 180 days  
4 after the date of the enactment of this Act, the At-  
5 torney General shall issue accuracy procedures (as  
6 defined in section 901(a) of the Foreign Intelligence  
7 Surveillance Act of 1978, as added by subsection  
8 (a)).

9           (2) REPEAL OF ACCURACY PROCEDURES RE-  
10 QUIREMENT FROM RISAA.—On the day that is 180  
11 days after the date of the enactment of this Act,  
12 paragraph (7) of section 10(a) of the Reforming In-  
13 telligence and Securing America Act (Public Law  
14 118–49; 50 U.S.C. 1804 note) is repealed.

15 **SEC. 304. CLARIFICATION REGARDING TREATMENT OF IN-**  
16 **FORMATION AND EVIDENCE ACQUIRED**  
17 **UNDER THE FOREIGN INTELLIGENCE SUR-**  
18 **VEILLANCE ACT OF 1978.**

19       (a) IN GENERAL.—Section 101 of the Foreign Intel-  
20 ligence Surveillance Act of 1978 (50 U.S.C. 1801), as  
21 amended by section 2(a), is further amended by adding  
22 at the end the following:



1       “(t) For the purposes of notification provisions of this  
2 Act, information or evidence is ‘derived’ from an electronic  
3 surveillance, physical search, use of a pen register or trap  
4 and trace device, production of tangible things, or acquisi-  
5 tion under this Act when the Government would not have  
6 originally possessed the information or evidence but for  
7 that electronic surveillance, physical search, use of a pen  
8 register or trap and trace device, production of tangible  
9 things, or acquisition, and regardless of any claim that  
10 the information or evidence is attenuated from the surveil-  
11 lance or search, would inevitably have been discovered, or  
12 was subsequently reobtained through other means.”.

13       (b) POLICIES AND GUIDANCE.—

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

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

21           (B) Guidance for all members of the intel-  
22 ligence community (as defined in section 3 of  
23 the National Security Act of 1947 (50 U.S.C.  
24 3003)) and all Federal agencies with law en-

1           enforcement responsibilities concerning the appli-  
2           cation of such subsection (t).

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

8   **SEC. 305. SUNSET ON GRANDFATHER CLAUSE OF SECTION**  
9                           **215 OF THE USA PATRIOT ACT.**

10          Section 102(b)(2) of the USA PATRIOT Improve-  
11          ment and Reauthorization Act of 2005 (Public Law 109–  
12          177; 50 U.S.C. 1805 note) is amended by inserting “, ex-  
13          cept that title V of the Foreign Intelligence Surveillance  
14          Act of 1978, as in effect on March 14, 2020, shall cease  
15          to have effect on the date that is 180 days after the date  
16          of the enactment of the Government Surveillance Reform  
17          Act of 2026” after “continue in effect”.

18   **SEC. 306. WRITTEN RECORD OF DEPARTMENT OF JUSTICE**  
19                           **INTERACTIONS WITH FOREIGN INTEL-**  
20                           **LIGENCE SURVEILLANCE COURT.**

21          Section 103 of the Foreign Intelligence Surveillance  
22          Act of 1978 (50 U.S.C. 1803) is amended by adding at  
23          the end the following:

24          “(n) WRITTEN RECORD OF INTERACTIONS.—

1           “(1) WRITTEN COMMUNICATIONS.—The Attor-  
 2       ney General shall maintain all written communica-  
 3       tions with the Foreign Intelligence Surveillance  
 4       Court, including the identity of the employees of the  
 5       court to or from whom the communications were  
 6       made, regarding an application or order made under  
 7       this title in a file associated with the application or  
 8       order.

9           “(2) ORAL COMMUNICATIONS.—The Attorney  
 10      General shall—

11           “(A) document a summary of any oral  
 12       communications with the Foreign Intelligence  
 13       Surveillance Court including the identity of the  
 14       employees of the court to or from whom the  
 15       communications were made, relating to an ap-  
 16       plication or order described in paragraph (1);  
 17       and

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

20   **SEC. 307. APPOINTMENT OF AMICI CURIAE AND ACCESS TO**  
 21       **INFORMATION.**

22       (a) EXPANSION OF APPOINTMENT AUTHORITY.—

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

1 (A) in subparagraph (A)—

2 (i) by striking clause (i) and inserting  
3 the following:

4 “(i) shall appoint one or more individ-  
5 uals who have been designated under para-  
6 graph (1) and who possesses expertise in  
7 privacy and civil liberties to serve as ami-  
8 cus curiae to assist such court in the con-  
9 sideration of any application or motion for  
10 an order or review, unless the court issues  
11 a written finding that such application nei-  
12 ther presents nor involves—

13 “(I) a novel or significant inter-  
14 pretation of the law;

15 “(II) a significant concern re-  
16 lated to constitutional rights;

17 “(III) a sensitive investigative  
18 matter;

19 “(IV) a request for approval of a  
20 new program, a new technology, or a  
21 new use of existing technology;

22 “(V) a request for reauthoriza-  
23 tion of programmatic surveillance; or

24 “(VI) any other privacy or civil  
25 liberties issue for which an appoint-

1                   ment of an amicus curiae to assist the  
2                   court in the consideration of the appli-  
3                   cation would be appropriate;”;

4                   (ii) in clause (ii), by striking “; and”  
5                   and inserting a period;

6                   (iii) by redesignating clause (ii) as  
7                   clause (iv) and moving such clause so as to  
8                   appear after clause (iii);

9                   (iv) by inserting after clause (i) the  
10                  following:

11                 “(ii) shall appoint one or more indi-  
12                 viduals who have been designated under  
13                 paragraph (1) and who possesses technical  
14                 expertise to serve as amicus curiae to as-  
15                 sist such court in the consideration of any  
16                 application for an order or review, unless  
17                 the court issues a written finding that such  
18                 application neither presents nor involves—

19                 “(I) a request for approval of a  
20                 new program, a new technology, or a  
21                 new use of existing technology;

22                 “(II) a request for approval of a  
23                 previously authorized program, tech-  
24                 nology, or use of existing technology  
25                 for which no prior application for ap-

1                   proval of such program, technology, or  
2                   use was considered by the court with  
3                   the assistance of an amicus curiae  
4                   who possesses technical expertise; or

5                   “(III) a technical issue material  
6                   to any legal determination for which  
7                   an appointment of an amicus curiae  
8                   who possesses technical expertise to  
9                   assist the court in the consideration of  
10                  the application would be appro-  
11                  priate;”; and

12                  (v) in clause (iii), by striking “, unless  
13                  the court issues a finding that such ap-  
14                  pointment is not appropriate or is likely to  
15                  result in undue delay.” and inserting “;  
16                  and”; and

17                  (B) by striking subparagraph (B).

18                  (2) DEFINITION OF SENSITIVE INVESTIGATIVE  
19                  MATTER.—Section 103(i) of such Act (50 U.S.C.  
20                  1803(i)) is amended by adding at the end the fol-  
21                  lowing:

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

1           “(A) an investigative matter involving the  
2           activities of—

3                   “(i) a domestic public official or polit-  
4                   ical candidate, or an individual serving on  
5                   the staff of such an official or candidate;

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

10                   “(iii) the domestic news media; or

11           “(B) any other investigative matter involv-  
12           ing a domestic entity or a known or suspected  
13           United States person that, in the judgment of  
14           the Foreign Intelligence Surveillance Court or  
15           the Foreign Intelligence Surveillance Court of  
16           Review, is similarly as sensitive as an investiga-  
17           tive matter described in subparagraph (A).”.

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

20                   (A) by inserting “cybersecurity, cryptog-  
21                   raphy,” after “communications technology,”;  
22                   and

23                   (B) by adding at the end the following:  
24           “Of such individuals, at least one shall possess

1           legal expertise and at least one shall possess  
2           technical expertise.”.

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

6           “(7) NOTIFICATION.—The presiding judge of  
7           the Foreign Intelligence Surveillance Court and the  
8           Foreign Intelligence Surveillance Court or Review  
9           shall, not less frequently than quarterly, provide to  
10          the Attorney General and the appropriate commit-  
11          tees of Congress—

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

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

17          (5) SECTION 702 RECERTIFICATION SCHED-  
18          ULE.—Section 702(j)(5)(A) of such Act (50 U.S.C.  
19          1881a(j)(5)(A)) is amended by striking “at least 30  
20          days prior to the expiration of such authorization”  
21          and inserting “such number of days, not less than  
22          30 days, before the expiration of such authorization  
23          as the Court considers necessary to permit review by  
24          amici curiae appointed under section  
25          103(i)(2)(A)(iii).”.



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

4 (1) in paragraph (4)—

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

7 (B) in the matter preceding subparagraph  
 8 (A), by striking “shall”;

9 (C) in subparagraph (B)—

10 (i) in the matter preceding clause (i),  
 11 by inserting “shall” before “provide”;

12 (ii) in clause (i), by striking “of  
 13 United States persons” and inserting the  
 14 following: “, including legal arguments re-  
 15 garding any privacy or civil liberties inter-  
 16 est of any United States person that would  
 17 be significantly affected by the application  
 18 or motion”; and

19 (iii) in clause (iii), by striking the pe-  
 20 riod at the end and inserting “; and”;

21 (D) by striking subparagraph (A);

22 (E) by redesignating subparagraph (B) as  
 23 subparagraph (A); and

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

1 “(B) may seek leave to raise any novel or  
2 significant privacy or civil liberties issue rel-  
3 evant to the application or motion or other  
4 issue directly affecting the legality of the pro-  
5 posed electronic surveillance with the court, re-  
6 gardless of whether the court has requested as-  
7 sistance on that issue.”;

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

11 (3) by inserting after paragraph (6) the fol-  
12 lowing:

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

15 “(A) FOREIGN INTELLIGENCE SURVEIL-  
16 LANCE COURT DECISIONS.—

17 “(i) PETITION.—Following issuance of  
18 an order under this Act by the Foreign In-  
19 telligence Surveillance Court, an amicus  
20 curiae appointed under paragraph (2) may  
21 petition the Foreign Intelligence Surveil-  
22 lance Court to certify for review to the  
23 Foreign Intelligence Surveillance Court of  
24 Review a question of law pursuant to sub-  
25 section (j).

1                   “(ii) DENIALS.—If the Foreign Intel-  
2                   ligence Surveillance Court denies a petition  
3                   described in clause (i), the court shall pro-  
4                   vide for the record a written statement of  
5                   the reasons for such denial.

6                   “(iii) CERTIFICATION.—Upon certifi-  
7                   cation of any question of law pursuant to  
8                   this subparagraph, the Foreign Intelligence  
9                   Surveillance Court of Review shall appoint  
10                  the amicus curiae to assist the Court of  
11                  Review in its consideration of the certified  
12                  question, unless the Court of Review issues  
13                  a finding that such appointment is not ap-  
14                  propriate.

15                  “(B) FOREIGN INTELLIGENCE SURVEIL-  
16                  LANCE COURT OF REVIEW DECISIONS.—An  
17                  amicus curiae appointed under paragraph (2)  
18                  may petition the Foreign Intelligence Surveil-  
19                  lance Court of Review to certify for review to  
20                  the Supreme Court of the United States any  
21                  question of law pursuant to section 1254(2) of  
22                  title 28, United States Code.

23                  “(C) DECLASSIFICATION OF REFER-  
24                  RALS.—For purposes of section 602, a petition  
25                  filed under subparagraph (A) or (B) of this

1 paragraph and all of its content shall be consid-  
2 ered a decision, order, or opinion issued by the  
3 Foreign Intelligence Surveillance Court or the  
4 Foreign Intelligence Surveillance Court of Re-  
5 view described in paragraph (2) of section  
6 602(a).”.

7 (c) ACCESS TO INFORMATION.—

8 (1) APPLICATION AND MATERIALS.—Section  
9 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is  
10 amended—

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

13 “(i) shall have access to, to the extent  
14 such information is available to the Gov-  
15 ernment—

16 “(I) the application, certification,  
17 petition, motion, and other informa-  
18 tion and supporting materials, includ-  
19 ing any information described in sec-  
20 tion 901, submitted to the Foreign In-  
21 telligence Surveillance Court in con-  
22 nection with the matter in which the  
23 amicus curiae has been appointed, in-  
24 cluding access to any relevant legal  
25 precedent (including any such prece-

1 dent that is cited by the Government,  
2 including in such an application);

3 “(II) any other information or  
4 materials that the court determines is  
5 relevant to the duties of the amicus  
6 curiae; and

7 “(III) an unredacted copy of  
8 each relevant decision made by the  
9 Foreign Intelligence Surveillance  
10 Court or the Foreign Intelligence Sur-  
11 veillance Court of Review in which the  
12 court decides a question of law, with-  
13 out regard to whether the decision is  
14 classified; and

15 “(ii) may make a submission to the  
16 court requesting access to any other par-  
17 ticular materials or information (or cat-  
18 egory of materials or information) that the  
19 amicus curiae believes to be relevant to the  
20 duties of the amicus curiae.”;

21 (B) by redesignating subparagraph (D) as  
22 subparagraph (F); and

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

1           “(D) SUPPORTING DOCUMENTATION RE-  
2           GARDING ACCURACY.—The Foreign Intelligence  
3           Surveillance Court, upon the motion of an ami-  
4           cus curiae appointed under paragraph (2) or  
5           upon its own motion, may require the Govern-  
6           ment to make available the supporting docu-  
7           mentation described in section 902.”.

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

11           (A) in subparagraph (B), by striking “The  
12           Attorney General may periodically” and insert-  
13           ing “Not less frequently than annually, the At-  
14           torney General shall”; and

15           (B) by striking subparagraph (C) and in-  
16           serting the following:

17           “(C) CLASSIFIED INFORMATION.—An ami-  
18           cus curiae appointed by the court shall have ac-  
19           cess to, to the extent such information is avail-  
20           able to the Government, unredacted copies of  
21           each opinion, order, transcript, pleading, or  
22           other document of the Foreign Intelligence Sur-  
23           veillance Court and the Foreign Intelligence  
24           Surveillance Court of Review, including, if the  
25           individual is eligible for access to classified in-

1           formation, any classified documents, informa-  
2           tion, and other materials or proceedings.”.

3           (3) CONSULTATION AMONG AMICI CURIAE.—  
4           Section 103(i)(6) of such Act (50 U.S.C.  
5           1803(i)(6)), as amended by paragraphs (1) and (2),  
6           is further amended—

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

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

12                   “(B) CONSULTATION.—If the Foreign In-  
13           telligence Surveillance Court or the Foreign In-  
14           telligence Surveillance Court of Review deter-  
15           mines that it is relevant to the duties of an  
16           amicus curiae appointed under paragraph (2),  
17           the amicus curiae may consult with one or more  
18           of the other individuals designated to serve as  
19           amicus curiae under paragraph (1) regarding  
20           any of the information relevant to any assigned  
21           proceeding.”.

1 **SEC. 308. DECLASSIFICATION OF SIGNIFICANT DECISIONS,**  
2 **ORDERS, AND OPINIONS.**

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

6 “(a) DECLASSIFICATION REQUIRED.—

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

10 “(A) conduct a declassification review of  
11 each decision, order, or opinion issued by the  
12 Foreign Intelligence Surveillance Court or the  
13 Foreign Intelligence Surveillance Court of Re-  
14 view (as defined in section 601(e)) that is de-  
15 scribed in paragraph (2);

16 “(B) consistent with that review, make  
17 publicly available to the greatest extent prac-  
18 ticable each such decision, order, or opinion;  
19 and

20 “(C) complete the declassification review  
21 required by subparagraph (A) and public re-  
22 lease of each such decision, order, or opinion  
23 pursuant to subparagraph (B) by not later than  
24 180 days after the date on which the Foreign  
25 Intelligence Surveillance Court or the Foreign



1 Intelligence Surveillance Court of Review issues  
2 such decision, order, or opinion.

3 “(2) DECISION, ORDER, OR OPINION DE-  
4 SCRIBED.—A decision, order, or opinion issued by  
5 the Foreign Intelligence Surveillance Court or the  
6 Foreign Intelligence Surveillance Court of Review  
7 that is described in this paragraph is any such deci-  
8 sion, order, or opinion issued before, on, or after the  
9 date of the enactment of this Act that—

10 “(A) includes a significant construction or  
11 interpretation of any provision of law, including  
12 any novel or significant construction or inter-  
13 pretation of any term;

14 “(B) involves a sensitive investigative mat-  
15 ter (as defined in section 103(i)(12)); or

16 “(C) has been nominated for a declassifica-  
17 tion review by an amicus curiae appointed by  
18 the court.”.

19 **SEC. 309. CLARIFICATION OF FOREIGN INTELLIGENCE SUR-**  
20 **VEILLANCE COURT JURISDICTION OVER**  
21 **RECORDS OF THE COURT AND OTHER ANCIL-**  
22 **LARY MATTERS.**

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

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

2 “(o) ANCILLARY CLAIMS.—

3 “(1) FOREIGN INTELLIGENCE SURVEILLANCE  
4 COURT.—The Foreign Intelligence Surveillance  
5 Court shall have jurisdiction to hear claims ancillary  
6 to any of its own proceedings, including jurisdiction  
7 to hear any claim for access to the court’s records,  
8 files, and proceedings under the Constitution of the  
9 United States, statute, common law, or any other  
10 authority. Upon deciding such a claim, the Court  
11 shall provide immediately for the record a written  
12 statement of the reasons for such decision. A party  
13 may file a petition for review of such decision with  
14 the Foreign Intelligence Surveillance Court of Re-  
15 view, which shall have jurisdiction to consider such  
16 petition and, upon deciding such petition, shall pro-  
17 vide for the record a written statement of the rea-  
18 sons for its decision.

19 “(2) FOREIGN INTELLIGENCE SURVEILLANCE  
20 COURT OF REVIEW.—The Foreign Intelligence Sur-  
21 veillance Court of Review shall have jurisdiction to  
22 hear claims ancillary to any of its own proceedings,  
23 including jurisdiction to hear any claim for access to  
24 the court’s records, files, and proceedings under the  
25 Constitution of the United States, statute, common

1 law, or any other authority. Upon deciding such a  
2 claim, the Court of Review shall provide immediately  
3 for the record a written statement of the reasons for  
4 such decision.

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

11 (2) in subsection (a)(2)(A), in the matter pre-  
12 ceding clause (i), by inserting “paragraph (1) of  
13 subsection (o) of this section or” before “paragraph  
14 (4) or (5) of section 702(i)”; and

15 (3) in subsection (k)(1), by striking “section  
16 1254(2) of title 28” and inserting “section 1254 of  
17 title 28”.

18 (b) TECHNICAL CORRECTIONS.—Section 103 of the  
19 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.  
20 1803), as amended by section (a), is further amended—

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

24 (2) in subsection (e), by striking “section  
25 501(f)(1) or” each place it appears.

1 **SEC. 310. GROUNDS FOR DETERMINING INJURY IN FACT IN**  
 2 **CIVIL ACTIONS RELATING TO SURVEILLANCE**  
 3 **UNDER THE FOREIGN INTELLIGENCE SUR-**  
 4 **VEILLANCE ACT OF 1978 OR PURSUANT TO**  
 5 **EXECUTIVE AUTHORITY.**

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

10 **“TITLE X—ADDITIONAL**  
 11 **MATTERS**

12 **“SEC. 1001. CHALLENGES TO GOVERNMENT SURVEIL-**  
 13 **LANCE.**

14 “(a) DEFINITIONS.—In this section, the terms ‘for-  
 15 eign intelligence information’, ‘person’, ‘United States’,  
 16 and ‘United States person’ have the meanings given such  
 17 terms in section 101.

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

1           “(1)(A) regularly communicates foreign intel-  
2           ligence information with persons who are not United  
3           States persons and who are located outside the  
4           United States; and

5           “(B) has taken or is taking objectively reason-  
6           able measures to avoid the acquisition, copying,  
7           querying, retention, access, or use of the person’s in-  
8           formation under this Act or pursuant to another au-  
9           thority of the executive branch of the Federal Gov-  
10          ernment; or

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

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

23          “(d) STATE SECRETS PRIVILEGE.—The procedures  
24          set forth in section 106(f) shall apply when the State se-  
25          crets privilege is asserted, with respect to any claim where

1 the plaintiff, who is a United States person or person lo-  
 2 cated in the United States, plausibly alleges an injury-in-  
 3 fact relating to the acquisition, copying, querying, reten-  
 4 tion, access, or use of information acquired under this Act  
 5 or pursuant to another authority of the executive branch  
 6 of the Federal Government and plausibly alleges that the  
 7 acquisition, copying, querying, retention, access, or use of  
 8 information violates the Constitution or laws of the United  
 9 States.”.

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

“TITLE X—ADDITIONAL MATTERS

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

14 **SEC. 311. ACCOUNTABILITY PROCEDURES FOR VIOLATIONS**  
 15 **BY FEDERAL EMPLOYEES.**

16 (a) IN GENERAL.—Title X of the Foreign Intel-  
 17 ligence Surveillance Act of 1978 (50 U.S.C. 1881 et seq.),  
 18 as added by section 310, is amended by adding at the end  
 19 the following:

20 **“SEC. 1002. ACCOUNTABILITY PROCEDURES FOR VIOLA-**  
 21 **TIONS BY FEDERAL EMPLOYEES.**

22 “(a) DEFINITIONS.—In this section:

23 “(1) APPROPRIATE COMMITTEES OF CON-  
 24 GRESS.—The term ‘appropriate committees of Con-

1       gress’ has the meaning given such term in section  
2       101.

3               “(2) COVERED AGENCY.—The term ‘covered  
4       agency’ means the Federal Bureau of Investigation,  
5       the Central Intelligence Agency, the National Secu-  
6       rity Agency, and the National Counterterrorism  
7       Center.

8               “(3) COVERED PERSON.—The term ‘covered  
9       person’ has the meaning given such term in section  
10       701(b).

11              “(4) COVERED VIOLATION.—The term ‘covered  
12       violation’ means a violation of this Act, the Govern-  
13       ment Surveillance Reform Act of 2026, or Executive  
14       Order 12333 (50 U.S.C. 3001 note; relating to  
15       United States intelligence activities), or successor  
16       order, by an employee of a covered agency that re-  
17       sults in the inappropriate collection, use, querying,  
18       or dissemination of any communication, record, or  
19       information of a covered person.

20              “(5) PERSON, UNITED STATES, AND UNITED  
21       STATES PERSON.—The terms ‘person’, ‘United  
22       States’, and ‘United States person’ have the mean-  
23       ings given such terms in section 101.

1       “(b) ACCOUNTABILITY PROCEDURES; DESIGNATED  
2 INVESTIGATIVE ENTITY.—The head of each covered agen-  
3 cy shall—

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

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

10          “(B) establish an internal process for the des-  
11 ignated entity to determine culpability for willful,  
12 knowing, reckless, and negligent covered violations.

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

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

18           “(2) Escalating consequences for willful, know-  
19 ing, reckless, and negligent covered violations, in-  
20 cluding—

21           “(A) consequences for an initial reckless or  
22 negligent covered violation, including, at a min-  
23 imum—

24           “(i) suspension of access to informa-  
25 tion acquired under this Act or to the



1 dataset that gave rise to the violation for  
2 not less than 90 days; and

3 “(ii) documentation of the incident in  
4 the personnel file of each employee respon-  
5 sible for the violation;

6 “(B) consequences for a second reckless or  
7 negligent covered violation, including, at a min-  
8 imum—

9 “(i) suspension of access to informa-  
10 tion acquired under this Act or to the  
11 dataset that gave rise to the violation for  
12 not less than 180 days; and

13 “(ii) reassignment of each employee  
14 responsible for the violation;

15 “(C) consequences for a third reckless or  
16 negligent covered violation, including, at a min-  
17 imum—

18 “(i) termination of security clearance;  
19 and

20 “(ii) reassignment or termination of  
21 each employee responsible for the violation;

22 “(D) consequences for an initial willful or  
23 knowing covered violation, including, at a min-  
24 imum—

1 “(i) suspension of access to informa-  
2 tion acquired under this Act or to the  
3 dataset that gave rise to the violation for  
4 not less than 180 days; and

5 “(ii) reassignment of each employee  
6 responsible for the violation; and

7 “(E) consequences for a second willful or  
8 knowing covered violation, including, at a min-  
9 imum—

10 “(i) termination of security clearance;  
11 and

12 “(ii) reassignment or termination of  
13 each employee responsible for the violation.

14 “(d) PRESUMPTION OF TERMINATION.—

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

19 “(2) JUSTIFICATION.—If the head of a covered  
20 agency determines not to terminate an employee for  
21 a third reckless or negligent violation under subpara-  
22 graph (C)(ii) of subsection (c)(2) or a second willful  
23 or knowing violation under subparagraph (E)(ii) of  
24 that subsection, the agency head shall submit to the

1 appropriate committees of Congress a written jus-  
2 tification for the determination.

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

9 (b) CLERICAL AMENDMENT.—The table of contents  
10 for such Act is amended by inserting after the item relat-  
11 ing to section 1001, as added by section 310, the fol-  
12 lowing:

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

13 (c) REPORT REQUIRED.—

14 (1) IN GENERAL.—Not later than 180 days  
15 after the date of the enactment of this Act, the head  
16 of each covered agency, as defined in section 1002  
17 of the Foreign Intelligence Surveillance Act of 1978  
18 (as added by subsection (a)), shall submit to the ap-  
19 propriate committees of Congress a report detail-  
20 ing—

21 (A) the procedures established under sec-  
22 tion 1002 of the Foreign Intelligence Surveil-  
23 lance Act of 1978, as added by subsection (a);  
24 and

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

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

7 (d) DECONFLICTION WITH RISAA ACCOUNTABILITY  
 8 PROCEDURES.—

9 (1) IN GENERAL.—Paragraph (4) of section  
 10 702(f) of such Act (50 U.S.C. 1881a(f)) is repealed.

11 (2) CONFORMING AMENDMENT.—Paragraph (6)  
 12 of such section 702(f), as added by section 101 and  
 13 redesignated by section 110, is redesignated as para-  
 14 graph (4) and moved before paragraph (5) of such  
 15 section 702(f).

16 (3) EFFECT DATE.—The amendments made by  
 17 paragraphs (1) and (2) shall take effect on the date  
 18 that is 180 days after the date of the enactment of  
 19 this Act.

20 **SEC. 312. REFORMS TO THE EXCLUSIVE MEANS LIMITA-**  
 21 **TIONS UNDER THE FOREIGN INTELLIGENCE**  
 22 **SURVEILLANCE ACT OF 1978.**

23 (a) CHAPTER 119 OF TITLE 18.—Section 2511(2)(f)  
 24 of title 18, United States Code, is amended to read as  
 25 follows:

1       “(f)(i) Other than as provided in subsection (ii), noth-  
2 ing contained in this chapter or chapter 121 or 206 of  
3 this title, or section 705 of the Communications Act of  
4 1934 (47 U.S.C. 605), shall be deemed to affect the acqui-  
5 sition by the United States Government of foreign intel-  
6 ligence information from international or foreign commu-  
7 nications, or foreign intelligence activities conducted in ac-  
8 cordance with otherwise applicable Federal law involving  
9 a foreign electronic communications system, utilizing a  
10 means other than electronic surveillance as defined in sec-  
11 tion 101 of the Foreign Intelligence Surveillance Act of  
12 1978 (50 U.S.C. 1801).

13       “(ii) The procedures in this chapter, chapter 121,  
14 and the Foreign Intelligence Surveillance Act of 1978 (50  
15 U.S.C. 1801 et seq.) shall be the exclusive means by which  
16 the United States Government may conduct—

17               “(A) electronic surveillance, as defined in sec-  
18 tion 101 of that Act;

19               “(B) the interception of wire, oral, and elec-  
20 tronic communications within the United States or  
21 from a domestic electronic communications system;  
22 or

23               “(C) the interception of wire, oral, and elec-  
24 tronic communications for which the sender and all

1 intended recipients are located within the United  
2 States.”.

3 (b) FOREIGN INTELLIGENCE SURVEILLANCE ACT.—  
4 Section 112 of the Foreign Intelligence Surveillance Act  
5 (50 U.S.C. 1812) is amended to read as follows:

6 “(a) Except as provided in subsection (b), the proce-  
7 dures of chapters 119, 121, and 206 of title 18 and this  
8 Act shall be the exclusive means by which the United  
9 States Government may conduct—

10 “(1) electronic surveillance, as defined in sec-  
11 tion 101;

12 “(2) the interception of wire, oral, and elec-  
13 tronic communications within the United States or  
14 from a domestic electronic communications system;  
15 or

16 “(3) the interception of wire, oral, and elec-  
17 tronic communications for which the sender and all  
18 intended recipients are located within the United  
19 States.

20 “(b) Only an express statutory authorization for elec-  
21 tronic surveillance or the interception of wire, oral, or elec-  
22 tronic communications described in subsection (a), other  
23 than as an amendment to this chapter or chapters 119,  
24 121, or 206 of title 18, shall constitute an additional ex-  
25 clusive means for the purpose of subsection (a).

1 “(c) The procedures in this Act and title IV of the  
 2 Government Surveillance Reform Act shall be the exclusive  
 3 means by which the location information of 1 or more per-  
 4 sons located in the United States may be acquired for for-  
 5 eign intelligence purposes by the United States Govern-  
 6 ment.”.

7 **TITLE IV—REFORMS RELATED**  
 8 **TO SURVEILLANCE CON-**  
 9 **DUCTED FOR FOREIGN IN-**  
 10 **TELLIGENCE PURPOSES**  
 11 **OTHER THAN UNDER THE**  
 12 **FOREIGN INTELLIGENCE**  
 13 **SURVEILLANCE ACT OF 1978**

14 **SEC. 401. DEFINITIONS.**

15 In this title:

16 (1) CONGRESSIONAL INTELLIGENCE COMMIT-  
 17 TEES, INTELLIGENCE, INTELLIGENCE COMMUNITY,  
 18 AND FOREIGN INTELLIGENCE.—The terms “congres-  
 19 sional intelligence committees”, “intelligence”, “in-  
 20 telligence community”, and “foreign intelligence”  
 21 have the meanings given such terms in section 3 of  
 22 the National Security Act of 1947 (50 U.S.C. 3003).

23 (2) ELECTRONIC SURVEILLANCE, PERSON,  
 24 STATE, UNITED STATES, AND UNITED STATES PER-  
 25 SON.—The terms “electronic surveillance”, “per-

son”, “State”, “United States”, and “United States person” have the meanings given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

**SEC. 402. PROTECTIONS RELATED TO WARRANTLESS QUERIES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS AND PERSONS LOCATED IN THE UNITED STATES.**

(a) DEFINITIONS.—In this section:

(1) COVERED INFORMATION.—The term “covered information” includes—

(A) communications content; and

(B) information, the compelled disclosure of which would require a probable cause warrant if sought for law enforcement purposes inside the United States.

(2) COVERED QUERY.—The term “covered query” means a query—

(A) using a term associated with 1 or more covered persons; or

(B) for a significant purpose of retrieving information of, or concerning 1 or more covered persons.

(3) QUERY.—



1 (A) IN GENERAL.—The term “query”  
2 means the use of 1 or more terms, whether con-  
3 ducted through manual or automated means, to  
4 retrieve any information described in subpara-  
5 graph (B), including retrieval from a subset of  
6 such information, whether that subset was cre-  
7 ated by retrieval through a query or other  
8 means.

9 (B) INFORMATION DESCRIBED.—The in-  
10 formation described in this subparagraph is in-  
11 formation that was acquired for foreign intel-  
12 ligence purposes, other than acquisitions au-  
13 thorized by the Foreign Intelligence Surveil-  
14 lance Act of 1978 (50 U.S.C. 1801 et seq.), re-  
15 gardless of whether such acquisition occurred  
16 inside or outside the United States.

17 (b) IN GENERAL.—Except as provided in subsections  
18 (c) and (d), no officer or employee of the Federal Govern-  
19 ment may access covered information returned in response  
20 to a covered query.

21 (c) EXCEPTIONS FOR CONCURRENT AUTHORIZATION,  
22 CONSENT, EMERGENCY SITUATIONS, AND CERTAIN DE-  
23 FENSIVE CYBERSECURITY QUERIES.—Subsection (b)  
24 shall not apply if—

1           (1) the covered person to whom the covered  
2       query relates is the subject of an order or emergency  
3       authorization authorizing electronic surveillance or  
4       physical search under section 105 or 304 of the For-  
5       eign Intelligence Surveillance Act of 1978 (50  
6       U.S.C. 1805, 1824), or a warrant issued pursuant  
7       to the Federal Rules of Criminal Procedure by a  
8       court of competent jurisdiction if—

9           (A) such order, authorization, or warrant  
10      covers the period of the covered query; and

11          (B) the covered query is conducted and  
12      covered information is accessed in compliance  
13      with all use, dissemination, querying, retention,  
14      and other minimization limitations required by  
15      the order, authorization, or warrant;

16          (2)(A) the officer or employee accessing the  
17      covered information has a reasonable belief that—

18           (i) an emergency exists involving an immi-  
19      nent threat of death or serious bodily harm;  
20      and

21           (ii) in order to prevent or mitigate the  
22      threat described in clause (i), the query must be  
23      conducted before authorization described in  
24      subparagraph (A) can, with due diligence, be  
25      obtained; and

1 (B) not later than 14 days after the covered in-  
2 formation is accessed, a description of the cir-  
3 cumstances justifying the accessing of the covered  
4 information is provided to the congressional intel-  
5 ligence committees in a timely manner;

6 (3) the covered person to whom the covered  
7 query relates or, if such person is incapable of pro-  
8 viding consent, a third party legally authorized to  
9 consent on behalf of the person, has provided con-  
10 sent for such access on a case-by-case basis; or

11 (4)(A) the covered information is used for de-  
12 fensive cybersecurity purposes, including the protec-  
13 tion of a covered person from cybersecurity attack;

14 (B) other than for such defensive cybersecurity  
15 purposes, no covered information is accessed or re-  
16 viewed; and

17 (C) not later than 14 days after the covered in-  
18 formation is accessed, a description of the cir-  
19 cumstances justifying the accessing of the covered  
20 information is provided to the congressional intel-  
21 ligence committees.

22 (d) MATTERS RELATING TO EMERGENCY QUE-  
23 RIES.—

24 (1) TREATMENT OF DENIALS.—If covered in-  
25 formation is accessed pursuant to an emergency au-

1       thorization described in subsection (c)(1) and the  
2       subsequent application to authorize electronic sur-  
3       veillance, a physical search, or an acquisition pursu-  
4       ant to section 105(e) or 304(e) of the Foreign Intel-  
5       ligence Surveillance Act of 1978 (50 U.S.C. 1805(e),  
6       1824(e)) is denied, or in any other case in which  
7       covered information is accessed in violation of this  
8       section—

9               (A) no covered information accessed, or  
10              evidence derived from such access, may be used,  
11              received in evidence, or otherwise disseminated  
12              in any investigation, trial, hearing, or other pro-  
13              ceeding in or before any court, grand jury, de-  
14              partment, office, agency, regulatory body, legis-  
15              lative committee, or other authority of the  
16              United States, a State, or political subdivision  
17              thereof; and

18              (B) no covered information accessed, or  
19              evidence derived from such access, concerning a  
20              covered person may subsequently be used or  
21              disclosed in any other manner without the con-  
22              sent of such covered person, except if the Attor-  
23              ney General approves the use or disclosure of  
24              such covered information in order to prevent

1           the death of or serious bodily harm to any per-  
2           son.

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

7           (e) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF  
8           1978.—This section shall not apply to the access of cov-  
9           ered information collected pursuant to the Foreign Intel-  
10          ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

11          (f) FOREIGN INTELLIGENCE PURPOSE REQUIRED  
12          FOR QUERIES.—

13               (1) IN GENERAL.—Except as provided in para-  
14               graph (2), no officer or employee of the Federal  
15               Government may conduct a query unless the query  
16               is—

17                       (A) reasonably likely to retrieve foreign in-  
18                       telligence information; and

19                       (B) made with a significant foreign intel-  
20                       ligence purpose.

21           (2) EXCEPTIONS.—An officer or employee of  
22           the Federal Government is permitted to conduct a  
23           query if an exception described in clauses (i) and (ii)  
24           of section 702(f)(2)(B) of the Foreign Intelligence

1 Surveillance Act of 1978, as amended by section  
2 101, applies.

3 (g) DOCUMENTATION.—No officer or employee of the  
4 Federal Government may conduct a covered query, or ac-  
5 cess covered information returned in response to a covered  
6 query, unless an electronic record is created that in-  
7 cludes—

8 (1) for each query—

9 (A) each term used for the conduct of the  
10 query;

11 (B) the date of the covered query;

12 (C) the identifier of the officer or employee  
13 who conducted the covered query;

14 (D) a statement of facts justifying that it  
15 is reasonably likely to retrieve foreign intel-  
16 ligence information or an exception under sub-  
17 section (f)(2) applies; and

18 (E) a description of the basis for the ex-  
19 ception; and

20 (2) for each access—

21 (A) the date of the access;

22 (B) the identifier of the officer or employee  
23 who did the particular access; and

1 (C) a statement of facts showing that an  
2 access is authorized by an exception under sub-  
3 section (c).

4 (h) QUERY RECORD SYSTEM.—

5 (1) IN GENERAL.—The head of each agency  
6 that may conduct a covered query shall ensure that  
7 a system, mechanism, or business practice is in place  
8 to maintain the records described in subsection (g),  
9 including ensuring that any covered queries, or ac-  
10 cesses to covered information returned in response  
11 to covered queries, that are conducted by automated  
12 means are attributed to the officer or employee who  
13 was the proximate cause of such covered query or  
14 access.

15 (2) COMPLIANCE REPORT.—Not later than 90  
16 days after the date of the enactment of this Act, the  
17 head of each applicable agency shall report to the  
18 congressional intelligence committees on its compli-  
19 ance with paragraph (1).

20 **SEC. 403. PROHIBITION ON REVERSE TARGETING OF**  
21 **UNITED STATES PERSONS AND PERSONS LO-**  
22 **CATED IN THE UNITED STATES.**

23 (a) PROHIBITION ON ACQUISITION.—No officer or  
24 employee of the Federal Government may intentionally  
25 target, for the purpose of acquiring foreign intelligence in-

1 formation, any person to acquire information, regardless  
2 of whether such targeting or acquisition occurs inside or  
3 outside the United States, if a significant purpose of the  
4 acquisition is to acquire the information of a particular,  
5 known covered person, unless—

6 (1)(A) the officer or employee has a reasonable  
7 belief that an emergency exists involving a threat of  
8 imminent death or serious bodily harm to such cov-  
9 ered person;

10 (B) the information is sought for the purpose  
11 of assisting that person; and

12 (C) not later than 14 days after the targeting,  
13 a description of the targeting is provided to the con-  
14 gressional intelligence committees in a timely man-  
15 ner; or

16 (2) the covered person has provided consent to  
17 the targeting, or if such covered person is incapable  
18 of providing consent, a third party legally authorized  
19 to consent on behalf of such covered person has pro-  
20 vided consent.

21 (b) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF  
22 1978 AND CRIMINAL WARRANTS.—This section shall not  
23 apply to—



1 (1) an acquisition carried out pursuant to the  
2 Foreign Intelligence Surveillance Act of 1978 (50  
3 U.S.C. 1801 et seq.); or

4 (2) an acquisition carried out pursuant to a  
5 warrant issued pursuant to the Federal Rules of  
6 Criminal Procedure by a court of competent jurisdic-  
7 tion covering the period of the acquisition and the  
8 acquisition is subject to the use, dissemination,  
9 querying, retention, and other minimization limita-  
10 tions required by such warrant.

11 **SEC. 404. PROHIBITION ON INTELLIGENCE ACQUISITION**  
12 **OF UNITED STATES PERSON DATA.**

13 (a) COVERED DATA DEFINED.—In this section, the  
14 term “covered data” means—

15 (1) data, derived data, or any unique identifier  
16 that is linked to or is reasonably linkable to a cov-  
17 ered person or to an electronic device that is linked  
18 to, or is reasonably linkable to, 1 or more covered  
19 persons in a household;

20 (2) includes anonymized data that, if combined  
21 with other data, can be linked to, or is reasonably  
22 linkable to, a covered person or to an electronic de-  
23 vice that is linked to, or is reasonably linkable to, 1  
24 or more covered persons in a household; and

25 (3) does not include data that—

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

4 (B) is reasonably believed to have been vol-  
5 untarily made available to the general public by  
6 the covered person; or

7 (C) is a specific communication or trans-  
8 action with a targeted individual who is not a  
9 covered person.

10 (b) LIMITATION.—

11 (1) IN GENERAL.—Subject to paragraphs (2)  
12 through (8), an element of the intelligence commu-  
13 nity may not acquire a dataset that includes covered  
14 data.

15 (2) AUTHORIZATION PURSUANT TO THE FOR-  
16 EIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—  
17 An element of the intelligence community may ac-  
18 quire covered data if the data has been authorized  
19 for collection pursuant to an order or emergency au-  
20 thorization pursuant to the Foreign Intelligence Sur-  
21 veillance Act of 1978 (50 U.S.C. 1801 et seq.) or  
22 the Federal Rules of Criminal Procedure by a court  
23 of competent jurisdiction covering the period of the  
24 acquisition, subject to the use, dissemination,

1 querying, retention, and other minimization limita-  
2 tions required by such authorization.

3 (3) AUTHORIZATION FOR EMPLOYMENT-RE-  
4 LATED USE.—An element of the intelligence commu-  
5 nity may acquire covered data about an employee of,  
6 or applicant for employment by, an element of the  
7 intelligence community for employment-related pur-  
8 poses, provided that—

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

11 (B) the covered data is destroyed at such  
12 time as it is no longer necessary for such pur-  
13 poses.

14 (4) EXCEPTION FOR COMPLIANCE PURPOSES.—  
15 An element of the intelligence community may ac-  
16 quire covered data for the purpose of supporting  
17 compliance with collection limitations and minimiza-  
18 tion requirements imposed by statute, guidelines,  
19 procedures, or the United States Constitution, pro-  
20 vided that—

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

23 (B) the covered data is destroyed at such  
24 time as it is no longer necessary for such pur-  
25 pose.

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

4                   (A) there is a reasonable belief that—

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

8                           (ii) in order to prevent or mitigate  
9                           this threat, the acquisition must be con-  
10                          ducted before authorization pursuant to  
11                          paragraph (2) can, with due diligence, be  
12                          obtained;

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

15                   (C) the covered data is destroyed at such  
16                   time as it is no longer necessary for such pur-  
17                   pose; and

18                   (D) not later than 14 days after the acqui-  
19                   sition, a description of the acquisition is pro-  
20                   vided to the congressional intelligence commit-  
21                   tees.

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

1 (A) each covered person linked or reason-  
2 ably linked to the covered data, or, if such per-  
3 son is incapable of providing consent, a third  
4 party legally authorized to consent on behalf of  
5 the person, has provided consent to the acquisi-  
6 tion and use of the data on a case-by-case  
7 basis;

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

11 (C) the covered data is destroyed at such  
12 time as it is no longer necessary for such pur-  
13 poses.

14 (7) EXCEPTION FOR NONSEGREGABLE DATA.—  
15 An element of the intelligence community may ac-  
16 quire a dataset that includes covered data if the cov-  
17 ered data is not reasonably segregable prior to ac-  
18 quisition, provided that the element of the intel-  
19 ligence community complies with the minimization  
20 procedures in subsection (c).

21 (8) EXCEPTION FOR NATIONAL SECURITY LET-  
22 TER DATA.—An element of the intelligence commu-  
23 nity may acquire, through noncompulsory means  
24 that are otherwise not contrary to a provision of  
25 Federal law, data that, in the United States, the

1 Federal Government has the authority to compel  
2 production through a national security letter pursu-  
3 ant to section 2709 of title 18, United States Code,  
4 section 626 or 627 of the Consumer Credit Protec-  
5 tion Act (15 U.S.C. 1681u, 1681v), or section 1114  
6 of the Right to Financial Privacy Act of 1978 (12  
7 U.S.C. 3414), provided—

8 (A) the person or entity in possession of  
9 the data is outside the United States and com-  
10 pelled production is not feasible;

11 (B) the acquisition is conducted consistent  
12 with the limitations that would apply if, in the  
13 United States, the Federal Government com-  
14 pelled production of such data with a national  
15 security letter pursuant to such provisions of  
16 law; and

17 (C) the element of the intelligence commu-  
18 nity maintains all records required by such pro-  
19 visions of law, including the content of relevant  
20 certifications, for each covered person or each  
21 instance of data, derived data or unique identi-  
22 fier linked to or reasonably linkable to a cov-  
23 ered person.

24 (c) MINIMIZATION PROCEDURES.—

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

6           (2) ACQUISITION AND RETENTION.—The proce-  
7       dures adopted under paragraph (1) shall require ele-  
8       ments of the intelligence community to exhaust all  
9       reasonable means—

10           (A) to exclude covered data not subject to  
11       1 or more exceptions set forth in subsection (b)  
12       from datasets prior to acquisition; and

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

18           (3) DESTRUCTION.—The procedures adopted  
19       under paragraph (1) shall require that if an element  
20       of the intelligence community identifies covered data  
21       acquired in violation of subsection (b), such covered  
22       data shall be promptly destroyed.

23           (d) PROHIBITION ON USE OF DATA OBTAINED IN  
24       VIOLATION OF THIS SECTION.—Covered data acquired by  
25       an element of the intelligence community in violation of

1 subsection (b), and any evidence derived therefrom, may  
2 not be used, received in evidence, or otherwise dissemi-  
3 nated in any investigation, trial, hearing, or other pro-  
4 ceeding in or before any court, grand jury, department,  
5 office, agency, regulatory body, legislative committee, or  
6 other authority of the United States, a State, or political  
7 subdivision thereof.

8 (e) REPORTING REQUIREMENT.—

9 (1) IN GENERAL.—Not later than 180 days  
10 after the date of the enactment of this Act and not  
11 less frequently than once each year thereafter, the  
12 Director of National Intelligence shall submit to the  
13 appropriate committees of Congress and the Privacy  
14 and Civil Liberties Oversight Board a report on ac-  
15 quisitions pursuant to this section.

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

18 (A) DATASETS.—A description of datasets  
19 that the Director determines contain informa-  
20 tion of covered persons that is significant in  
21 volume proportion, or sensitivity, including—

22 (i) the covered person information in  
23 each dataset; and

24 (ii) an estimate of the amount of cov-  
25 ered person information in each dataset;



1 (B) DATA COLLECTION.—A description of  
2 data collected pursuant to subsection (b)(8), in-  
3 cluding—

4 (i) a description of the covered person  
5 information for each acquisition; and

6 (ii) the number of covered persons or  
7 instances of data, derived data or unique  
8 identifiers linked to or reasonably linkable  
9 to a covered person, disaggregated by the  
10 national security letter authority for which  
11 compelled production would be required.

12 (C) DETECTED VIOLATIONS.—A descrip-  
13 tion of covered data identified as having been  
14 acquired in violation of subsection (b) in the  
15 preceding year, including—

16 (i) an estimate of the number of cov-  
17 ered persons whose information was ac-  
18 quired in violation of subsection (b); and

19 (ii) any changes made to the proce-  
20 dures in subsection (c) to address compli-  
21 ance issues.

22 (3) NOTIFICATIONS.—After submitting the re-  
23 port required by paragraph (1), the Director shall,  
24 in coordination with the Under Secretary, notify the

1 appropriate committees of Congress of any changes  
2 to the information contained in such report.

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

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

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

10 (f) RULE OF CONSTRUCTION.—Nothing in this sec-  
11 tion shall authorize an acquisition otherwise prohibited by  
12 this Act, the Foreign Intelligence Surveillance Act of 1978  
13 (50 U.S.C. 1801 et seq.), or title 18, United States Code.

14 **SEC. 405. PROHIBITION ON THE WARRANTLESS ACQUISI-**  
15 **TION OF DOMESTIC COMMUNICATIONS.**

16 No officer or employee of the Federal Government  
17 may intentionally acquire, for the purpose of acquiring for-  
18 eign intelligence information, any communication as to  
19 which the sender and all intended recipients are known  
20 to be located in the United States at the time of acquisi-  
21 tion or the time of communication, regardless of whether  
22 such acquisition occurs inside or outside the United  
23 States, except—

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

(2) if—

(A) the officer or employee has a reasonable belief that—

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

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

(B) not later than 14 days after the acquisition, a description of the acquisition is provided to the congressional intelligence committees.

**SEC. 406. DATA RETENTION LIMITS.**

(a) PROCEDURES.—

(1) IN GENERAL.—Each head of an element of the intelligence community shall develop and implement procedures governing the retention of information described in paragraph (2).

1           (2) INFORMATION DESCRIBED.—The informa-  
2           tion described in this paragraph is information that  
3           was acquired for foreign intelligence purposes, other  
4           than acquisitions authorized by the Foreign Intel-  
5           ligence Surveillance Act of 1978 (50 U.S.C. 1801 et  
6           seq.), regardless of whether such acquisition oc-  
7           curred inside or outside the United States.

8           (b) REQUIREMENTS.—

9           (1) COVERED INFORMATION DEFINED.—In this  
10          subsection, the term “covered information” in-  
11          cludes—

12                 (A) any information or communication per-  
13                 taining to a covered person, including an  
14                 encrypted communication to or from a covered  
15                 person, that has been evaluated and is not spe-  
16                 cifically known to contain foreign intelligence  
17                 information; and

18                 (B) any unevaluated information, unless it  
19                 can reasonably be determined that the  
20                 unevaluated information does not contain any  
21                 information or communications pertaining to a  
22                 covered person, including any encrypted com-  
23                 munication to or from a covered person.

24          (2) IN GENERAL.—The procedures developed  
25          and implemented pursuant to subsection (a) shall

1 ensure, with respect to information described in such  
2 subsection, that covered information shall be de-  
3 stroyed within 5 years of collection unless the Attor-  
4 ney General determines in writing that—

5 (A) the information is the subject of a  
6 preservation obligation in pending administra-  
7 tive, civil, or criminal litigation, in which case  
8 the covered information shall be segregated, re-  
9 tained, and used solely for that purpose and  
10 shall be destroyed as soon as it is no longer re-  
11 quired to be preserved for such litigation; or

12 (B) the information is being used in a pro-  
13 ceeding or investigation consistent with section  
14 706(a) of the Foreign Intelligence Surveillance  
15 Act of 1978 (50 U.S.C. 1881e(a)).

16 **SEC. 407. REPORTS ON VIOLATIONS OF LAW OR EXECUTIVE**  
17 **ORDER.**

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

21 “(c) PUBLIC AVAILABILITY.—

22 “(1) IN GENERAL.—The Director of National  
23 Intelligence shall make each report submitted under  
24 subsection (a) publicly available on an internet

1 website, with such redactions as may be necessary to  
 2 protect sources and methods.

3 “(2) RETROACTIVE REPORT PUBLICATION.—

4 With respect to a report submitted under subsection  
 5 (a) prior to the date of the enactment of the Govern-  
 6 ment Surveillance Reform Act of 2026, such report  
 7 shall be made publicly available pursuant to para-  
 8 graph (1) by not later than 180 days after the date  
 9 of the enactment of such Act.

10 “(d) DEPARTMENT OF JUSTICE REPORT.—The At-  
 11 torney General, in consultation with the Director of Na-  
 12 tional Intelligence, shall submit to the Committee on the  
 13 Judiciary of the Senate and the Committee on the Judici-  
 14 ary of the House of Representatives a version of the report  
 15 described in subsection (a) that only addresses violations  
 16 of the Foreign Intelligence Surveillance Act of 1978 (50  
 17 U.S.C. 1801 et seq.).”.

## 18 **TITLE V—INDEPENDENT** 19 **OVERSIGHT**

### 20 **SEC. 501. INSPECTOR GENERAL OVERSIGHT OF ORDERS** 21 **UNDER THE FOREIGN INTELLIGENCE SUR-** 22 **VEILLANCE ACT OF 1978.**

23 (a) AUDIT.—Not later than 1 year after the date of  
 24 the enactment of this Act, the Inspector General of the  
 25 Department of Justice and the Inspector General of each

1 element of the intelligence community shall each initiate  
2 an audit of the applications for court orders made under  
3 the Foreign Intelligence Surveillance Act of 1978 (50  
4 U.S.C. 1801 et seq.) and directives issued under section  
5 702(i) of such Act by the Department or the element, re-  
6 spectively.

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

9 (1) an Inspector General shall—

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

14 (B) assess whether—

15 (i) adequate safeguards are in place to  
16 ensure that the assertions made in applica-  
17 tions are scrupulously accurate;

18 (ii) adequate safeguards are in place  
19 to ensure that each application includes all  
20 information required by the amendments  
21 made by section 10 of the Reforming Intel-  
22 ligence and Securing America Act (Public  
23 Law 118–49) and made by sections 302  
24 and 303 of this Act; and

1 (iii) in the determination of the In-  
2 spector General, there are any other areas  
3 of potential risk or violation; and

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

7 (2) the Inspector General of the Department of  
8 Justice shall assess the information provided by the  
9 Department of Justice under subsection (f) of sec-  
10 tion 603 of the Foreign Intelligence Surveillance Act  
11 of 1978 (50 U.S.C. 1873), as added by section 803  
12 of this Act, and include a determination on the accu-  
13 racy and completeness of the information provided  
14 under that section.

15 (c) REPORT.—

16 (1) IN GENERAL.—For each audit conducted by  
17 an Inspector General under subsection (a), such In-  
18 spector General shall submit to the persons specified  
19 in paragraph (2) a report of the audit, including  
20 findings and recommendations of the Inspector Gen-  
21 eral and any remediations taken by the Department  
22 or element, respectively.

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

25 (A) The Attorney General.



1 (B) The Director of National Intelligence.

2 (C) The Privacy and Civil Liberties Over-  
3 sight Board.

4 (D) The appropriate committees of Con-  
5 gress.

6 (E) The Foreign Intelligence Surveillance  
7 Court (as defined in section 601(e) of the For-  
8 eign Intelligence Surveillance Act of 1978 (50  
9 U.S.C. 1871(e))).

10 (F) Any amicus curiae appointed under  
11 section 103(i)(2) of the Foreign Intelligence  
12 Surveillance Act of 1978 (50 U.S.C.  
13 1803(i)(2)).

14 (d) COOPERATION.—The Attorney General and head  
15 of each element of the intelligence community shall ensure  
16 full and complete cooperation with the respective Inspector  
17 General conducting an audit under subsection (a), includ-  
18 ing by providing access to all evidence and information  
19 relevant to the assessments required under subsection  
20 (b)(2), subject to such procedures as are necessary to pro-  
21 tect the national security of the United States.

22 (e) AVAILABILITY TO THE PUBLIC.—The Inspector  
23 General of each element of the intelligence community  
24 shall each make publicly available on a website of the rel-  
25 evant element an unclassified version of any report sub-

mitted under subsection (c) by the respective Inspector General.

**SEC. 502. INTELLIGENCE COMMUNITY PARITY AND COMMUNICATIONS WITH PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.**

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

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

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

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

1 section may exceed the highest amount paid by any ele-  
 2 ment of the intelligence community for a comparable posi-  
 3 tion, based on salary information provided to the chairman  
 4 of the Board by the Director of National Intelligence.”.

5 **SEC. 503. CONGRESSIONAL OVERSIGHT OF GRANTS OF IM-**  
 6 **MUNITY BY THE ATTORNEY GENERAL FOR**  
 7 **WARRANTLESS SURVEILLANCE ASSISTANCE.**

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

11 “(iv) Not later than 30 days after providing a certifi-  
 12 cation described in clause (B) of the first sentence of sub-  
 13 paragraph (ii) to a provider of wire or electronic commu-  
 14 nication service, an officer, employee, or agent thereof, a  
 15 landlord, a custodian, or another person, the person pro-  
 16 viding the certification shall submit the certification to the  
 17 appropriate committees of Congress, as defined in section  
 18 101 of the Foreign Intelligence Surveillance Act of 1978  
 19 (50 U.S.C. 1801).”.

20 (b) ONGOING PROGRAMS.—

21 (1) DEFINITIONS.—In this subsection—

22 (A) the term “appropriate committees of  
 23 Congress” has the meaning given that term in  
 24 section 101 of the Foreign Intelligence Surveil-

1           lance Act of 1978 (50 U.S.C. 1801), as amend-  
2           ed by section 2 of this Act;

3           (B) the terms “electronic communication”,  
4           “electronic communication service”, and “wire  
5           communication” have the meanings given such  
6           terms in section 2510 of title 18, United States  
7           Code; and

8           (C) the term “ongoing certification” means  
9           a certification described in clause (B) of the  
10          first sentence of section 2511(2)(a)(ii) of title  
11          18, United States Code, pursuant to which a  
12          provider of wire or electronic communication  
13          service, an officer, employee, or agent thereof,  
14          a landlord, a custodian, or another person is  
15          providing information, facilities, or technical as-  
16          sistance on the date of enactment of this Act.

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

1 **TITLE VI—REFORMS TO THE**  
2 **ELECTRONIC COMMUNICA-**  
3 **TIONS PRIVACY ACT OF 1986**

4 **SEC. 601. WARRANT PROTECTIONS FOR LOCATION INFOR-**  
5 **MATION, WEB BROWSING RECORDS, AND**  
6 **SEARCH QUERY RECORDS.**

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

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

11 (A) in subsection (a)—

12 (i) in the subsection heading, by strik-  
13 ing “CONTENTS OF WIRE OR ELECTRONIC  
14 COMMUNICATIONS” and inserting “LOCA-  
15 TION INFORMATION, WEB BROWSING  
16 RECORDS, SEARCH QUERY RECORDS, OR  
17 CONTENTS OF WIRE OR ELECTRONIC  
18 COMMUNICATIONS”; and

19 (ii) in the first sentence, by inserting  
20 “location information, a web browsing  
21 record, a search query record, or” before  
22 “the contents of a wire”; and

23 (B) in subsection (c)(1), in the matter pre-  
24 ceding subparagraph (A), by inserting “location

1 information, a web browsing record, a search  
2 query record, or” before “the contents”.

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

5 (A) in the matter preceding paragraph (1),  
6 by inserting “(a) IN GENERAL.—” before “As  
7 used”;

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

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

11 (ii) in paragraph (4), by striking the  
12 period at the end and inserting a semi-  
13 colon; and

14 (iii) by adding at the end the fol-  
15 lowing:

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

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

22 “(A) means a record that reveals, in part  
23 or in whole, the identity of a service provided  
24 by an online service provider, or the identity of  
25 a customer, subscriber, user, or device, for any

1 attempted or successful communication or  
2 transmission between an online service provider  
3 and such a customer, subscriber, user, or de-  
4 vice;

5 “(B) includes a record that reveals, in part  
6 or in whole—

7 “(i) the domain name, uniform re-  
8 source locator, internet protocol address,  
9 or other identifier for a service provided by  
10 an online service provider with which a  
11 customer, subscriber, user, or device has  
12 exchanged or attempted to exchange a  
13 communication or transmission; or

14 “(ii) the network traffic generated by  
15 an attempted or successful communication  
16 or transmission between a service provided  
17 by an online service provider and a cus-  
18 tomer, subscriber, user, or device; and

19 “(C) does not include a record that reveals  
20 information about an attempted or successful  
21 communication or transmission between a  
22 known service and a particular known cus-  
23 tomer, subscriber, user, or device, if the record  
24 is maintained by the known service and is lim-  
25 ited to revealing additional identifying informa-

1           tion about the particular known customer, sub-  
2           scriber, user, or device; and

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

4                 “(A) means a record that reveals a query  
5           term or instruction submitted, in written,  
6           verbal, or other format, by a customer, sub-  
7           scriber, user, or device to any service provided  
8           by an online service provider, including a search  
9           engine, voice assistant, chat bot, or navigation  
10          service; and

11                “(B) includes a record that reveals the re-  
12          sponse provided by any service provided by an  
13          online service provider to a query term or in-  
14          struction by a customer, subscriber, user, or de-  
15          vice.”; and

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

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

21                “(1) The contents of a communication.

22                “(2) Location information.

23                “(3) A web browsing record.

24                “(4) A search query record.”.



1 (b) REAL-TIME SURVEILLANCE OF LOCATION IN-  
2 FORMATION.—Section 3117 of title 18, United States  
3 Code, is amended—

4 (1) in the section heading, by striking “**Mo-**  
5 **bile tracking devices**” and inserting “**Track-**  
6 **ing orders for Federal departments and**  
7 **agencies**”;

8 (2) by striking subsection (b);

9 (3) by redesignating subsection (a) as sub-  
10 section (c);

11 (4) by inserting before subsection (c), as so re-  
12 designated, the following:

13 “(a) IN GENERAL.—No officer or employee of a gov-  
14 ernmental entity may install or direct the installation of  
15 a tracking device, except pursuant to a warrant issued  
16 using the procedures described in the Federal Rules of  
17 Criminal Procedure (or, in the case of a State court,  
18 issued using State warrant procedures and, in the case  
19 of a court-martial or other proceeding under chapter 47  
20 of title 10 (the Uniform Code of Military Justice), issued  
21 under section 846 of that title, in accordance with regula-  
22 tions prescribed by the President) by a court of competent  
23 jurisdiction.

24 “(b) EMERGENCIES.—

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

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

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

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

15           “(3) TERMINATION ABSENT WARRANT.—In the  
16           absence of a warrant, use of a tracking device under  
17           the authority under paragraph (1) shall immediately  
18           terminate when the investigative information sought  
19           is obtained or when the application for the warrant  
20           is denied, whichever is earlier.

21           “(4) LIMITATION.—In the event an application  
22           for a warrant described in paragraph (2) is denied,  
23           or in any other case where the use of a tracking de-  
24           vice under the authority under paragraph (1) is ter-  
25           minated without a warrant having been issued, the

1 information obtained shall be treated as having been  
2 obtained in violation of this section, and an inven-  
3 tory describing the installation and use of the track-  
4 ing device shall be served on the person named in  
5 the warrant application.”;

6 (5) in subsection (c), as so redesignated—

7 (A) in the subsection heading, by striking  
8 “IN GENERAL” and inserting “JURISDICTION”;

9 (B) by striking “or other order”;

10 (C) by striking “mobile”;

11 (D) by striking “such order” and inserting  
12 “such warrant”; and

13 (E) by adding at the end the following:

14 “For purposes of this subsection, the installa-  
15 tion of a tracking device occurs within the juris-  
16 diction in which the device is physically located  
17 when the installation is complete.”; and

18 (6) by adding at the end the following:

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

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

22 “(2) the term ‘court of competent jurisdiction’  
23 has the meaning given that term in section 2711;

24 “(3) the term ‘governmental entity’—

1           “(A) means a department or agency of the  
2           United States; and

3           “(B) does not include a department or  
4           agency of a State or a political subdivision  
5           thereof.

6           “(4) the term ‘installation of a tracking device’  
7           means, whether performed by an officer or employee  
8           of a governmental entity or by a provider at the di-  
9           rection of a governmental entity—

10           “(A) the physical placement of a tracking  
11           device;

12           “(B) the remote activation of the tracking  
13           software or functionality of a tracking device; or

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

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

22           (c) PROSPECTIVE SURVEILLANCE OF WEB BROWS-  
23           ING RECORDS AND LOCATION INFORMATION.—Section  
24           2703 of title 18, United States Code, is amended by add-  
25           ing at the end the following:

1       “(i) PROSPECTIVE DISCLOSURE OF WEB BROWSING  
2 RECORDS.—

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

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

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

1 **SEC. 602. 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. 603. 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  
10 (1)—

11 (i) by striking “divulge” and inserting  
12 “disclose”; and

13 (ii) by inserting “wire or electronic”  
14 before “communication”;

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

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

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

1 “(3) with the lawful consent of the originator,  
 2 addressee, or intended recipient of such communica-  
 3 tion, or of the subscriber or customer on whose be-  
 4 half the provider stores, holds, or maintains such  
 5 communication;”; and

6 (3) in subsection (c)—

7 (A) in the matter preceding paragraph  
 8 (1)—

9 (i) by striking “divulge” and inserting  
 10 “disclose”; and

11 (ii) by inserting “wire or electronic”  
 12 before “communications”; and

13 (B) by amending paragraph (2) to read as  
 14 follows:

15 “(2) with the lawful consent of the subscriber  
 16 or customer;”.

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

20 (1) in subsection (a), in the first sentence—

21 (A) by striking “A governmental entity”  
 22 and inserting “Except as provided in sub-  
 23 sections (l) and (m), a governmental entity”;

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



1 (C) by striking “by a court of competent  
2 jurisdiction.” and inserting “that is issued by a  
3 court of competent jurisdiction and that may  
4 indicate the date by which the provider must  
5 make the disclosure to the governmental entity.  
6 In the absence of a date on the warrant indi-  
7 cating the date by which the provider must  
8 make disclosure to the governmental entity, the  
9 provider shall promptly respond to the war-  
10 rant.”;

11 (2) in subsection (c)—

12 (A) in paragraph (1)—

13 (i) in the matter preceding subpara-  
14 graph (A)—

15 (I) by striking “A governmental  
16 entity” and inserting “Except as pro-  
17 vided in subsections (l) and (m), a  
18 governmental entity”; and

19 (II) by striking “only when the  
20 governmental entity—” and inserting  
21 “only—”;

22 (ii) in subparagraph (A)—

23 (I) by striking “obtains a war-  
24 rant issued” and inserting “if the gov-  
25 ernmental entity obtains a warrant”;

- 1 (II) by striking “by the Presi-  
2 dent) by a court” and inserting the  
3 following: “by the President) that—  
4 “(i) is issued by a court”;
- 5 (III) by inserting “and” after  
6 “jurisdiction;”; and
- 7 (IV) by adding at the end the fol-  
8 lowing:
- 9 “(ii) may indicate the date by which the  
10 online service provider must make the disclo-  
11 sure to the governmental entity;”;
- 12 (iii) in subparagraph (B), by inserting  
13 “if the governmental entity” before “ob-  
14 tains”;
- 15 (iv) in subparagraph (C), by striking  
16 “has the consent of the subscriber or cus-  
17 tomer to such disclosure;” and inserting  
18 “with the lawful consent of the subscriber  
19 or customer; or”;
- 20 (v) by striking subparagraph (D);
- 21 (vi) by redesignating subparagraph  
22 (E) as subparagraph (D); and
- 23 (vii) in subparagraph (D), as so reded-  
24 ignated, by striking “seeks information”

1 and inserting “as otherwise authorized”;

2 and

3 (B) in paragraph (2)—

4 (i) in the matter preceding subpara-  
5 graph (A), by inserting “, in response to  
6 an administrative subpoena authorized by  
7 Federal or State statute, a grand jury,  
8 trial, or civil discovery subpoena, or any  
9 means available under paragraph (1),”  
10 after “shall”; and

11 (ii) in the matter following subpara-  
12 graph (F), by striking “of a subscriber”  
13 and all that follows and inserting “of a  
14 subscriber or customer of such online serv-  
15 ice provider.”;

16 (3) in subsection (d)—

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

19 (B) by striking “sought,” and inserting  
20 “sought”; and

21 (C) by striking “section” and inserting  
22 “subsection”; and

23 (4) by adding after subsection (j), as added by  
24 section 601(c) of this Act, the following:

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

5       “(l) RULE OF CONSTRUCTION RELATED TO LEGAL  
6 PROCESS.—Nothing in this section or in section 2702  
7 shall modify the authorities for a governmental entity to  
8 obtain a wire or electronic communication (including the  
9 contents of that communication) from a provider of a re-  
10 mote computing service or electronic communication serv-  
11 ice if—

12               “(1) the originator, addressee, or intended re-  
13 cipient of such communication is an officer, director,  
14 employee, or agent of the provider acting in their ca-  
15 pacity as such an officer, director, employee, or  
16 agent; or

17               “(2) the communication—

18                       “(A) advertises or promotes a product or  
19 service; and

20                       “(B) has been made readily available to  
21 the general public.

22       “(m) RULE OF CONSTRUCTION RELATED TO CON-  
23 GRESSIONAL SUBPOENAS.—Nothing in this section or in  
24 section 2702 shall limit the power of inquiry vested in the

1 Congress by article I of the Constitution of the United  
2 States.”.

3 (d) WARRANT REQUIREMENT FOR STORED COMMU-  
4 NICATIONS CONTENT.—Section 2703 of title 18, United  
5 States Code, is amended—

6 (1) in subsection (a)—

7 (A) by striking “, that is in electronic stor-  
8 age in an electronic communications system for  
9 one hundred and eighty days or less,”; and

10 (B) by striking the last sentence;

11 (2) by striking subsection (b) and inserting the  
12 following:

13 “(b) [Repealed].”; and

14 (3) in subsection (d) by striking “(b) or”.

15 **SEC. 604. CONSISTENT PROTECTIONS FOR DEMANDS FOR**  
16 **DATA HELD BY INTERACTIVE COMPUTING**  
17 **SERVICES.**

18 (a) DEFINITION.—Subsection (a) of section 2711 of  
19 title 18, United States Code, as so designated and amend-  
20 ed by section 601 of this Act, is amended by adding at  
21 the end the following:

22 “(8) the term ‘online service provider’ means a  
23 provider of electronic communication service, a pro-  
24 vider of remote computing service, or a provider of  
25 an interactive computer service (as defined in section

1       230(f) of the Communications Act of 1934 (47  
2       U.S.C. 230(f)); and”.

3       (b) REQUIRED DISCLOSURE.—Section 2703 of title  
4 18, United States Code, is amended—

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

8           (2) in subsection (c)—

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

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

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

1 **SEC. 605. CONSISTENT PROTECTIONS FROM FEDERAL LAW**  
2 **ENFORCEMENT FOR REAL-TIME AND HISTOR-**  
3 **ICAL METADATA.**

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

6 (1) in section 3122(b), by striking paragraph  
7 (2) and inserting the following:

8 “(2)(A) for an application submitted by an at-  
9 torney for the Government, a certification by the ap-  
10 plicant providing specific and articulable facts show-  
11 ing there are reasonable grounds to believe that the  
12 information likely to be obtained is relevant and ma-  
13 terial to an ongoing criminal investigation being con-  
14 ducted by that agency; or”; and

15 (2) in section 3123(a)(1), in the first sen-  
16 tence—

17 (A) by striking “the court shall enter” and  
18 inserting “the court may enter”; and

19 (B) by striking “certified to the court that  
20 the information likely to be obtained by such in-  
21 stallation and use is relevant” and inserting  
22 “submitted a certification providing specific and  
23 articulable facts showing there are reasonable  
24 grounds to believe that the information likely to  
25 be obtained by such installation and use is rel-  
26 evant and material”.

1 **SEC. 606. SUBPOENAS FOR CERTAIN SUBSCRIBER INFOR-**  
2 **MATION.**

3 Section 2703(c)(2) of title 18, United States Code,  
4 is amended, in the matter following subparagraph (F), as  
5 amended by section 603(c) of this Act, by inserting “with  
6 respect to whom the governmental entity identifies the  
7 name, address, temporarily assigned network address, or  
8 account identifier (such as a user name)” before the pe-  
9 riod at the end.

10 **SEC. 607. MINIMIZATION STANDARDS FOR VOLUNTARY DIS-**  
11 **CLOSURE OF CUSTOMER COMMUNICATIONS**  
12 **OR RECORDS.**

13 (a) IN GENERAL.—Not later than 180 days after the  
14 date of enactment of this Act, the Attorney General shall  
15 issue and make publicly available minimization procedures  
16 applicable to disclosures to a Federal agency under para-  
17 graph (5) or (8) of subsection (b) or paragraph (3) or  
18 (4) of subsection (c) of section 2702 of title 18, United  
19 States Code.

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

22 (1) limit, to the greatest extent possible, the ac-  
23 quisition, use, and dissemination of the contents of  
24 communication and records and other information to  
25 that which is required for the specific purpose for  
26 which the disclosure was intended;



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

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

8           (4) ensure that no contents of communications  
9           or records or other information are retained by the  
10          agency to which the disclosure was made, or any  
11          agency to which the contents of communications or  
12          records or other information were disclosed, after  
13          the completion of the investigation or action for  
14          which the disclosure was intended.

15 **SEC. 608. CONSISTENT PRIVACY PROTECTIONS FOR DATA**  
16 **HELD BY DATA BROKERS.**

17          Section 2703 of title 18, United States Code, as  
18          amended by section 603 of this Act, is amended by adding  
19          at the end the following:

20          “(n) COVERED PERSONAL DATA.—

21                 “(1) DEFINITIONS.—In this subsection, the  
22          terms ‘covered personal data’ and ‘covered organiza-  
23          tion’ have the meanings given such terms in section  
24          2702(e).

1           “(2) LIMITATION.—Unless a governmental enti-  
2           ty obtains an order in accordance with paragraph  
3           (3), the governmental entity may not require a cov-  
4           ered organization that is not an online service pro-  
5           vider to disclose covered personal data if a court  
6           order would be required for the governmental entity  
7           to require an online service provider to disclose such  
8           covered personal data that is a record of a customer  
9           or subscriber of the online service provider.

10           “(3) ORDERS.—

11                   “(A) IN GENERAL.—A court may only  
12                   issue an order requiring a covered organization  
13                   that is not an online service provider to disclose  
14                   covered personal data on the same basis and  
15                   subject to the same limitations as would apply  
16                   to a court order to require disclosure by an on-  
17                   line service provider.

18                   “(B) STANDARD.—For purposes of sub-  
19                   paragraph (A), a court shall apply the most  
20                   stringent standard under Federal statute or the  
21                   Constitution of the United States that would be  
22                   applicable to a request for a court order to re-  
23                   quire a comparable disclosure by an online serv-  
24                   ice provider of comparable records of a cus-

1           tomer or subscriber of the online service pro-  
2           vider.”.

3 **SEC. 609. PROTECTION OF DATA ENTRUSTED TO INTER-**  
4 **MEDIARY OR ANCILLARY SERVICE PRO-**  
5 **VIDERS.**

6           (a) DEFINITION.—Subsection (a) of section 2711 of  
7 title 18, United States Code, as so designated and amend-  
8 ed by sections 601 and 604 of this Act, is amended by  
9 adding at the end the following:

10           “(9) the term ‘intermediary or ancillary service  
11       provider’ means an entity or facilities owner or oper-  
12       ator that directly or indirectly delivers, transmits,  
13       stores, or processes communications or any other  
14       covered personal data (as defined in section 2702(e)  
15       of this title) for, or on behalf of, an online service  
16       provider.”.

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

19           (1) in paragraph (1), by striking “and” at the  
20       end;

21           (2) in paragraph (2)(B), by striking “and” at  
22       the end;

23           (3) in paragraph (3), by striking the period at  
24       the end and inserting “; and”; and

25           (4) by adding at the end the following:

1 “(4) an intermediary or ancillary service pro-  
 2 vider may not knowingly disclose—

3 “(A) to any person or entity the contents  
 4 of a communication while in electronic storage  
 5 by that intermediary or ancillary service pro-  
 6 vider; or

7 “(B) to any governmental entity a record  
 8 or other information pertaining to a subscriber  
 9 to or customer of, a recipient of a communica-  
 10 tion from a subscriber to or customer of, or the  
 11 sender of a communication to a subscriber to or  
 12 customer of, the online service provider for, or  
 13 on behalf of, which the intermediary or ancil-  
 14 lary service provider directly or indirectly deliv-  
 15 ers, transmits, stores, or processes communica-  
 16 tions or any other covered personal data (as de-  
 17 fined in subsection (e)).”.

18 **SEC. 610. MODERNIZING CRIMINAL SURVEILLANCE RE-**  
 19 **PORTS.**

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

22 (1) **IN GENERAL.**—Section 2703 of title 18,  
 23 United States Code, as amended by section 608 of  
 24 this Act, is amended by adding at the end the fol-  
 25 lowing:

1       “(o) REPORTS CONCERNING ACCESS TO CUSTOMER  
2 COMMUNICATIONS OR RECORDS.—

3               “(1) IN GENERAL.—In January of each year,  
4 any judge who has issued an order under this sec-  
5 tion or a warrant to obtain records described in this  
6 section, or who has denied approval of an application  
7 under this section during the preceding year, shall  
8 report to the Administrative Office of the United  
9 States Courts—

10               “(A) the fact that the order or warrant  
11 was applied for;

12               “(B) the type of records sought in the  
13 order or warrant;

14               “(C) whether the order or warrant was—

15                       “(i) granted as applied for;

16                       “(ii) granted as modified; or

17                       “(iii) denied;

18               “(D) the subsection of this section under  
19 which the application for the order or warrant  
20 was filed;

21               “(E) the nature of the offense or criminal  
22 investigation that was the basis for the applica-  
23 tion for the order or warrant;

24               “(F) the name of each provider of elec-  
25 tronic communication service or remote com-

1           puting service served with the order or warrant,  
2           if so granted; and

3           “(G) the investigative or law enforcement  
4           agency that submitted the application.

5           “(2) PUBLIC REPORT.—In June of each year,  
6           the Director of the Administrative Office of the  
7           United States Courts shall publish on the website of  
8           the Administrative Office of the United States  
9           Courts and include in the report required under sec-  
10          tion 2519(3)—

11           “(A) a full and complete report concerning  
12           the number of applications for orders or war-  
13           rants requiring the disclosure of, during the  
14           preceding calendar year—

15           “(i) the contents of wire or electronic  
16           communications in electronic storage under  
17           subsection (a); and

18           “(ii) records concerning electronic  
19           communication service or remote computer  
20           service under subsection (c);

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

24           “(C) a detailed summary and analysis of  
25           each category of data required to be filed with

1 the Administrative Office of the United States  
2 Courts under paragraph (1).

3 “(3) FORMAT.—Not later than 180 days after  
4 the date of enactment of the Government Surveil-  
5 lance Reform Act of 2026, the Director of the Ad-  
6 ministrative Office of the United States Courts shall,  
7 in consultation with the National Institute of Stand-  
8 ards and Technology, the Administrator of General  
9 Services, the Electronic Public Access Public User  
10 Group, private entities offering electronic case man-  
11 agement software, the National Center for State  
12 Courts, and the National American Indian Court  
13 Judges Association, publish a machine readable form  
14 that shall be used for any report required under  
15 paragraph (1).

16 “(4) REGULATIONS.—The Director of the Ad-  
17 ministrative Office of the United States Courts may  
18 issue binding regulations with respect to the content  
19 and form of the reports required under paragraph  
20 (1).”.

21 (2) TECHNICAL AND CONFORMING AMEND-  
22 MENT.—Section 2519(3) of title 18, United States  
23 Code, is amended, in the first sentence, by inserting  
24 “publish on the website of the Administrative Office  
25 of the United States Courts and” before “transmit”.

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

4 **“§ 3126. Reports concerning pen registers and trap**  
5 **and trace devices**

6 “(a) IN GENERAL.—In January of each year, any  
7 judge who has issued an order (or an extension thereof)  
8 under section 3123 that expired during the preceding  
9 year, or who has denied approval of an installation and  
10 use of a pen register or trap and trace device during that  
11 year, shall report to the Administrative Office of the  
12 United States Courts—

13 “(1) the fact that an order or extension was ap-  
14 plied for;

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

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

18 “(4) the period of installation and use of a pen  
19 register or trap and trace device authorized by the  
20 order, and the number and duration of any exten-  
21 sions of the order;

22 “(5) the offense specified in the order or appli-  
23 cation, or extension of an order;



1           “(6) the precise nature of the facilities affected  
2           and the precise nature of the information sought;  
3           and

4           “(7) the investigative or law enforcement agen-  
5           cy that submitted the application.

6           “(b) PUBLIC REPORT.—In June of each year, the Di-  
7           rector of the Administrative Office of the United States  
8           Courts shall publish on the website of the Administrative  
9           Office of the United States Courts and include in the re-  
10          port required under section 2519(3)—

11           “(1) a full and complete report concerning—

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

16                   “(B) the number of orders and extensions  
17                   granted or denied pursuant to this chapter dur-  
18                   ing the preceding calendar year; and

19           “(2) a detailed summary and analysis of each  
20           category of data required to be reported under sub-  
21           section (a).

22           “(c) FORMAT.—Not later than 180 days after the  
23           date of enactment of the Government Surveillance Reform  
24           Act of 2026, the Director of the Administrative Office of  
25           the United States Courts shall, in consultation with the

1 National Institute of Standards and Technology and the  
 2 Administrator of General Services, private entities offering  
 3 electronic case management software, the National Center  
 4 for State Courts, and the National American Indian Court  
 5 Judges Association, publish a machine readable form that  
 6 shall be used for any report required under subsection (a).

7 “(d) REGULATIONS.—The Director of the Adminis-  
 8 trative Office of the United States Courts may issue bind-  
 9 ing regulations with respect to the content and form of  
 10 the reports required under subsection (a).”.

11 (c) REPORTING OF VOLUNTARY DISCLOSURES.—Sec-  
 12 tion 2702(d) of title 18, United States Code, is amended—

13 (1) in the heading, by striking “EMERGENCY”  
 14 and inserting “VOLUNTARY”;

15 (2) in the matter preceding paragraph (1), by  
 16 inserting “and publish on the website of the Depart-  
 17 ment of Justice” after “Senate”;

18 (3) in paragraph (1)—

19 (A) by striking “the Department of Jus-  
 20 tice” and inserting “each Federal agency”; and

21 (B) by striking “subsection (b)(8)” and in-  
 22 serting “paragraph (5) or (8) of subsection (b)  
 23 or paragraph (3) or (4) of subsection (c), bro-  
 24 ken down by each such paragraph”;

25 (4) in paragraph (2)(A)—

1 (A) by striking “Department of Justice”  
 2 and inserting “Federal agency”; and  
 3 (B) by striking “subsection (b)(8)” and in-  
 4 serting “paragraph (5) or (8) of subsection (b)  
 5 or paragraph (3) or (4) of subsection (c)”; and  
 6 (5) by striking paragraph (3).

7 **SEC. 611. LIMITATION OF AMENDMENTS TO FEDERAL DE-**  
 8 **PARTMENTS AND AGENCIES.**

9 (a) IN GENERAL.—

10 (1) VOLUNTARY DISCLOSURE.—

11 (A) IN GENERAL.—Section 2702 of title  
 12 18, United States Code, is amended by adding  
 13 after subsection (g), as added by section 201 of  
 14 this Act, the following:

15 “(h) SPECIAL PROCEDURES FOR VOLUNTARY DIS-  
 16 CLOSURE TO NON-FEDERAL ENTITIES.—

17 “(1) IN GENERAL.—The prohibitions in sub-  
 18 section (a) shall not apply to disclosures to a State  
 19 or local governmental entity.

20 “(2) SPECIFIC PROHIBITIONS.—Except as pro-  
 21 vided in paragraphs (3) and (4)—

22 “(A) a person or entity providing an elec-  
 23 tronic communication service to the public shall  
 24 not knowingly divulge to a department or agen-  
 25 cy of a State or local government the contents

1 of a communication while in electronic storage  
2 by that service;

3 “(B) a person or entity providing remote  
4 computing service to the public shall not know-  
5 ingly divulge to a department or agency of a  
6 State or local government the contents of any  
7 communication which is carried or maintained  
8 on that service—

9 “(i) on behalf of, and received by  
10 means of electronic transmission from (or  
11 created by means of computer processing  
12 of communications received by means of  
13 electronic transmission from), a subscriber  
14 or customer of such service; and

15 “(ii) solely for the purpose of pro-  
16 viding storage or computer processing serv-  
17 ices to such subscriber or customer, if the  
18 provider is not authorized to access the  
19 contents of any such communications for  
20 purposes of providing any services other  
21 than storage or computer processing; and

22 “(C) a provider of remote computing serv-  
23 ice or electronic communication service to the  
24 public shall not knowingly divulge a record or  
25 other information pertaining to a subscriber to

1 or customer of such service (not including the  
2 contents of communications covered by sub-  
3 paragraph (A) or (B)) to a department or agen-  
4 cy of a State or local government.

5 “(3) EXCEPTIONS FOR DISCLOSURE OF COMMU-  
6 NICATIONS.—A provider described in paragraph (2)  
7 may divulge the contents of a communication—

8 “(A) to an addressee or intended recipient  
9 of such communication or an agent of such ad-  
10 dressee or intended recipient;

11 “(B) as otherwise authorized in section  
12 2517, 2511(2)(a), or 2703A of this title;

13 “(C) with the lawful consent of the origi-  
14 nator or an addressee or intended recipient of  
15 such communication, or the subscriber in the  
16 case of remote computing service;

17 “(D) to a person employed or authorized  
18 or whose facilities are used to forward such  
19 communication to its destination;

20 “(E) as may be necessarily incident to the  
21 rendition of the service or to the protection of  
22 the rights or property of the provider of that  
23 service;

24 “(F) to a law enforcement agency of a  
25 State or local government, if the contents—

1                   “(i) were inadvertently obtained by  
2                   the service provider; and

3                   “(ii) appear to pertain to the commis-  
4                   sion of a crime; or

5                   “(G) to a department or agency of a State  
6                   or local government, if the provider, in good  
7                   faith, believes that an emergency involving dan-  
8                   ger of death or serious physical injury to any  
9                   person requires disclosure without delay of com-  
10                  munications relating to the emergency.

11                  “(4) EXCEPTIONS FOR DISCLOSURE OF CUS-  
12                  TOMER RECORDS.—A provider described in para-  
13                  graph (2) may divulge a record or other information  
14                  pertaining to a subscriber to or a customer of such  
15                  service (not including the contents of communica-  
16                  tions covered by subparagraph (A) or (B) of para-  
17                  graph (2))—

18                         “(A) as otherwise authorized in section  
19                         2703A;

20                         “(B) with the lawful consent of the cus-  
21                         tomer or subscriber;

22                         “(C) as may be necessarily incident to the  
23                         rendition of the service or to the protection of  
24                         the rights or property of the provider of that  
25                         service; or

1           “(D) to a department or agency of a State  
 2           or local government, if the provider, in good  
 3           faith, believes that an emergency involving dan-  
 4           ger of death or serious physical injury to any  
 5           person requires disclosure without delay of in-  
 6           formation relating to the emergency.”.

7           (2) REQUIRED DISCLOSURE.—

8           (A) IN GENERAL.—Section 2703 of title  
 9           18, United States Code is amended—

10           (i) in the section heading, by adding  
 11           **“to Federal departments and**  
 12           **agencies”** at the end; and

13           (ii) by adding after subsection (o), as  
 14           added by section 610 of this Act, the fol-  
 15           lowing:

16           “(p) LIMITATION TO FEDERAL ENTITIES.—Notwith-  
 17           standing section 2711, in this section, the term ‘govern-  
 18           mental entity’—

19           “(1) means a department or agency of the  
 20           United States; and

21           “(2) does not include a department or agency  
 22           of a State or a political subdivision thereof.”.

23           (B) PROCEDURES FOR NON-FEDERAL EN-  
 24           TITIES.—Chapter 121 of title 18, United States

1 Code, is amended by inserting after section  
2 2703 the following:

3 **“§ 2703A. Required disclosure of customer commu-**  
4 **nications or records to State and local de-**  
5 **partments and agencies**

6 “(a) CONTENTS OF WIRE OR ELECTRONIC COMMU-  
7 NICATIONS IN ELECTRONIC STORAGE.—A governmental  
8 entity may require the disclosure by a provider of elec-  
9 tronic communication service of the contents of a wire or  
10 electronic communication, that is in electronic storage in  
11 an electronic communications system for one hundred and  
12 eighty days or less, only pursuant to a warrant issued  
13 using the procedures described in the Federal Rules of  
14 Criminal Procedure (or, in the case of a State court,  
15 issued using State warrant procedures and, in the case  
16 of a court-martial or other proceeding under chapter 47  
17 of title 10 (the Uniform Code of Military Justice), issued  
18 under section 846 of that title, in accordance with regula-  
19 tions prescribed by the President) by a court of competent  
20 jurisdiction. A governmental entity may require the disclo-  
21 sure by a provider of electronic communications services  
22 of the contents of a wire or electronic communication that  
23 has been in electronic storage in an electronic communica-  
24 tions system for more than one hundred and eighty days



1 by the means available under subsection (b) of this sec-  
2 tion.

3 “(b) CONTENTS OF WIRE OR ELECTRONIC COMMU-  
4 NICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A  
5 governmental entity may require a provider of remote  
6 computing service to disclose the contents of any wire or  
7 electronic communication to which this paragraph is made  
8 applicable by paragraph (2) of this subsection—

9 “(A) without required notice to the subscriber  
10 or customer, if the governmental entity obtains a  
11 warrant issued using the procedures described in the  
12 Federal Rules of Criminal Procedure (or, in the case  
13 of a State court, issued using State warrant proce-  
14 dures and, in the case of a court-martial or other  
15 proceeding under chapter 47 of title 10 (the Uni-  
16 form Code of Military Justice), issued under section  
17 846 of that title, in accordance with regulations pre-  
18 scribed by the President) by a court of competent  
19 jurisdiction; or

20 “(B) with prior notice from the governmental  
21 entity to the subscriber or customer if the govern-  
22 mental entity—

23 “(i) uses an administrative subpoena au-  
24 thorized by a Federal or State statute or a Fed-  
25 eral or State grand jury or trial subpoena; or

1                   “(ii) obtains a court order for such dislo-  
2                   sure under subsection (d) of this section;  
3           except that delayed notice may be given pursuant to  
4           section 2705 of this title.

5           “(2) Paragraph (1) is applicable with respect to any  
6   wire or electronic communication that is held or main-  
7   tained on that service—

8                   “(A) on behalf of, and received by means of  
9           electronic transmission from (or created by means of  
10          computer processing of communications received by  
11          means of electronic transmission from), a subscriber  
12          or customer of such remote computing service; and

13                   “(B) solely for the purpose of providing storage  
14          or computer processing services to such subscriber  
15          or customer, if the provider is not authorized to ac-  
16          cess the contents of any such communications for  
17          purposes of providing any services other than stor-  
18          age or computer processing.

19           “(c) RECORDS CONCERNING ELECTRONIC COMMU-  
20   NICATION SERVICE OR REMOTE COMPUTING SERVICE.—

21   (1) A governmental entity may require a provider of elec-  
22   tronic communication service or remote computing service  
23   to disclose a record or other information pertaining to a  
24   subscriber to or customer of such service (not including

1 the contents of communications) only when the govern-  
2 mental entity—

3           “(A) obtains a warrant issued using the proce-  
4 dures described in the Federal Rules of Criminal  
5 Procedure (or, in the case of a State court, issued  
6 using State warrant procedures and, in the case of  
7 a court-martial or other proceeding under chapter  
8 47 of title 10 (the Uniform Code of Military Jus-  
9 tice), issued under section 846 of that title, in ac-  
10 cordance with regulations prescribed by the Presi-  
11 dent) by a court of competent jurisdiction;

12           “(B) obtains a court order for such disclosure  
13 under subsection (d) of this section;

14           “(C) has the consent of the subscriber or cus-  
15 tomer to such disclosure;

16           “(D) submits a formal written request relevant  
17 to a law enforcement investigation concerning tele-  
18 marketing fraud for the name, address, and place of  
19 business of a subscriber or customer of such pro-  
20 vider, which subscriber or customer is engaged in  
21 telemarketing (as such term is defined in section  
22 2325 of this title); or

23           “(E) seeks information under paragraph (2).

1       “(2) A provider of electronic communication service  
2 or remote computing service shall disclose to a govern-  
3 mental entity the—

4               “(A) name;

5               “(B) address;

6               “(C) local and long distance telephone connec-  
7 tion records, or records of session times and dura-  
8 tions;

9               “(D) length of service (including start date)  
10 and types of service utilized;

11               “(E) telephone or instrument number or other  
12 subscriber number or identity, including any tempo-  
13 rarily assigned network address; and

14               “(F) means and source of payment for such  
15 service (including any credit card or bank account  
16 number),

17 of a subscriber to or customer of such service when the  
18 governmental entity uses an administrative subpoena au-  
19 thorized by a Federal or State statute or a Federal or  
20 State grand jury or trial subpoena or any means available  
21 under paragraph (1).

22       “(3) A governmental entity receiving records or infor-  
23 mation under this subsection is not required to provide  
24 notice to a subscriber or customer.

1       “(d) REQUIREMENTS FOR COURT ORDER.—A court  
2 order for disclosure under subsection (b) or (c) may be  
3 issued by any court that is a court of competent jurisdic-  
4 tion and shall issue only if the governmental entity offers  
5 specific and articulable facts showing that there are rea-  
6 sonable grounds to believe that the contents of a wire or  
7 electronic communication, or the records or other informa-  
8 tion sought, are relevant and material to an ongoing crimi-  
9 nal investigation. Such a court order shall not issue if pro-  
10 hibited by the law of the applicable State. A court issuing  
11 an order pursuant to this section, on a motion made  
12 promptly by the service provider, may quash or modify  
13 such order, if the information or records requested are un-  
14 usually voluminous in nature or compliance with such  
15 order otherwise would cause an undue burden on such pro-  
16 vider.

17       “(e) NO CAUSE OF ACTION AGAINST A PROVIDER  
18 DISCLOSING INFORMATION UNDER THIS CHAPTER.—No  
19 cause of action shall lie in any court against any provider  
20 of wire or electronic communication service, its officers,  
21 employees, agents, or other specified persons for providing  
22 information, facilities, or assistance in accordance with the  
23 terms of a court order, warrant, subpoena, statutory au-  
24 thorization, or certification under this chapter.

25       “(f) REQUIREMENT TO PRESERVE EVIDENCE.—

1           “(1) IN GENERAL.—A provider of wire or elec-  
2       tronic communication services or a remote com-  
3       puting service, upon the request of a governmental  
4       entity, shall take all necessary steps to preserve  
5       records and other evidence in its possession pending  
6       the issuance of a court order or other process.

7           “(2) PERIOD OF RETENTION.—Records referred  
8       to in paragraph (1) shall be retained for a period of  
9       90 days, which shall be extended for an additional  
10      90-day period upon a renewed request by the gov-  
11      ernmental entity.

12          “(g) PRESENCE OF OFFICER NOT REQUIRED.—Not-  
13      withstanding section 3105 of this title, the presence of an  
14      officer shall not be required for service or execution of a  
15      search warrant issued in accordance with this chapter re-  
16      quiring disclosure by a provider of electronic communica-  
17      tions service or remote computing service of the contents  
18      of communications or records or other information per-  
19      taining to a subscriber to or customer of such service.

20          “(h) LIMITATION TO NON-FEDERAL ENTITIES.—  
21      Notwithstanding section 2711, in this section, the term  
22      ‘governmental entity’—

23              “(1) means a department or agency of a State  
24      or a political subdivision thereof; and

1           “(2) does not include a department or agency  
2           of the United States.”.

3           (3) TRACKING ORDERS BY DEPARTMENTS AND  
4           AGENCIES OF STATES AND LOCAL GOVERNMENTS.—  
5           Chapter 205 of title 18, United States Code, is  
6           amended by inserting after section 3117 the fol-  
7           lowing:

8   **“§ 3117A. Mobile tracking devices for State and local**  
9           **departments and agencies**

10          “(a) IN GENERAL.—If a court is empowered to issue  
11          a warrant or other order for the installation of a mobile  
12          tracking device, such order may authorize the use of that  
13          device by a department or agency of a State or a political  
14          subdivision of a State within the jurisdiction of the court,  
15          and outside that jurisdiction if the device is installed in  
16          that jurisdiction.

17          “(b) DEFINITION.—As used in this section, the term  
18          ‘tracking device’ means an electronic or mechanical device  
19          which permits the tracking of the movement of a person  
20          or object.”.

21          (4) CONSISTENT PROTECTIONS FROM STATE  
22          AND LOCAL LAW ENFORCEMENT FOR REAL-TIME  
23          AND HISTORICAL METADATA.—Section 3122(b)(2) of  
24          title 18, United States Code, as amended by section

1       605(1) of this Act, is amended by inserting after  
2       subparagraph (A) the following:

3               “(B) for an application submitted by a State  
4       law enforcement or investigative officer, a certifi-  
5       cation by the applicant that the information likely to  
6       be obtained is relevant to an ongoing criminal inves-  
7       tigation being conducted by that agency.”.

8       (b) LIMITATION ON FEDERAL GOVERNMENTAL EN-  
9       TITIES .—

10           (1) IN GENERAL.—A department or agency of  
11       the United States may not obtain or acquire any  
12       communications, data, records, or other information,  
13       or any evidence derived therefrom, from a depart-  
14       ment or agency of a State or a political subdivision  
15       thereof that was obtained or acquired by the depart-  
16       ment or agency of a State or political subdivision  
17       thereof in a manner that would be a violation of  
18       Federal law if obtained or acquired by the depart-  
19       ment or agency of the United States, or in a manner  
20       that would not satisfy the legal standards applicable  
21       to the department or agency of the United States.

22           (2) LIMITATION OF USE AS EVIDENCE.—Com-  
23       munications, data, records, other information, or evi-  
24       dence obtained or acquired in violation of paragraph  
25       (1), and any evidence derived therefrom, may not be



1       used, received in evidence, or otherwise disseminated  
2       by, on behalf of, or upon a motion or other action  
3       by a department or agency of the United States in  
4       any investigation, trial, hearing, or other proceeding  
5       by, in, or before any court, grand jury, department,  
6       officer, agency, regulatory body, legislative com-  
7       mittee, or other authority of the United States, a  
8       State, or a political subdivision thereof.

9               (3) USE BY AGGRIEVED PARTIES.—Nothing in  
10       paragraph (2) shall be construed to limit the use of  
11       any information by a person aggrieved of a violation  
12       of paragraph (1) in connection with any action relat-  
13       ing to such a violation.

14       (c) TECHNICAL AND CONFORMING AMENDMENTS.—

15               (1) HOMELAND SECURITY ACT OF 2002.—The  
16       Homeland Security Act of 2002 (6 U.S.C. 101 et  
17       seq.) is amended—

18                       (A) in section 2207(d)(2) (6 U.S.C.  
19                       657(d)(2)), by striking “section 2702(b)” and  
20                       inserting “subsection (b) or (h) of section 2702,  
21                       as applicable,”; and

22                       (B) in section 2220C(e) (6 U.S.C.  
23                       665i(e)), by striking “section 2702” and insert-  
24                       ing “subsection (b) or (h) of section 2702, as  
25                       applicable,”.

1           (2) CHAPTER 110.—Chapter 110 of title 18,  
2       United States Code, is amended—

3           (A) in section 2258A(g)(4), by inserting  
4       “or subparagraphs (C) through (G) of section  
5       2702(h)(3), as applicable” after “section  
6       2702(b)”; and

7           (B) in section 2258B—

8           (i) in subsection (b)(2)(C), by striking  
9       “sections 2258A, 2258C, 2702, or 2703”  
10      and inserting “section 2258A, section  
11      2258C, subsection (b) or (h) of section  
12      2702 (as applicable), or section 2703 or  
13      2703A (as applicable)”; and

14          (ii) in subsection (d)(2)(B)(iii)(II), by  
15      striking “sections 2258A, 2258C, 2702, or  
16      2703” and inserting “section 2258A, sec-  
17      tion 2258C, subsection (b) or (h) of section  
18      2702 (as applicable), or section 2703 or  
19      2703A (as applicable)”.

20          (3) CHAPTER 121.—Chapter 121 of title 18,  
21      United States Code, is amended—

22          (A) in section 2701(c)(3), by striking “sec-  
23      tion 2703” and inserting “section 2703 or  
24      2703A (as applicable)”; and

25          (B) in section 2705—

1 (i) by striking “section 2703(b)” each  
2 place it appears and inserting “section  
3 2703A(b)”;

4 (ii) in subsection (a)(4), by striking  
5 “section 2703” and inserting “section  
6 2703 or 2703A, as applicable,”; and

7 (iii) in subsection (b), in the matter  
8 preceding paragraph (1)—

9 (I) by striking “section 2703”  
10 and inserting “section 2703 or  
11 2703A, as applicable,”; and

12 (II) by striking “section  
13 2703(b)(1)” and inserting “section  
14 2703A(b)(1)”;

15 (C) in section 2706—

16 (i) in subsection (a), by striking “sec-  
17 tion 2702, 2703, or 2704 of this title” and  
18 inserting “subsection (b) or (h) of section  
19 2702 (as applicable), section 2703 or  
20 2703A (as applicable), or section 2704”;  
21 and

22 (ii) in subsection (c), by striking “sec-  
23 tion 2703 of this title” and inserting “sec-  
24 tion 2703 or 2703A, as applicable,”; and

25 (D) in section 2707—

1 (i) in subsection (a), by striking “sec-  
2 tion 2703(e),” and inserting “section  
3 2703(e) or section 2703A(e), as applica-  
4 ble,”;

5 (ii) in subsection (e)(1), by striking  
6 “section 2703(f) of this title” and insert-  
7 ing “section 2703(f) or section 2703A(f),  
8 as applicable”; and

9 (iii) in subsection (g), by striking  
10 “section 2703 of this title,” and inserting  
11 “section 2703 or 2703A, as applicable,”.

12 (4) DEFINITION OF ELECTRONIC COMMUNICA-  
13 TION.—Section 2510(12)(C) of title 18, United  
14 States Code, is amended to read as follows:

15 “(C)(i) in the case of a department or  
16 agency of the United States, a communication  
17 from a lawfully installed tracking device (as de-  
18 fined in section 3117 of this title), if—

19 “(I) the tracking device is physically  
20 placed; or

21 “(II) the tracking software or  
22 functionality of the tracking device is re-  
23 motely activated and the communication is  
24 transmitted by the tracking software or

1                    functionality as a result of the remote acti-  
 2                    vation; or

3                    “(ii) in the case of a department or agency  
 4                    of a State or a political subdivision thereof, any  
 5                    communication from a tracking device (as de-  
 6                    fined in section 3117A of this title); or”.

7                    (5) CHAPTER 121 TABLE OF SECTIONS.—The  
 8                    table of sections for chapter 121 of title 18, United  
 9                    States Code, is amended by striking the item relat-  
 10                    ing to section 2703 and inserting the following:

“2703. Required disclosure of customer communications or records to Federal depart-  
 ments and agencies.

“2703A. Required disclosure of customer communications or records to State  
 and local departments and agencies.”.

11                    (6) CHAPTER 205 TABLE OF SECTIONS.—The  
 12                    table of sections for chapter 205 of title 18, United  
 13                    States Code, is amended by striking the item relat-  
 14                    ing to section 3117 and inserting the following:

“3117. Tracking orders for Federal departments and agencies.

“3117A. Mobile tracking devices for State and local departments and agencies.”.

15                    (d) CONFORMING AMENDMENTS TO THE EMAIL PRI-  
 16                    VACY ACT.—Section 2704 of title 18, United States Code,  
 17                    is amended—

18                    (1) in subsection (a)—

19                    (A) in paragraph (1), by striking “section  
 20                    2703(b)(2)”            and            inserting            “section  
 21                    2703A(b)(2)”; and

1 (B) in paragraph (5), by striking “section  
2 2703” and inserting “section 2703A”; and

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

4 “(c) LIMITATION TO NON-FEDERAL ENTITIES.—  
5 Notwithstanding section 2711, in this section, the term  
6 ‘governmental entity’—

7 “(1) means a department or agency of a State  
8 or a political subdivision thereof; and

9 “(2) does not include a department or agency  
10 of the United States.”.

11 **TITLE VII—PROTECTION OF CAR**  
12 **DATA FROM FEDERAL**  
13 **WARRANTLESS SEARCHES**

14 **SEC. 701. PROTECTION OF CAR DATA FROM FEDERAL**  
15 **WARRANTLESS SEARCHES.**

16 (a) IN GENERAL.—Part I of title 18, United States  
17 Code, is amended by adding at the end the following:

18 **“CHAPTER 124—ACCESSING VEHICLE**  
19 **DATA**

“Sec.

“2730. Definitions.

“2731. Prohibition on Federal access to vehicle data.

“2732. Prohibition on use of acquired information as evidence.

20 **“§ 2730. Definitions**

21 “In this chapter:

22 “(1) ACCESS.—The term ‘access’ means any re-  
23 trieval of covered vehicle data, regardless of—

1           “(A) whether the data is obtained as the  
2 information is being produced or from digital  
3 storage; and

4           “(B) where the vehicle data is stored or  
5 transmitted, including by wire or radio.

6           “(2) CONSENT.—The term ‘consent’—

7           “(A) means an affirmative, express, and  
8 voluntary agreement that—

9           “(i) states that the person providing  
10 the consent is providing consent to a gov-  
11 ernment official to access the digital con-  
12 tents, access credential, or online account  
13 information, or other information being  
14 sought;

15           “(ii) specifies the type of content, ac-  
16 cess credential, or online account informa-  
17 tion the person is providing access to;

18           “(iii) specifies the time period of the  
19 covered vehicle data to be accessed;

20           “(iv) informs the person providing  
21 consent that consent is optional and that  
22 the government official attempting to ob-  
23 tain consent must otherwise acquire a war-  
24 rant if consent is not obtained;

1 “(v) does not involve sanctions or the  
2 threat of sanctions for withholding consent;  
3 and

4 “(vi) uses clear, simple, and com-  
5 prehensible language that is presented in a  
6 way that is accessible to the person pro-  
7 viding consent; and

8 “(B) does not include consent obtained  
9 through agreement to a generic privacy policy  
10 or a terms of service agreement.

11 “(3) COVERED VEHICLE DATA.—The term ‘cov-  
12 ered vehicle data’—

13 “(A) means all onboard and telematics  
14 data generated by, processed by, or stored on a  
15 noncommercial vehicle using computing, storage  
16 and communication systems installed, attached  
17 to, or carried in the vehicle, including diagnostic  
18 data, entertainment system data, navigation  
19 data, images or data captured by onboard sen-  
20 sors, or cameras, including images or data used  
21 to support automated features or autonomous  
22 driving, internet access, and communication to  
23 and from vehicle occupants;

24 “(B) includes data gathered by event data  
25 recorders; and



1 “(C) does not include—

2 “(i) automotive software installed by  
3 the manufacturer, as defined by applicable  
4 industry standards or regulations;

5 “(ii) any data subject to chapter 119  
6 of this title or section 104 of the Foreign  
7 Intelligence Surveillance Act of 1978 (50  
8 U.S.C. 1804); or

9 “(iii) data that is collected from out-  
10 side the vehicle, including speed data and  
11 geolocation data, for purposes of traffic,  
12 law enforcement, or toll collection.

13 “(4) EVENT DATA RECORDER.—The term  
14 ‘event data recorder’ has the meaning given the term  
15 in section 563.5 of title 49, Code of Federal Regula-  
16 tions (as in effect on March 5, 2019).

17 “(5) FEDERAL INVESTIGATIVE OR LAW EN-  
18 FORCEMENT OFFICER.—The term ‘Federal inves-  
19 tigative or law enforcement officer’ means any offi-  
20 cer of the United States, who is empowered by law  
21 to execute searches, to seize evidence, or to make ar-  
22 rests for a violation of any Federal law.

23 “(6) NONCOMMERCIAL VEHICLE.—The term  
24 ‘noncommercial vehicle’ has the meaning given the

1 term ‘non-CMV’ in section 383.5 of title 49, Code of  
2 Federal Regulations.

3 “(7) VEHICLE OPERATOR.—The term ‘vehicle  
4 operator’ means—

5 “(A) a person who controls the operation  
6 of a vehicle at the time consent is sought; and

7 “(B) with respect to a vehicle that is not  
8 classified as a highly autonomous vehicle by the  
9 Secretary of Transportation, the driver of the  
10 vehicle.

11 **“§ 2731. Prohibition on Federal access to vehicle data**

12 “(a) IN GENERAL.—Except as provided in subsection  
13 (b), a Federal investigative or law enforcement officer may  
14 not access covered vehicle data unless pursuant to a war-  
15 rant issued in accordance with the procedures described  
16 in rule 41 of the Federal Rules of Criminal Procedure by  
17 a court of competent jurisdiction, or as otherwise provided  
18 in this chapter or sections 104 and 303 of the Foreign  
19 Intelligence Surveillance Act of 1978 (50 U.S.C. 1804,  
20 1823).

21 “(b) EXCEPTIONS.—

22 “(1) CONSENT.—

23 “(A) IN GENERAL.—A Federal investiga-  
24 tive or law enforcement officer may access cov-  
25 ered vehicle data if—

1 “(i) the vehicle operator provides prior  
2 consent to such access; and

3 “(ii) no passenger 14 years of age or  
4 older objects to the access.

5 “(B) VEHICLE OWNER.—If the vehicle op-  
6 erator cannot be located with reasonable effort,  
7 the vehicle owner or, in the case of a leased ve-  
8 hicle, the lessee, may provide consent under this  
9 paragraph.

10 “(C) UNLAWFUL POSSESSION.—No indi-  
11 vidual may provide or withhold consent under  
12 this paragraph or object to another individual  
13 accessing covered vehicle data if the indi-  
14 vidual—

15 “(i) is the vehicle operator who is in  
16 unlawful possession of the vehicle; or

17 “(ii) is a passenger who unlawfully  
18 obtained access to the vehicle.

19 “(D) ORAL CONSENT.—Consent provided  
20 under this paragraph shall be in writing un-  
21 less—

22 “(i) the person providing the consent  
23 requests that the consent be made orally;  
24 and

1 “(ii) the request for consent and the  
2 consent are recorded.

3 “(E) CONSENT OF VEHICLE OPERATOR.—  
4 If the vehicle operator is not the owner of the  
5 vehicle and provides consent under this para-  
6 graph, the consent is valid only with respect to  
7 covered vehicle data generated during the lawful  
8 possession and use of the vehicle by the vehicle  
9 operator.

10 “(2) EMERGENCY.—

11 “(A) IN GENERAL.—A Federal investiga-  
12 tive or law enforcement officer, the Attorney  
13 General, the Deputy Attorney General, or the  
14 Associate Attorney General may access covered  
15 vehicle data if—

16 “(i) such officer reasonably deter-  
17 mines that an emergency situation exists  
18 that—

19 “(I) involves immediate danger of  
20 death or serious physical injury to any  
21 person; and

22 “(II) requires access to covered  
23 vehicle data before such officer can,  
24 with due diligence, obtain a warrant;

1           “(ii) there are grounds upon which a  
2           warrant could be granted to authorize such  
3           access; and

4           “(iii) an application for a warrant ap-  
5           proving such access is submitted to a court  
6           within 48 hours after the access has oc-  
7           curred or begins to occur.

8           “(B) DENIAL.—If an application for a  
9           warrant submitted pursuant to subparagraph  
10          (A)(iii) is denied, any covered vehicle data  
11          accessed under this paragraph shall be treated  
12          as having been obtained in violation of this  
13          chapter.

14          “(3) EVENT DATA RECORDER FOR MOTOR VE-  
15          HICLE SAFETY.—In addition to the exceptions in  
16          paragraphs (1) and (2), data recorded or trans-  
17          mitted by an event data recorder may be accessed  
18          from a noncommercial vehicle if authorized by para-  
19          graph (3), (4), or (5) of section 24302(b) of the  
20          Driver Privacy Act of 2015 (49 U.S.C. 30101 note).

21          “(4) RULE OF CONSTRUCTION.—Nothing in  
22          this section shall be interpreted to require the trans-  
23          mission or storage of data that is not otherwise  
24          transmitted or stored, or the retrieval of data that  
25          is not generally retrievable.

1   **“§ 2732. Prohibition on use of acquired information**  
2                   **as evidence**

3           “(a) IN GENERAL.—If any covered vehicle data has  
4   been acquired in violation of this chapter, no part of such  
5   information and no evidence derived therefrom may be  
6   used, received in evidence, or otherwise disseminated in  
7   any investigation, trial, hearing, or other proceeding by,  
8   in, or before any court, grand jury, department, officer,  
9   agency, regulatory body, legislative committee, or other  
10   authority of the United States, a State, or a political sub-  
11   division thereof.

12          “(b) PROBABLE CAUSE.—No data described in sec-  
13   tion 2731(b)(3) may be used to establish probable cause.”.

14          (b) TECHNICAL AND CONFORMING AMENDMENTS.—

15               (1) DRIVER PRIVACY ACT OF 2015.—Section  
16       24302 of the Driver Privacy Act of 2015 (49 U.S.C.  
17       30101 note) is amended—

18                   (A) in subsection (b), in the matter pre-  
19               ceding paragraph (1), by striking “Data” and  
20               inserting “Except as provided in subsection (c),  
21               data”; and

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

23           “(c) FEDERAL INVESTIGATIVE OR LAW ENFORCE-  
24   MENT OFFICERS.—A Federal investigative or law enforce-  
25   ment officer (as defined in section 2730 of title 18, United  
26   States Code), may only access or retrieve data recorded

1 or transmitted by an event data recorder described in sub-  
 2 section (a) in accordance with chapter 124 of title 18,  
 3 United States Code.”.

4 (2) TABLE OF CHAPTERS.—The table of chap-  
 5 ters for part 1 of title 18, United States Code, is  
 6 amended by adding at the end the following:

“124. Accessing vehicle data ..... 2730”.

7 **TITLE VIII—INTELLIGENCE**  
 8 **TRANSPARENCY**

9 **SEC. 801. ENHANCED ANNUAL REPORTS BY DIRECTOR OF**  
 10 **THE ADMINISTRATIVE OFFICE OF THE**  
 11 **UNITED STATES COURTS.**

12 Section 603(a)(1) of the Foreign Intelligence Surveil-  
 13 lance Act of 1978 (50 U.S.C. 1873(a)(1)) is amended—

14 (1) in subparagraph (F), by striking “; and”  
 15 and inserting a semicolon;

16 (2) in subparagraph (G), by striking the period  
 17 at the end and inserting a semicolon; and

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

19 “(H) the number of certifications by the  
 20 Foreign Intelligence Surveillance Court pursu-  
 21 ant to section 103(j);

22 “(I) the number of petitions to certify a  
 23 question made by an amicus curiae pursuant to  
 24 section 103(i)(7)(A);

1           “(J) the number of hearings or rehearings  
 2           by the Foreign Intelligence Surveillance Court  
 3           en banc pursuant to section 103(a)(2),  
 4           disaggregated by hearings or rehearings by  
 5           such court en banc pursuant to clause (i) or (ii)  
 6           of such section; and

7           “(K) the number of times amici curiae  
 8           have been appointed pursuant to section  
 9           103(i)(2).”.

10 **SEC. 802. ENHANCED ANNUAL REPORTS BY DIRECTOR OF**  
 11 **NATIONAL INTELLIGENCE.**

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

15           (1) in paragraph (2)(C), by striking the semi-  
 16           colon and inserting “; and”;

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

19           (3) by inserting after paragraph (2) the fol-  
 20           lowing:

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

23           “(4) statistics revealing the number of persons  
 24           and identifiers targeted under section 702(a),



1 disaggregated by certification under which the per-  
2 son or identifier was targeted;

3 “(5) the total number of directives issued pur-  
4 suant to section 702(i)(1), disaggregated by each  
5 type of electronic communication service provider de-  
6 scribed in each of the subparagraphs of section  
7 701(b)(4);”; and

8 (4) by adding at the end the following:

9 “(11)(A) the total number of disseminated in-  
10 telligence reports derived from collection pursuant to  
11 section 702 containing the identities of United  
12 States persons regardless of whether the identities of  
13 the United States persons were openly included or  
14 masked;

15 “(B) the total number of disseminated intel-  
16 ligence reports derived from collection pursuant to  
17 section 702 containing the identities of United  
18 States persons in which the identities of the United  
19 States persons were masked;

20 “(C) the total number of disseminated intel-  
21 ligence reports derived from collection outside the  
22 authorities provided by this Act containing the iden-  
23 tities of United States persons in which the identi-  
24 ties of the United States persons were masked;

1           “(D) the total number of disseminated intel-  
2           ligence reports derived from collection pursuant to  
3           section 702 containing the identities of United  
4           States persons in which the identities of the United  
5           States persons were openly included; and

6           “(E) the total number of disseminated intel-  
7           ligence reports derived from collection outside the  
8           authorities provided by this Act containing the iden-  
9           tities of United States persons in which the identi-  
10          ties of the United States persons were openly in-  
11          cluded;

12          “(12)(A) the number of queries conducted in an  
13          effort to find communications or information of or  
14          about a covered person that required a warrant pur-  
15          suant to section 302 of the Government Surveillance  
16          Reform Act of 2026; and

17          “(B) the number of queries conducted in an ef-  
18          fort to find communications or information of or  
19          about a covered person that did not require a war-  
20          rant pursuant to section 302 of the Government  
21          Surveillance Reform Act of 2026; and

22          “(13) the number of criminal proceedings in  
23          which the Federal Government or a government of  
24          a State or political subdivision thereof entered into  
25          evidence or otherwise used or disclosed in a criminal

1 proceeding any information obtained or derived from  
 2 an acquisition conducted for foreign intelligence pur-  
 3 poses outside the authorities provided by this Act,  
 4 regardless of whether such acquisition occurred in-  
 5 side or outside the United States.”.

6 (b) REPEAL OF NONAPPLICABILITY TO FEDERAL  
 7 BUREAU OF INVESTIGATION OF CERTAIN REQUIRE-  
 8 MENTS.—Subsection (d) of such section is amended—

9 (1) by striking paragraph (2); and

10 (2) by redesignating paragraph (3) as para-  
 11 graph (2).

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

15 **SEC. 803. ANNUAL REPORTING ON ACCURACY AND COM-**  
 16 **PLETENESS OF APPLICATIONS.**

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

19 (1) by redesignating subsections (f) and (g) as  
 20 subsections (g) and (h), respectively; and

21 (2) by inserting after subsection (e) the fol-  
 22 lowing:

23 “(f) ANNUAL REPORT BY ATTORNEY GENERAL ON  
 24 ACCURACY AND COMPLETENESS OF APPLICATIONS.—

1           “(1) REPORT REQUIRED.—In April each year,  
2           the Attorney General shall submit to the appropriate  
3           committees of Congress and publish on the website  
4           of the Department of Justice, subject to a declas-  
5           sification review, a report setting forth, with respect  
6           to the preceding calendar year, the following:

7                   “(A) A summary of all accuracy or com-  
8                   pleteness reviews of applications for court or-  
9                   ders submitted to the Foreign Intelligence Sur-  
10                  veillance Court by the Federal Bureau of Inves-  
11                  tigation under this Act.

12                  “(B) The total number of such applica-  
13                  tions reviewed for accuracy or completeness.

14                  “(C) The total number of material errors  
15                  or omissions identified during such reviews.

16                  “(D) The total number of nonmaterial er-  
17                  rors or omissions identified during such reviews.

18                  “(E) The total number of instances in  
19                  which facts contained in an application were  
20                  not supported by documentation that existed in  
21                  the applicable file being reviewed at the time of  
22                  the review.

23                  “(F) An explanation for any increase or  
24                  decrease in the number of errors identified  
25                  under subparagraphs (C) and (D), and in the

1 event of an increase in the number of errors, a  
 2 description of any action taken by the Depart-  
 3 ment to improve compliance and accuracy.

4 “(2) INSPECTOR GENERAL RISK ASSESS-  
 5 MENT.—In addition to conducting audits under sec-  
 6 tion 501 of the Government Surveillance Reform Act  
 7 of 2026, the Inspector General of the Department of  
 8 Justice shall—

9 “(A) periodically assess the reports re-  
 10 quired by paragraph (1); and

11 “(B) as determined by the Inspector Gen-  
 12 eral, report any risks identified through such  
 13 assessments to the appropriate committees of  
 14 Congress.

15 “(3) DEFINITION OF APPROPRIATE COMMIT-  
 16 TEES OF CONGRESS.—In this subsection, the term  
 17 ‘appropriate committees of Congress’ has the mean-  
 18 ing given that term in section 101.”.

19 **SEC. 804. ALLOWING MORE GRANULAR AGGREGATE RE-**  
 20 **PORTING BY RECIPIENTS OF FOREIGN INTEL-**  
 21 **LIGENCE SURVEILLANCE ORDERS.**

22 (a) MODIFICATION OF AGGREGATION BANDING.—  
 23 Subsection (a) of section 604 of the Foreign Intelligence  
 24 Surveillance Act of 1978 (50 U.S.C. 1874) is amended—

1           (1) by striking paragraphs (1) through (3) and  
2       inserting the following:

3           “(1) A semiannual report that aggregates the  
4       number of orders, directives, or national security let-  
5       ters with which the person was required to comply  
6       into separate categories of—

7           “(A) the number of national security let-  
8       ters received, reported—

9           “(i) for the first 1,000 national secu-  
10       rity letters received, in bands of 200 start-  
11       ing with 1–200; and

12          “(ii) for more than 1,000 national se-  
13       curity letters received, the precise number  
14       of national security letters received;

15          “(B) the number of customer selectors tar-  
16       geted by national security letters, reported—

17          “(i) for the first 1,000 customer selec-  
18       tors targeted, in bands of 200 starting  
19       with 1–200; and

20          “(ii) for more than 1,000 customer se-  
21       lectors targeted, the precise number of cus-  
22       tomer selectors targeted;

23          “(C) the number of orders or directives re-  
24       ceived, combined, under this Act for contents—

25          “(i) reported—

1                   “(I) for the first 1,000 orders  
2                   and directives received, in bands of  
3                   200 starting with 1–200; and

4                   “(II) for more than 1,000 orders  
5                   and directives received, the precise  
6                   number of orders received; and

7                   “(ii) disaggregated by whether the  
8                   order or directive was issued under section  
9                   105, 402, or 702;

10                  “(D) the number of customer selectors tar-  
11                  geted under orders or directives received, com-  
12                  bined, under this Act for contents—

13                   “(i) reported—

14                   “(I) for the first 1,000 customer  
15                   selectors targeted, in bands of 200  
16                   starting with 1–200; and

17                   “(II) for more than 1,000 cus-  
18                   tomer selectors targeted, the precise  
19                   number of customer selectors tar-  
20                   geted; and

21                   “(ii) disaggregated by whether the  
22                   order or directive was issued under section  
23                   105, 402, or 702;

24                   “(E) the number of orders or directives re-  
25                   ceived under this Act for noncontents—

1 “(i) reported—

2 “(I) for the first 1000 orders or  
3 directives received, in bands of 200  
4 starting with 1–200; and

5 “(II) for more than 1,000 orders  
6 or directives received, the precise  
7 number of orders received; and

8 “(ii) disaggregated by whether the  
9 order or directive was issued under section  
10 105, 402, or 702; and

11 “(F) the number of customer selectors tar-  
12 geted under orders or directives under this Act  
13 for noncontents—

14 “(i) reported—

15 “(I) for the first 1,000 customer  
16 selectors targeted, in bands of 200  
17 starting with 1–200; and

18 “(II) for more than 1,000 cus-  
19 tomer selectors targeted, the precise  
20 number of customer selectors tar-  
21 geted; and

22 “(ii) disaggregated by whether the  
23 order or directive was issued under section  
24 105, 402, or 702.”; and



1           (2) by redesignating paragraph (4) as para-  
2       graph (2).

3       (b) ADDITIONAL DISCLOSURES.—Such section is  
4       amended—

5           (1) by redesignating subsections (b) through (d)  
6       as subsections (c) through (e), respectively; and

7           (2) by inserting after subsection (a) the fol-  
8       lowing:

9       “(b) ADDITIONAL DISCLOSURES.—A person who  
10      publicly reports information under subsection (a) may also  
11      publicly report, using a semiannual report, information re-  
12      lating to the previous 180 days that indicates whether the  
13      person was or was not required to comply with an order,  
14      directive, or national security letter issued under each of  
15      sections 105, 402, and 702 and the provisions listed in  
16      section 603(f)(3).”.

17      (c) CONFORMING AMENDMENTS.—Subsection (c) of  
18      such section, as redesignated by subsection (b)(1) of this  
19      section, is amended—

20           (1) in paragraph (1), by striking “or (2)”;

21           (2) by striking paragraph (2);

22           (3) by redesignating paragraph (3) as para-  
23      graph (2); and

24           (4) in paragraph (2), as so redesignated, by  
25      striking “(4)” and inserting “(2)”.

1 **SEC. 805. REPORT ON USE OF FOREIGN INTELLIGENCE**  
2 **SURVEILLANCE AUTHORITIES REGARDING**  
3 **PROTECTED ACTIVITIES AND PROTECTED**  
4 **CLASSES.**

5 (a) REPORT.—Not later than 1 year after the date  
6 of the enactment of this Act, the Privacy and Civil Lib-  
7 erties Oversight Board shall make publicly available and  
8 submit to the appropriate committees of Congress a report  
9 on the use of activities and protected classes described in  
10 subsection (b) in—

11 (1) applications for orders made by the United  
12 States Government under the Foreign Intelligence  
13 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.);  
14 and

15 (2) investigations for which such orders are  
16 sought.

17 (b) ACTIVITIES AND PROTECTED CLASSES DE-  
18 SCRIBED.—The activities and protected classes described  
19 in this subsection are the following:

20 (1) Activities and expression protected by the  
21 First Amendment to the Constitution of the United  
22 States.

23 (2) Race, ethnicity, national origin, and reli-  
24 gious affiliation.

25 (c) FORM.—In addition to the report made publicly  
26 available and submitted under subsection (a), the Board

1 may submit to the appropriate committees of Congress a  
2 classified annex.

3 **SEC. 806. PUBLICATION OF ESTIMATES REGARDING COM-**  
4 **MUNICATIONS COLLECTED UNDER CERTAIN**  
5 **PROVISIONS OF THE FOREIGN INTEL-**  
6 **LIGENCE SURVEILLANCE ACT OF 1978.**

7 Not later than 90 days after the date of the enact-  
8 ment of this Act, the Director of National Intelligence  
9 shall publish a good faith estimate of—

10 (1) the number of United States persons whose  
11 communications are collected under section 702 of  
12 the Foreign Intelligence Surveillance Act of 1978  
13 (50 U.S.C. 1881a); or

14 (2) the number of communications collected  
15 under such section to which a party is a person lo-  
16 cated in the United States at the time of commu-  
17 nication.

18 **SEC. 807. ENHANCED REPORTING OF ASSESSMENTS OF**  
19 **COMPLIANCE WITH EMERGENCY ORDER RE-**  
20 **QUIREMENTS UNDER CERTAIN PROVISIONS**  
21 **OF THE FOREIGN INTELLIGENCE SURVEIL-**  
22 **LANCE ACT OF 1978.**

23 (a) ELECTRONIC SURVEILLANCE.—

24 (1) ANNUAL ASSESSMENT.—Section 105(e)(6)  
25 of the Foreign Intelligence Surveillance Act of 1978

1 (50 U.S.C. 1805(e)(6)) is amended by striking  
2 “shall assess compliance” and inserting “shall not  
3 less frequently than annually assess compliance”.

4 (2) REPORTING.—Section 108(a)(2) of the For-  
5 eign Intelligence Surveillance Act of 1978 (50  
6 U.S.C. 1808(a)(2)) is amended—

7 (A) in subparagraph (C), by striking “;  
8 and” and inserting a semicolon;

9 (B) in subparagraph (D), by striking “sec-  
10 tion 301(e).” and inserting “section 304(e);  
11 and”; and

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

13 “(E) the annual assessment conducted  
14 pursuant to section 105(e)(6).”.

15 (b) PHYSICAL SEARCHES.—

16 (1) ANNUAL ASSESSMENT.—Section 304(e)(6)  
17 of the Foreign Intelligence Surveillance Act of 1978  
18 (50 U.S.C. 1824(e)(6)) is amended by striking  
19 “shall assess compliance” and inserting “shall not  
20 less frequently than annually assess compliance”.

21 (2) REPORTING.—Section 306 of the Foreign  
22 Intelligence Surveillance Act of 1978 (50 U.S.C.  
23 1826) is amended—

24 (A) in paragraph (3), by striking “; and”  
25 and inserting a semicolon;

1 (B) in paragraph (4), by striking the pe-  
2 riod and inserting “; and”; and

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

4 “(5) the annual assessment conducted pursuant  
5 to section 304(e)(6).”.

6 **TITLE IX—SEVERABILITY AND**  
7 **LIMITED DELAYS IN IMPLE-**  
8 **MENTATION**

9 **SEC. 901. RULE OF CONSTRUCTION WITH RESPECT TO**  
10 **STATE AND LOCAL LAW ENFORCEMENT AU-**  
11 **THORITIES.**

12 Nothing in this Act, or an amendment made by this  
13 Act, shall be construed to modify the authorities or affect  
14 the procedures for the acquisition of records by any de-  
15 partment or agency of a State or a political subdivision  
16 thereof as in effect on the day before the date of the enact-  
17 ment of this Act.

18 **SEC. 902. SEVERABILITY.**

19 If any provision of this Act, an amendment made by  
20 this Act, or the application of such a provision or amend-  
21 ment to any person or circumstance, is held to be uncon-  
22 stitutional, the remaining provisions of and amendments  
23 made by this Act, and the application of the provision or  
24 amendment held to be unconstitutional to any other per-  
25 son or circumstance, shall not be affected thereby.

1 **SEC. 903. LIMITED DELAYS IN IMPLEMENTATION.**

2       The Attorney General may, in coordination with the  
3 Director of National Intelligence as may be appropriate,  
4 delay implementation of a provision of this Act or an  
5 amendment made by this Act for a period of not more  
6 than 1 year upon a showing to the appropriate committees  
7 of Congress that the delay is necessary—

- 8           (1) to develop and implement technical systems  
9       needed to comply with the provision or amendment;  
10       or  
11           (2) to hire or train personnel needed to comply  
12       with the provision or amendment.

○