

**AMENDMENT IN THE NATURE OF A SUBSTITUTE**  
**TO H.R. \_\_\_\_\_**  
**OFFERED BY M. \_\_\_\_\_**

Strike all that follows after the enacting clause and  
insert the following:

**1 SECTION 1. SHORT TITLE.**

2       This Act may be cited as the “Protect Liberty and  
3 End Warrantless Surveillance Act of 2023”.

**4 SEC. 2. QUERY PROCEDURE REFORM.**

5       (a) LIMITATION ON ELIGIBILITY TO CONDUCT QUE-  
6 RIES.—Section 702(f)(1) of the Foreign Intelligence Sur-  
7 veillance Act of 1978 (50 U.S.C. 1881a(f)(1)) is amended  
8 by adding at the end the following:

9               “(D) LIMITATION ON ELIGIBILITY OF FBI  
10               PERSONNEL TO CONDUCT UNITED STATES PER-  
11               SON QUERIES.—The Attorney General shall en-  
12               sure that the procedures adopted under sub-  
13               paragraph (A) limit the authority to conduct  
14               queries such that—

15               “(i) for each field office of the Federal  
16               Bureau of Investigation, the most senior  
17               official whose primary duty station is that  
18               field office is authorized to designate not

1 more than five individuals whose primary  
2 duty station is that field office who are eli-  
3 gible to conduct a query using a United  
4 States person query term; and

5 “(ii) for the headquarters of the Fed-  
6 eral Bureau of Investigation, the Director  
7 of the Federal Bureau of Investigation is  
8 authorized to designate not more than five  
9 individuals whose primary duty station is  
10 the Headquarters of the Federal Bureau of  
11 Investigation who are eligible to conduct a  
12 query using a United States person query  
13 term.”.

14 (b) PROHIBITION ON WARRANTLESS QUERIES FOR  
15 THE COMMUNICATIONS OF UNITED STATES PERSONS  
16 AND PERSONS LOCATED IN THE UNITED STATES.—Sec-  
17 tion 702(f) of the Foreign Intelligence Surveillance Act of  
18 1978 (50 U.S.C. 1881a(f)), as amended by subsection (a),  
19 is further amended—

20 (1) in paragraph (1)—

21 (A) in subparagraph (A), by inserting  
22 “and the limitations and requirements in para-  
23 graph (2)” after “Constitution of the United  
24 States”; and

1 (B) in subparagraph (B), by striking  
2 “United States person query term used for a  
3 query” and inserting “term for a United States  
4 person or person reasonably believed to be in  
5 the United States used for a query as required  
6 by paragraph (3)”;

7 (2) by redesignating paragraph (3) as para-  
8 graph (6); and

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

11 “(2) PROHIBITION ON WARRANTLESS QUERIES  
12 FOR THE COMMUNICATIONS AND OTHER INFORMA-  
13 TION OF UNITED STATES PERSONS AND PERSONS  
14 LOCATED IN THE UNITED STATES.—

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

1           the query or the time of the communication or  
2           creation of the information.

3           “(B) EXCEPTIONS FOR CONCURRENT AU-  
4           THORIZATION, CONSENT, EMERGENCY SITUA-  
5           TIONS, AND CERTAIN DEFENSIVE CYBERSECU-  
6           RITY QUERIES.—

7           “(i) IN GENERAL.—Subparagraph (A)  
8           shall not apply to a query related to a  
9           United States person or person reasonably  
10          believed to be located in the United States  
11          at the time of the query or the time of the  
12          communication or creation of the informa-  
13          tion if—

14          “(I) such person is the subject of  
15          an order or emergency authorization  
16          authorizing electronic surveillance or  
17          physical search under section 105 or  
18          304 of this Act, or a warrant issued  
19          pursuant to the Federal Rules of  
20          Criminal Procedure by a court of  
21          competent jurisdiction covering the  
22          period of the query;

23          “(II)(aa) the officer or employee  
24          carrying out the query has a reason-  
25          able belief that—

1                   “(AA) an emergency exists  
2 involving an imminent threat of  
3 death or serious bodily harm; and

4                   “(BB) in order to prevent or  
5 mitigate this threat, the query  
6 must be conducted before author-  
7 ization pursuant to subparagraph  
8 (I) can, with due diligence, be ob-  
9 tained; and

10                   “(bb) a description of the  
11 query is provided to the Foreign  
12 Intelligence Surveillance Court  
13 and the congressional intelligence  
14 committees and the Committees  
15 on the Judiciary of the House of  
16 Representatives and of the Sen-  
17 ate in a timely manner;

18                   “(III) such person or, if such  
19 person is incapable of providing con-  
20 sent, a third party legally authorized  
21 to consent on behalf of such person,  
22 has provided consent to the query on  
23 a case-by-case basis; or

1                   “(IV)(aa) the query uses a  
2                   known cybersecurity threat signature  
3                   as a query term;

4                   “(bb) the query is conducted, and the results of the  
5 query are used, for the sole purpose of identifying targeted  
6 recipients of malicious software and preventing or miti-  
7 gating harm from such malicious software;

8                   “(cc) no additional contents of communications re-  
9 trieved as a result of the query are accessed or reviewed;  
10 and

11                   “(dd) all such queries are reported to the Foreign In-  
12 telligence Surveillance Court.

13                   “(ii) LIMITATIONS.—

14                   “(I) USE IN SUBSEQUENT PRO-  
15 CEEDINGS AND INVESTIGATIONS.—No  
16 information retrieved pursuant to a  
17 query authorized by clause (i)(II) or  
18 information derived from such query  
19 may be used, received in evidence, or  
20 otherwise disseminated in any inves-  
21 tigation, trial, hearing, or other pro-  
22 ceeding in or before any court, grand  
23 jury, department, office, agency, regu-  
24 latory body, legislative committee, or  
25 other authority of the United States,

1 a State, or political subdivision there-  
2 of, except in proceedings or investiga-  
3 tions that arise from the threat that  
4 prompted the query.

5 “(II) ASSESSMENT OF COMPLI-  
6 ANCE.—The Attorney General shall  
7 not less frequently than annually as-  
8 sess compliance with the requirements  
9 under subclause (I).

10 “(C) MATTERS RELATING TO EMERGENCY  
11 QUERIES.—

12 “(i) TREATMENT OF DENIALS.—In  
13 the event that a query for communications  
14 or information, the compelled production of  
15 which would require a probable cause war-  
16 rant if sought for law enforcement pur-  
17 poses in the United States, of or about 1  
18 more United States persons or persons  
19 reasonably believed to be located in the  
20 United States at the time of the query or  
21 the time of the communication or creation  
22 of the information is conducted pursuant  
23 to an emergency authorization described in  
24 subparagraph (B)(i)(I) and the application  
25 for such emergency authorization is denied,

1 or in any other case in which the query has  
2 been conducted and no order is issued ap-  
3 proving the query—

4 “(I) no information obtained or  
5 evidence derived from such query may  
6 be used, received in evidence, or other-  
7 wise disseminated in any investiga-  
8 tion, trial, hearing, or other pro-  
9 ceeding in or before any court, grand  
10 jury, department, office, agency, regu-  
11 latory body, legislative committee, or  
12 other authority of the United States,  
13 a State, or political subdivision there-  
14 of; and

15 “(II) no information concerning  
16 any United States person or person  
17 reasonably believed to be located in  
18 the United States at the time of the  
19 query or the time of the communica-  
20 tion or the creation of the information  
21 acquired from such query may subse-  
22 quently be used or disclosed in any  
23 other manner without the consent of  
24 such person, except with the approval  
25 of the Attorney General if the infor-



1                   mation indicates a threat of death or  
2                   serious bodily harm to any person.

3                   “(ii) ASSESSMENT OF COMPLIANCE.—

4                   The Attorney General shall not less fre-  
5                   quently than annually assess compliance  
6                   with the requirements under clause (i).

7                   “(D) FOREIGN INTELLIGENCE PURPOSE.—

8                   Except as provided in subparagraph (B)(i), no  
9                   officer or employee of the United States may  
10                  conduct a query of information acquired under  
11                  this section in an effort to find information of  
12                  or about 1 or more United States persons or  
13                  persons reasonably believed to be located in the  
14                  United States at the time of the query or the  
15                  time of the communication or creation of the in-  
16                  formation unless the query is reasonably likely  
17                  to retrieve foreign intelligence information.

18                  “(3) DOCUMENTATION.—No officer or employee  
19                  of the United States may conduct a query of infor-  
20                  mation acquired under this section in an effort to  
21                  find information of or about 1 or more United  
22                  States persons or persons reasonably believed to be  
23                  located in the United States at the time of query or  
24                  the time of the communication or the creation of the  
25                  information, unless first an electronic record is cre-

1       ated, and a system, mechanism, or business practice  
2       is in place to maintain such record, that includes the  
3       following:

4               “(A) Each term used for the conduct of  
5       the query.

6               “(B) The date of the query.

7               “(C) The identifier of the officer or em-  
8       ployee.

9               “(D) A statement of facts showing that the  
10       use of each query term included under subpara-  
11       graph (A) is—

12                       “(i) reasonably likely to retrieve for-  
13       eign intelligence information; or

14                       “(ii) in furtherance of the exceptions  
15       described in paragraph (2)(B)(i).

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

1 communications or information a query for which is  
2 otherwise prohibited under this section.

3 “(5) FEDERATED DATASETS.—The prohibitions  
4 and requirements in this section shall apply to que-  
5 ries of federated and mixed datasets that include in-  
6 formation acquired under this section, unless a  
7 mechanism exists to limit the query to information  
8 not acquired under this section.”

9 **SEC. 3. LIMITATION ON USE OF INFORMATION OBTAINED**  
10 **UNDER SECTION 702 OF THE FOREIGN INTEL-**  
11 **LIGENCE SURVEILLANCE ACT OF 1978 RELAT-**  
12 **ING TO UNITED STATES PERSONS AND PER-**  
13 **SONS LOCATED IN THE UNITED STATES IN**  
14 **CRIMINAL, CIVIL, AND ADMINISTRATIVE AC-**  
15 **TIONS.**

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

19 “(2) LIMITATION ON USE IN CRIMINAL, CIVIL,  
20 AND ADMINISTRATIVE PROCEEDINGS AND INVES-  
21 TIGATIONS.—No information acquired pursuant to  
22 section 702(f) of or about a United States person or  
23 person reasonably believed to be located in the  
24 United States at the time of acquisition or commu-  
25 nication may be introduced as evidence against such

1 person in any criminal, civil, or administrative pro-  
2 ceeding or used as part of any criminal, civil, or ad-  
3 ministrative investigation, except—

4 “(A) with the prior approval of the Attor-  
5 ney General; and

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

9 “(i) the commission of a Federal  
10 crime of terrorism under any of clauses (i)  
11 through (iii) of section 2332b(g)(5)(B) of  
12 title 18, United States Code;

13 “(ii) actions necessitating counter-  
14 intelligence (as defined in section 3 of the  
15 National Security Act of 1947 (50 U.S.C.  
16 3003));

17 “(iii) the proliferation or the use of a  
18 weapon of mass destruction (as defined in  
19 section 2332a(e) of title 18, United States  
20 Code);

21 “(iv) a cybersecurity breach or attack  
22 from a foreign country;

23 “(v) incapacitation or destruction of  
24 critical infrastructure (as defined in section  
25 1016(e) of the Uniting and Strengthening

1 America by Providing Appropriate Tools  
2 Required to Intercept and Obstruct Ter-  
3 rorism (USA PATRIOT ACT) Act of 2001  
4 (42 U.S.C. 5195c(e));

5 “(vi) an attack against the armed  
6 forces of the United States or an ally of  
7 the United States or to other personnel of  
8 the United States Government or a govern-  
9 ment of an ally of the United States; or  
10 “(vii) international narcotics traf-  
11 ficking.”.

12 **SEC. 4. REPEAL OF AUTHORITY FOR THE RESUMPTION OF**  
13 **ABOUTS COLLECTION.**

14 (a) IN GENERAL.—Section 702(b)(5) of the Foreign  
15 Intelligence Surveillance Act of 1978 (50 U.S.C.  
16 1881a(b)(5)) is amended by striking “, except as provided  
17 under section 103(b) of the FISA Amendments Reauthor-  
18 ization Act of 2017”.

19 (b) CONFORMING AMENDMENTS.—

20 (1) FOREIGN INTELLIGENCE SURVEILLANCE  
21 ACT OF 1978.—Section 702(m) of the Foreign Intel-  
22 ligence Surveillance Act of 1978 (50 U.S.C.  
23 1881a(m)) is amended—

1 (A) in the subsection heading, by striking  
2 “REVIEWS, AND REPORTING” and inserting  
3 “AND REVIEWS”; and

4 (B) by striking paragraph (4).

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

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

10 (B) by striking “(a) IN GENERAL.—”.

11 **SEC. 5. FOREIGN INTELLIGENCE SURVEILLANCE COURT**  
12 **REFORM.**

13 (a) REQUIREMENT FOR SAME JUDGE TO HEAR RE-  
14 NEWAL APPLICATIONS.—Section 103(a)(1) of the Foreign  
15 Intelligence Surveillance Act of 1978 (50 U.S.C.  
16 1803(a)(1)) is amended by adding at the end the fol-  
17 lowing: “To the extent practicable, no judge designated  
18 under this subsection shall hear a renewal application for  
19 electronic surveillance under this Act, which application  
20 was previously granted by another judge designated under  
21 this subsection, unless the term of the judge who granted  
22 the application has expired, or that judge is otherwise no  
23 longer serving on the court.”.

24 (b) USE OF AMICI CURIAE IN FOREIGN INTEL-  
25 LIGENCE SURVEILLANCE COURT PROCEEDINGS.—

1           (1) EXPANSION OF APPOINTMENT AUTHOR-  
2           ITY.—

3           (A) IN GENERAL.—Section 103(i)(2) of the  
4           Foreign Intelligence Surveillance Act of 1978  
5           (50 U.S.C. 1803(i)(2)) is amended—

6           (i) by striking subparagraph (A) and  
7           inserting the following:

8           “(A) shall, unless the court issues a find-  
9           ing that appointment is not appropriate, ap-  
10          point 1 or more individuals who have been des-  
11          ignated under paragraph (1), not fewer than 1  
12          of whom possesses privacy and civil liberties ex-  
13          pertise, unless the court finds that such a quali-  
14          fication is inappropriate, to serve as amicus cu-  
15          riae to assist the court in the consideration of  
16          any application or motion for an order or review  
17          that, in the opinion of the court—

18                 “(i) presents a novel or significant in-  
19                 terpretation of the law;

20                 “(ii) presents significant concerns  
21                 with respect to the activities of a United  
22                 States person that are protected by the  
23                 first amendment to the Constitution of the  
24                 United States;

1 “(iii) presents or involves a sensitive  
2 investigative matter;

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

6 “(v) presents a request for reauthor-  
7 ization of programmatic surveillance;

8 “(vi) otherwise presents novel or sig-  
9 nificant civil liberties issues; or

10 “(vii) otherwise involves the activities  
11 of a United States person; and”;

12 (ii) in subparagraph (B), by striking  
13 “an individual or organization” each place  
14 the term appears and inserting “1 or more  
15 individuals or organizations”.

16 (B) DEFINITION OF SENSITIVE INVESTIGA-  
17 TIVE MATTER.—Section 103(i) of the Foreign  
18 Intelligence Surveillance Act of 1978 (50  
19 U.S.C. 1803(i)) is amended by adding at the  
20 end the following:

21 “(12) DEFINITION.—In this subsection, the  
22 term ‘sensitive investigative matter’ means—

23 “(A) an investigative matter involving the  
24 activities of—



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

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

8                   “(iii) the domestic news media; or

9                   “(B) any other investigative matter involv-  
10                  ing a domestic entity or a known or suspected  
11                  United States person that, in the judgment of  
12                  the applicable court established under sub-  
13                  section (a) or (b), is as sensitive as an inves-  
14                  tigative matter described in subparagraph  
15                  (A).”.

16                  (2) **AUTHORITY TO SEEK REVIEW.**—Section  
17                  103(i) of the Foreign Intelligence Surveillance Act of  
18                  1978 (50 U.S.C. 1803(i)), as amended by subsection  
19                  (a) of this section, is amended—

20                         (A) in paragraph (4)—

21                                 (i) in the paragraph heading, by in-  
22                                 serting “; **AUTHORITY**” after “**DUTIES**”;

23                                 (ii) by redesignating subparagraphs  
24                                 (A), (B), and (C) as clauses (i), (ii), and

1 (iii), respectively, and adjusting the mar-  
2 gins accordingly;

3 (iii) in the matter preceding clause (i),  
4 as so redesignated, by striking “the amicus  
5 curiae shall” and inserting the following:  
6 “the amicus curiae—  
7 “(A) shall”;

8 (iv) in subparagraph (A)(i), as so re-  
9 designated, by inserting before the semi-  
10 colon at the end the following: “, including  
11 legal arguments regarding any privacy or  
12 civil liberties interest of any United States  
13 person that would be significantly im-  
14 pacted by the application or motion”;

15 (v) by striking the period at the end  
16 and inserting the following: “; and

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

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

4 (C) by inserting after paragraph (6) the  
5 following:

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

8 “(A) FISA COURT DECISIONS.—

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

18 “(ii) WRITTEN STATEMENT OF REA-  
19 SONS.—If the Foreign Intelligence Surveil-  
20 lance Court denies a petition under this  
21 subparagraph, the Foreign Intelligence  
22 Surveillance Court shall provide for the  
23 record a written statement of the reasons  
24 for the denial.

1                   “(iii) APPOINTMENT.—Upon certifi-  
2                   cation of any question of law pursuant to  
3                   this subparagraph, the Court of Review  
4                   shall appoint the amicus curiae to assist  
5                   the Court of Review in its consideration of  
6                   the certified question, unless the Court of  
7                   Review issues a finding that such appoint-  
8                   ment is not appropriate.

9                   “(B) FISA COURT OF REVIEW DECI-  
10                  SIONS.—An amicus curiae appointed under  
11                  paragraph (2) may petition the Foreign Intel-  
12                  ligence Surveillance Court of Review to certify  
13                  for review to the Supreme Court of the United  
14                  States any question of law pursuant to section  
15                  1254(2) of title 28, United States Code.

16                  “(C) DECLASSIFICATION OF REFER-  
17                  RALS.—For purposes of section 602, a petition  
18                  filed under subparagraph (A) or (B) of this  
19                  paragraph and all of its content shall be consid-  
20                  ered a decision, order, or opinion issued by the  
21                  Foreign Intelligence Surveillance Court or the  
22                  Foreign Intelligence Surveillance Court of Re-  
23                  view described in paragraph (2) of section  
24                  602(a).”.

25                  (3) ACCESS TO INFORMATION.—

1           (A) APPLICATION AND MATERIALS.—Sec-  
2           tion 103(i)(6) of the Foreign Intelligence Sur-  
3           veillance Act of 1978 (50 U.S.C. 1803(i)(6)) is  
4           amended by striking subparagraph (A) and in-  
5           serting the following:

6           “(A) IN GENERAL.—

7           “(i) RIGHT OF AMICUS.—If a court  
8           established under subsection (a) or (b) ap-  
9           points an amicus curiae under paragraph  
10          (2), the amicus curiae—

11           “(I) shall have access, to the ex-  
12          tent such information is available to  
13          the Government, to—

14           “(aa) the application, certifi-  
15          cation, petition, motion, and  
16          other information and supporting  
17          materials, including any informa-  
18          tion described in section 901,  
19          submitted to the Foreign Intel-  
20          ligence Surveillance Court in con-  
21          nection with the matter in which  
22          the amicus curiae has been ap-  
23          pointed, including access to any  
24          relevant legal precedent (includ-  
25          ing any such precedent that is

1 cited by the Government, includ-  
2 ing in such an application);

3 “(bb) an unredacted copy of  
4 each relevant decision made by  
5 the Foreign Intelligence Surveil-  
6 lance Court or the Foreign Intel-  
7 ligence Surveillance Court of Re-  
8 view in which the court decides a  
9 question of law, without regard  
10 to whether the decision is classi-  
11 fied; and

12 “(cc) any other information  
13 or materials that the court deter-  
14 mines are relevant to the duties  
15 of the amicus curiae; and

16 “(II) may make a submission to  
17 the court requesting access to any  
18 other particular materials or informa-  
19 tion (or category of materials or infor-  
20 mation) that the amicus curiae be-  
21 lieves to be relevant to the duties of  
22 the amicus curiae.

23 “(ii) SUPPORTING DOCUMENTATION  
24 REGARDING ACCURACY.—The Foreign In-  
25 telligence Surveillance Court, upon the mo-

1           tion of an amicus curiae appointed under  
2           paragraph (2) or upon its own motion,  
3           may require the Government to make  
4           available the supporting documentation de-  
5           scribed in section 902.”.

6           (B) CLARIFICATION OF ACCESS TO CER-  
7           TAIN INFORMATION.—Section 103(i)(6) of the  
8           Foreign Intelligence Surveillance Act of 1978  
9           (50 U.S.C. 1803(i)(6)) is amended—

10           (i) in subparagraph (B), by striking  
11           “may” and inserting “shall”; and

12           (ii) by striking subparagraph (C) and  
13           inserting the following:

14           “(C) CLASSIFIED INFORMATION.—An ami-  
15           cus curiae designated or appointed by the court  
16           shall have access, to the extent such informa-  
17           tion is available to the Government, to  
18           unredacted copies of each opinion, order, tran-  
19           script, pleading, or other document of the For-  
20           eign Intelligence Surveillance Court and the  
21           Foreign Intelligence Surveillance Court of Re-  
22           view, including, if the individual is eligible for  
23           access to classified information, any classified  
24           documents, information, and other materials or  
25           proceedings.”.

1           (4) **EFFECTIVE DATE.**—The amendments made  
2           by this section shall take effect on the date of enact-  
3           ment of this Act and shall apply with respect to pro-  
4           ceedings under the Foreign Intelligence Surveillance  
5           Act of 1978 (50 U.S.C. 1801 et seq.) that take place  
6           on or after, or are pending on, that date.

7   **SEC. 6. APPLICATION FOR AN ORDER APPROVING ELEC-**  
8                                   **TRONIC SURVEILLANCE.**

9           (a) **DISCLOSURE REQUIREMENT.**—Section 104(a) of  
10          the Foreign Intelligence Surveillance Act of 1978 (50  
11          U.S.C. 1804(a)) is amended—

12                  (1) in paragraph (6)(E)(ii), by inserting before  
13                  the semicolon at the end “(and a description of such  
14                  techniques)”;

15                  (2) in paragraph (8), by striking “and” at the  
16                  end;

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

19                  (4) by inserting after paragraph (9) the fol-  
20                  lowing:

21                          “(10) all information material to the applica-  
22                          tion, including any information that tends to  
23                          rebut—

24    “(A) any allegation set forth in the appli-  
25    cation; or



1           “(B) the existence of probable cause to be-  
2           lieve that—

3                   “(i) the target of the electronic sur-  
4                   veillance is a foreign power or an agent of  
5                   a foreign power; and

6                   “(ii) each of the facilities or places at  
7                   which the electronic surveillance is directed  
8                   is being used, or is about to be used, by a  
9                   foreign power or an agent of a foreign  
10                  power; and

11                 “(11) an affidavit executed by each Federal em-  
12                 ployee who contributed to the drafting of the appli-  
13                 cation attesting to the accuracy of the application.”.

14                 (b) PROHIBITION ON USE OF CERTAIN INFORMA-  
15                 TION.—Section 104 of the Foreign Intelligence Surveil-  
16                 lance Act of 1978 (50 U.S.C. 1804) is amended by adding  
17                 at the end the following:

18                   “(e) The statement of facts and circumstances under  
19                   subsection (a)(3) may only include information obtained  
20                   from the content of a media source or information gath-  
21                   ered by a political campaign if—

22                   “(1) such information is disclosed in the appli-  
23                   cation as having been so obtained or gathered; and

1           “(2) such information is not the sole source of  
2           the information used to justify the applicant’s belief  
3           described in subsection (a)(3).”.

4           (c) LIMITATION ON ISSUANCE OF ORDER.—Section  
5 105(a) of the Foreign Intelligence Surveillance Act of  
6 1978 (50 U.S.C. 1805(a)) is amended—

7           (1) in paragraph (3), by striking “; and” and  
8           inserting a semicolon;

9           (2) in paragraph (4), by striking the period and  
10          inserting “; and”; and

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

12           “(5) the statement of facts and circumstances  
13          under subsection (a)(3) may only include informa-  
14          tion obtained from the content of a media source or  
15          information gathered by a political campaign if—

16           “(A) such information is disclosed in the  
17          application as having been so obtained or gath-  
18          ered; and

19           “(B) such information is not the sole  
20          source of the information used to justify the ap-  
21          plicant’s belief described in subsection (a)(3).”.

22 **SEC. 7. PUBLIC DISCLOSURE AND DECLASSIFICATION OF**  
23 **CERTAIN DOCUMENTS.**

24          (a) SUBMISSION TO CONGRESS.—Section 601(c)(1)  
25 of the Foreign Intelligence Surveillance Act of 1978 (50

1 U.S.C. 1871(c)) is amended by inserting “, including de-  
2 classified copies that have undergone review under section  
3 602” before “; and”.

4 (b) **TIMELINE FOR DECLASSIFICATION REVIEW.**—  
5 Section 602(a) of the Foreign Intelligence Surveillance  
6 Act of 1978 (50 U.S.C. 1872(a)) is amended—

7 (1) by inserting after “shall conduct a declas-  
8 sification review” the following: “, to be concluded  
9 not later than 45 days after the commencement of  
10 such review,”; and

11 (2) by inserting after “a significant construc-  
12 tion or interpretation of any provision of law” the  
13 following: “or results in a change of application of  
14 any provision of this Act or a novel application of  
15 any provision of this Act”.

16 **SEC. 8. TRANSCRIPTIONS OF PROCEEDINGS; ATTENDANCE**  
17 **OF CERTAIN CONGRESSIONAL OFFICIALS AT**  
18 **CERTAIN PROCEEDINGS.**

19 Section 103(c) of the Foreign Intelligence Surveil-  
20 lance Act of 1978 (50 U.S.C. 1803(c)) is amended—

21 (1) by striking “Proceedings under this Act”  
22 and inserting the following: “(1) Proceedings under  
23 this Act”;

24 (2) by striking “including applications made  
25 and orders granted” and inserting “including appli-

1 cations made, orders granted, and transcriptions of  
2 proceedings,”; and

3 (3) by adding at the end:

4 “(2) The chair and ranking minority member of each  
5 of the congressional intelligence committees and of the  
6 Committees on the Judiciary of the House of Representa-  
7 tives and of the Senate shall be entitled to attend any pro-  
8 ceeding of the Foreign Intelligence Surveillance Court or  
9 any proceeding of the Foreign Intelligence Surveillance  
10 Court of Review. Each person entitled to attend a pro-  
11 ceeding pursuant to this paragraph may designate not  
12 more than 2 Members of Congress and not more than 2  
13 staff members of such committee to attend on their behalf,  
14 pursuant to such procedures as the Attorney General, in  
15 consultation with the Director of National Intelligence  
16 may establish. Not later than 45 days after any such pro-  
17 ceeding, a copy of any application made, order granted,  
18 or transcription of the proceeding shall be made available  
19 for review to each person who is entitled to attend a pro-  
20 ceeding pursuant to this paragraph or who is designated  
21 under this paragraph. Terms used in this paragraph have  
22 the meanings given such terms in section 701(b).”.

1 **SEC. 9. ANNUAL AUDIT OF FISA COMPLIANCE BY INSPEC-**  
2 **TOR GENERAL.**

3 (a) REPORT REQUIRED.—Title VI of the Foreign In-  
4 telligence Surveillance Act of 1978 (50 U.S.C. 1871 et  
5 seq.) is amended by adding at the end the following:

6 **“SEC. 605. ANNUAL AUDIT OF FISA COMPLIANCE BY IN-**  
7 **SPECTOR GENERAL.**

8 “Beginning with the first calendar year that begins  
9 after the effective date of this section, by not later than  
10 June 30th of that year and each year thereafter, the In-  
11 spector General of the Department of Justice shall con-  
12 duct an audit on alleged violations and failures to comply  
13 with the requirements of this Act and any procedures es-  
14 tablished pursuant to this Act, and submit a report there-  
15 on to the congressional intelligence committees and the  
16 Committees on the Judiciary of the House of Representa-  
17 tives and of the Senate.”.

18 (b) CLERICAL AMENDMENT.—The table of contents  
19 for the Foreign Intelligence Surveillance Act of 1978 (50  
20 U.S.C. 1801 et seq.) is amended by adding at the end  
21 the following:

“605. Annual audit of FISA compliance by Inspector General.”.

22 **SEC. 10. REPORTING ON ACCURACY AND COMPLETENESS**  
23 **OF APPLICATIONS.**

24 Section 603 of the Foreign Intelligence Surveillance  
25 Act of 1978 (50 U.S.C. 1873) is amended—

1 (1) in subsection (a)(1)—

2 (A) by redesignating subparagraphs (B)  
3 through (F) as subparagraphs (C) through (G)  
4 respectively; and

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

7 “(B) an analysis of the accuracy and com-  
8 pleteness of such applications and certifications  
9 submitted;” and

10 (2) in subsection (a)(2), by striking “subpara-  
11 graph (F)” and inserting “subparagraph (G)”.

12 **SEC. 11. ANNUAL REPORT OF THE FEDERAL BUREAU OF IN-**  
13 **VESTIGATION.**

14 (a) REPORT REQUIRED.—Title VI of the Foreign In-  
15 telligence Surveillance Act of 1978 (50 U.S.C. 1871 et  
16 seq.), as amended by this Act, is further amended by add-  
17 ing at the end the following:

18 **“SEC. 606. ANNUAL REPORT OF THE FEDERAL BUREAU OF**  
19 **INVESTIGATION.**

20 “Not later than 1 year after the date of enactment  
21 of this section, and annually thereafter, the Director of  
22 the Federal Bureau of Investigation shall submit to the  
23 congressional intelligence committees and the Committees  
24 on the Judiciary of the House of Representatives and of  
25 the Senate—

1           “(1) a report on disciplinary activities taken by  
2           the Director to address violations of the require-  
3           ments of law or the procedures established under  
4           this Act, including a comprehensive account of dis-  
5           ciplinary investigations, including—

6                   “(A) all such investigations ongoing as of  
7                   the date the report is submitted;

8                   “(B) the adjudications of such investiga-  
9                   tions when concluded; and

10                   “(C) disciplinary actions taken as a result  
11                   of such adjudications; and

12           “(2) a report on the conduct of queries con-  
13           ducted under section 702 for the preceding year  
14           using a United States person query term, includ-  
15           ing—

16                   “(A) the number of such queries con-  
17                   ducted;

18                   “(B) what terms were used;

19                   “(C) the number of warrants issued and  
20                   denied under section 702(f)(1); and

21                   “(D) the number of times exceptions were  
22                   alleged under 702(f)(2).”.

23           (b) CLERICAL AMENDMENT.—The table of contents  
24           for the Foreign Intelligence Surveillance Act of 1978 (50

1 U.S.C. 1801 et seq.), as amended by this Act, is further  
2 amended by adding at the end the following:

“606. Annual report of the Federal Bureau of Investigation.”.

3 **SEC. 12. EXTENSION OF TITLE VII OF FISA; EXPIRATION OF**  
4 **FISA AUTHORITIES; EFFECTIVE DATES.**

5 (a) **EFFECTIVE DATES.**—Section 403(b) of the FISA  
6 Amendments Act of 2008 (Public Law 110–261; 122 Stat.  
7 2474) is amended—

8 (1) in paragraph (1)—

9 (A) by striking “December 31, 2023” and  
10 inserting “December 31, 2026”; and

11 (B) by striking “, as amended by section  
12 101 and by the FISA Amendments Reauthor-  
13 ization Act of 2017,” and inserting “, as most  
14 recently amended,”; and

15 (2) in paragraph (2) in the matter preceding  
16 subparagraph (A), by striking “December 31, 2023”  
17 and inserting “December 31, 2026”.

18 (b) **CONFORMING AMENDMENTS.**—Section 404(b) of  
19 the FISA Amendments Act of 2008 (Public Law 110–261;  
20 122 Stat. 2476), is amended—

21 (1) in paragraph (1)—

22 (A) in the heading, by striking “DECEM-  
23 BER 31, 2023” and inserting “DECEMBER 31,  
24 2026”; and



1 (B) by striking “, as amended by section  
2 101(a) and by the FISA Amendments Reau-  
3 thorization Act of 2017,” and inserting “, as  
4 most recently amended,”;

5 (2) in paragraph (2), by striking “, as amended  
6 by section 101(a) and by the FISA Amendments Re-  
7 authorization Act of 2017,” and inserting “, as most  
8 recently amended,”; and

9 (3) in paragraph (4)—

10 (A) by striking “, as added by section  
11 101(a) and amended by the FISA Amendments  
12 Reauthorization Act of 2017,” both places it  
13 appears and inserting “, as added by section  
14 101(a) and as most recently amended,”; and

15 (B) by striking “, as amended by section  
16 101(a) and by the FISA Amendments Reau-  
17 thorization Act of 2017,” and inserting “, as  
18 most recently amended,” both places it appears.

19 **SEC. 13. CRIMINAL PENALTIES FOR VIOLATIONS OF FISA.**

20 (a) **IN GENERAL.**—Section 109 of the Foreign Intel-  
21 ligence Surveillance Act of 1978 (50 U.S.C. 1809) is  
22 amended as follows:

23 (1) **ADDITIONAL OFFENSES.**—In subsection  
24 (a)—

1 (A) in the matter preceding paragraph (1),  
2 by striking “intentionally”;

3 (B) in paragraph (1)—

4 (i) by inserting “intentionally” before  
5 “engages in”; and

6 (ii) by striking “or” at the end;

7 (C) in paragraph (2)—

8 (i) by inserting “intentionally” before  
9 “discloses or uses”; and

10 (ii) by striking the period at the end  
11 and inserting a semicolon; and

12 (D) by adding at the end the following: .

13 “(3) knowingly submits any document to or  
14 makes any false statement before the Foreign Intel-  
15 ligence Surveillance Court or the Foreign Intel-  
16 ligence Surveillance Court of Review, knowing such  
17 document or statement to contain—

18 “(A) a false material declaration; or

19 “(B) a material omission; or

20 “(4) knowingly discloses the existence of an ap-  
21 plication for an order authorizing surveillance under  
22 this title, or any information contained therein, to  
23 any person not authorized to receive such informa-  
24 tion.”.

1           (2) ENHANCED PENALTIES.—In subsection (c),  
2           is amended to read as follows:

3           “(c) PENALTIES.—In the case of an offense under  
4 any of paragraphs (1) through (4) of subsection (a), the  
5 offense is punishable by a fine of not more than \$10,000  
6 or imprisonment for not more than 8 years, or both.”.

7           (b) RULE OF CONSTRUCTION.—This Act and the  
8 amendments made by this Act may not be construed to  
9 interfere with the enforcement of section 798 of title 18,  
10 United States Code, or any other provision of law regard-  
11 ing the unlawful disclosure of classified information.

12 **SEC. 14. CONTEMPT POWER OF FISC AND FISC-R.**

13           (a) IN GENERAL.—Chapter 21 of title 18, United  
14 States Code, is amended—

15           (1) in section 402, by inserting after “any dis-  
16 trict court of the United States” the following: “,  
17 the Foreign Intelligence Surveillance Court, the For-  
18 eign Intelligence Surveillance Court of Review,”; and

19           (2) by adding at the end the following:

20 **“§ 404. Definitions**

21           “For purposes of this chapter—

22           “(1) the term ‘court of the United States’ in-  
23 cludes the Foreign Intelligence Surveillance Court or  
24 the Foreign Intelligence Surveillance Court of Re-  
25 view; and

1           “(2) the terms ‘Foreign Intelligence Surveil-  
2           lance Court’ and ‘Foreign Intelligence Surveillance  
3           Court of Review’ have the meanings given such  
4           terms in section 601(e) of the Foreign Intelligence  
5           Surveillance Act of 1978.”.

6           (b) CLERICAL AMENDMENT.—The table of sections  
7           for such chapter is amended by inserting after the item  
8           pertaining to section 403 the following:

          “404. Definitions.”.

9           (c) REPORT.—Not later than one year after the date  
10          of enactment, and annually thereafter the Foreign Intel-  
11          ligence Surveillance Court and the Foreign Intelligence  
12          Surveillance Court of Review (as such terms are defined  
13          in section 601(e) of the Foreign Intelligence Surveillance  
14          Act of 1978) shall jointly submit to Congress a report on  
15          the exercise of authority under chapter 21 of title 18,  
16          United States Code, by such courts during the previous  
17          year.

18       **SEC. 15. INCREASED PENALTIES FOR CIVIL ACTIONS.**

19          (a) INCREASED PENALTIES.—Section 110(a) of the  
20          Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.  
21          1810(a)) is amended to read as follows:

22               “(a) actual damages, but not less than liq-  
23               uidated damages equal to the greater of—



1 **SEC. 16. ACCOUNTABILITY PROCEDURES FOR INCIDENTS**  
2 **RELATING TO QUERIES CONDUCTED BY THE**  
3 **FEDERAL BUREAU OF INVESTIGATION.**

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

7 **“SEC. 709. ACCOUNTABILITY PROCEDURES FOR INCIDENTS**  
8 **RELATING TO QUERIES CONDUCTED BY THE**  
9 **FEDERAL BUREAU OF INVESTIGATION.**

10 “(a) IN GENERAL.—The Director of the Federal Bu-  
11 reau of Investigation shall establish procedures to hold  
12 employees of the Federal Bureau of Investigation account-  
13 able for violations of law, guidance, and procedure gov-  
14 erning queries of information acquired pursuant to section  
15 702.

16 “(b) ELEMENTS.—The procedures established under  
17 subsection (a) shall include the following:

18 “(1) Centralized tracking of individual employee  
19 performance incidents involving negligent violations  
20 of law, guidance, and procedure described in sub-  
21 section (a), over time.

22 “(2) Escalating consequences for such inci-  
23 dents, including—

24 “(A) consequences for initial incidents, in-  
25 cluding, at a minimum—

1 “(i) suspension of access to informa-  
2 tion acquired under this Act; and

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

6 “(B) consequences for subsequent inci-  
7 dents, including, at a minimum—

8 “(i) possible indefinite suspension of  
9 access to information acquired under this  
10 Act;

11 “(ii) reassignment of each employee  
12 responsible for the violation; and

13 “(iii) referral of the incident to the  
14 Inspection Division of the Federal Bureau  
15 of Investigation for review of potentially  
16 reckless conduct.

17 “(3) Clarification of requirements for referring  
18 intentional misconduct and reckless conduct to the  
19 Inspection Division of the Federal Bureau of Inves-  
20 tigation for investigation and disciplinary action by  
21 the Office of Professional Responsibility of the Fed-  
22 eral Bureau of Investigation.”.

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

“709. Accountability procedures for incidents relating to queries conducted by the Federal Bureau of Investigation.”.

1 (c) REPORT REQUIRED.—

2 (1) INITIAL REPORT.—Not later than 180 days  
3 after the date of the enactment of this Act, the Di-  
4 rector of the Federal Bureau of Investigation shall  
5 submit to the Committees on the Judiciary of the  
6 House of Representatives and of the Senate and to  
7 the congressional intelligence committees (as such  
8 term is defined in section 801 of the Foreign Intel-  
9 ligence Surveillance Act of 1978 (50 U.S.C. 1885))  
10 a report detailing the procedures established under  
11 section 709 of the Foreign Intelligence Surveillance  
12 Act of 1978, as added by subsection (a).

13 (2) ANNUAL REPORT.—Not later than 1 year  
14 after the date of enactment of this Act, and annually  
15 thereafter, the Federal Bureau of Investigation shall  
16 submit to the Committees on the Judiciary of the  
17 House of Representatives and of the Senate and to  
18 the congressional intelligence committees (as such  
19 term is defined in section 801 of the Foreign Intel-  
20 ligence Surveillance Act of 1978 (50 U.S.C. 1885))  
21 a report on any disciplinary actions taken pursuant  
22 to the procedures established under section 709 of  
23 the Foreign Intelligence Surveillance Act of 1978, as  
24 added by subsection (a), including a description of



1 the circumstances surrounding each such discipli-  
2 nary action, and the results of each such disciplinary  
3 action.

4 (3) FORM.—The reports required under para-  
5 graphs (1) and (2) shall be submitted in unclassified  
6 form, but may include a classified annex to the ex-  
7 tent necessary to protect sources and methods.

8 **SEC. 17. AGENCY PROCEDURES TO ENSURE COMPLIANCE.**

9 (a) AGENCY PROCEDURES TO ENSURE COMPLI-  
10 ANCE.—Title VI of the Foreign Intelligence Surveillance  
11 Act of 1978 (50 U.S.C. 1871 et seq.), as amended by this  
12 Act, is further amended by adding at the end the fol-  
13 lowing:

14 **“SEC. 607. AGENCY PROCEDURES TO ENSURE COMPLI-**  
15 **ANCE.**

16 “The head of each Federal department or agency au-  
17 thorized to acquire foreign intelligence information under  
18 this Act shall establish procedures—

19 “(1) setting forth clear rules on what con-  
20 stitutes a violation of this Act by an officer or em-  
21 ployee of that department or agency; and

22 “(2) for taking appropriate adverse personnel  
23 action against any officer or employee of the depart-  
24 ment or agency who engages in such a violation, in-

1 including more severe adverse actions for any subse-  
2 quent violation.”.

3 (b) CLERICAL AMENDMENT.—The table of contents  
4 for the Foreign Intelligence Surveillance Act of 1978 (50  
5 U.S.C. 1801 et seq.), as amended by this Act, is further  
6 amended by adding at the end the following:

“607. Agency procedures to ensure compliance.”.

7 (c) REPORT.—Not later than 3 months after the date  
8 of enactment of this Act, the head of each Federal depart-  
9 ment or agency that is required to establish procedures  
10 under section 607 of the Foreign Intelligence Surveillance  
11 Act of 1978 shall report to Congress on such procedures.

12 **SEC. 18. PROTECTION OF RECORDS HELD BY DATA BRO-**  
13 **KERS.**

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

16 “(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR  
17 ANYTHING OF VALUE CERTAIN RECORDS AND INFORMA-  
18 TION BY LAW ENFORCEMENT AND INTELLIGENCE AGEN-  
19 CIES.—

20 “(1) DEFINITIONS.—In this subsection—

21 “(A) the term ‘covered customer or sub-  
22 scriber record’ means a covered record that is—

23 “(i) disclosed to a third party by—

24 “(I) a provider of an electronic  
25 communication service to the public or

1 a provider of a remote computing  
2 service of which the covered person  
3 with respect to the covered record is a  
4 subscriber or customer; or

5 “(II) an intermediary service pro-  
6 vider that delivers, stores, or proc-  
7 esses communications of such covered  
8 person;

9 “(ii) collected by a third party from  
10 an online account of a covered person; or

11 “(iii) collected by a third party from  
12 or about an electronic device of a covered  
13 person;

14 “(B) the term ‘covered person’ means—

15 “(i) a person who is located inside the  
16 United States; or

17 “(ii) a person—

18 “(I) who is located outside the  
19 United States or whose location can-  
20 not be determined; and

21 “(II) who is a United States per-  
22 son, as defined in section 101 of the  
23 Foreign Intelligence Surveillance Act  
24 of 1978 (50 U.S.C. 1801);

1           “(C) the term ‘covered record’ means a  
2 record or other information that—

3           “(i) pertains to a covered person; and

4           “(ii) is—

5           “(I) a record or other informa-  
6 tion described in the matter preceding  
7 paragraph (1) of subsection (c);

8           “(II) the contents of a commu-  
9 nication; or

10           “(III) location information;

11           “(D) the term ‘electronic device’ has the  
12 meaning given the term ‘computer’ in section  
13 1030(e);

14           “(E) the term ‘illegitimately obtained in-  
15 formation’ means a covered record that—

16           “(i) was obtained—

17           “(I) from a provider of an elec-  
18 tronic communication service to the  
19 public or a provider of a remote com-  
20 puting service in a manner that—

21           “(aa) violates the service  
22 agreement between the provider  
23 and customers or subscribers of  
24 the provider; or

1                   “(bb) is inconsistent with  
2                   the privacy policy of the provider;

3                   “(II) by deceiving the covered  
4                   person whose covered record was ob-  
5                   tained; or

6                   “(III) through the unauthorized  
7                   accessing of an electronic device or  
8                   online account; or

9                   “(ii) was—

10                   “(I) obtained from a provider of  
11                   an electronic communication service to  
12                   the public, a provider of a remote  
13                   computing service, or an intermediary  
14                   service provider; and

15                   “(II) collected, processed, or  
16                   shared in violation of a contract relat-  
17                   ing to the covered record;

18                   “(F) the term ‘intelligence community’ has  
19                   the meaning given that term in section 3 of the  
20                   National Security Act of 1947 (50 U.S.C.  
21                   3003);

22                   “(G) the term ‘location information’ means  
23                   information derived or otherwise calculated  
24                   from the transmission or reception of a radio  
25                   signal that reveals the approximate or actual

1 geographic location of a customer, subscriber,  
2 or device;

3 “(H) the term ‘obtain in exchange for any-  
4 thing of value’ means to obtain by purchasing,  
5 to receive in connection with services being pro-  
6 vided for consideration, or to otherwise obtain  
7 in exchange for consideration, including an ac-  
8 cess fee, service fee, maintenance fee, or licens-  
9 ing fee;

10 “(I) the term ‘online account’ means an  
11 online account with an electronic communica-  
12 tion service to the public or remote computing  
13 service;

14 “(J) the term ‘pertain’, with respect to a  
15 person, means—

16 “(i) information that is linked to the  
17 identity of a person; or

18 “(ii) information—

19 “(I) that has been anonymized to  
20 remove links to the identity of a per-  
21 son; and

22 “(II) that, if combined with other  
23 information, could be used to identify  
24 a person; and

1           “(K) the term ‘third party’ means a person  
2           who—

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

4                   “(ii) in connection with the collection,  
5           disclosure, obtaining, processing, or shar-  
6           ing of the covered record at issue, was not  
7           acting as—

8                   “(I) a provider of an electronic  
9                   communication service to the public;

10                   or

11                   “(II) a provider of a remote com-  
12           puting service.

13           “(2) LIMITATION.—

14                   “(A) IN GENERAL.—A law enforcement  
15           agency of a governmental entity and an element  
16           of the intelligence community may not obtain  
17           from a third party in exchange for anything of  
18           value a covered customer or subscriber record  
19           or any illegitimately obtained information.

20                   “(B) INDIRECTLY ACQUIRED RECORDS  
21           AND INFORMATION.—The limitation under sub-  
22           paragraph (A) shall apply without regard to  
23           whether the third party possessing the covered  
24           customer or subscriber record or illegitimately  
25           obtained information is the third party that ini-

1           tially obtained or collected, or is the third party  
2           that initially received the disclosure of, the cov-  
3           ered customer or subscriber record or illegit-  
4           imately obtained information.

5           “(3) LIMIT ON SHARING BETWEEN AGEN-  
6           CIES.—An agency of a governmental entity that is  
7           not a law enforcement agency or an element of the  
8           intelligence community may not provide to a law en-  
9           forcement agency of a governmental entity or an ele-  
10          ment of the intelligence community a covered cus-  
11          tomer or subscriber record or illegitimately obtained  
12          information that was obtained from a third party in  
13          exchange for anything of value.

14          “(4) PROHIBITION ON USE AS EVIDENCE.—A  
15          covered customer or subscriber record or illegit-  
16          imately obtained information obtained by or pro-  
17          vided to a law enforcement agency of a governmental  
18          entity or an element of the intelligence community in  
19          violation of paragraph (2) or (3), and any evidence  
20          derived therefrom, may not be received in evidence  
21          in any trial, hearing, or other proceeding in or be-  
22          fore any court, grand jury, department, officer,  
23          agency, regulatory body, legislative committee, or  
24          other authority of the United States, a State, or a  
25          political subdivision thereof.



1 “(5) MINIMIZATION PROCEDURES.—

2 “(A) IN GENERAL.—The Attorney General  
3 shall adopt specific procedures that are reason-  
4 ably designed to minimize the acquisition and  
5 retention, and prohibit the dissemination, of in-  
6 formation pertaining to a covered person that is  
7 acquired in violation of paragraph (2) or (3).

8 “(B) USE BY AGENCIES.—If a law enforce-  
9 ment agency of a governmental entity or ele-  
10 ment of the intelligence community acquires in-  
11 formation pertaining to a covered person in vio-  
12 lation of paragraph (2) or (3), the law enforce-  
13 ment agency of a governmental entity or ele-  
14 ment of the intelligence community shall mini-  
15 mize the acquisition and retention, and prohibit  
16 the dissemination, of the information in accord-  
17 ance with the procedures adopted under sub-  
18 paragraph (A).”.

19 **SEC. 19. REQUIRED DISCLOSURE.**

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

22 “(i) COVERED CUSTOMER OR SUBSCRIBER RECORDS  
23 AND ILLEGITIMATELY OBTAINED INFORMATION.—

24 “(1) DEFINITIONS.—In this subsection, the  
25 terms ‘covered customer or subscriber record’, ‘ille-

1       gitimately obtained information’, and ‘third party’  
2       have the meanings given such terms in section  
3       2702(e).

4               “(2) LIMITATION.—Unless a governmental enti-  
5       ty obtains an order in accordance with paragraph  
6       (3), the governmental entity may not require a third  
7       party to disclose a covered customer or subscriber  
8       record or any illegitimately obtained information if a  
9       court order would be required for the governmental  
10      entity to require a provider of remote computing  
11      service or a provider of electronic communication  
12      service to the public to disclose such a covered cus-  
13      tomer or subscriber record or illegitimately obtained  
14      information that is a record of a customer or sub-  
15      scriber of the provider.

16              “(3) ORDERS.—

17                      “(A) IN GENERAL.—A court may only  
18                      issue an order requiring a third party to dis-  
19                      close a covered customer or subscriber record or  
20                      any illegitimately obtained information on the  
21                      same basis and subject to the same limitations  
22                      as would apply to a court order to require dis-  
23                      closure by a provider of remote computing serv-  
24                      ice or a provider of electronic communication

1 service to the public of a record of a customer  
2 or subscriber of the provider.

3 “(B) STANDARD.—For purposes of sub-  
4 paragraph (A), a court shall apply the most  
5 stringent standard under Federal statute or the  
6 Constitution of the United States that would be  
7 applicable to a request for a court order to re-  
8 quire a comparable disclosure by a provider of  
9 remote computing service or a provider of elec-  
10 tronic communication service to the public of a  
11 record of a customer or subscriber of the pro-  
12 vider.”.

13 **SEC. 20. INTERMEDIARY SERVICE PROVIDERS.**

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

16 (1) in paragraph (3), by striking “and” at the  
17 end;

18 (2) in paragraph (4), by striking the period at  
19 the end and inserting “; and”; and

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

21 “(5) the term ‘intermediary service provider’  
22 means an entity or facilities owner or operator that  
23 directly or indirectly delivers, stores, or processes  
24 communications for or on behalf of a provider of

1 electronic communication service to the public or a  
2 provider of remote computing service.”.

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

5 (1) in paragraph (1), by striking “and” at the  
6 end;

7 (2) in paragraph (2), by striking “and” at the  
8 end;

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

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

12 “(4) an intermediary service provider shall not  
13 knowingly divulge—

14 “(A) to any person or entity the contents  
15 of a communication while in electronic storage  
16 by that provider; or

17 “(B) to any governmental entity a record  
18 or other information pertaining to a subscriber  
19 to or customer of, a recipient of a communica-  
20 tion from a subscriber to or customer of, or the  
21 sender of a communication to a subscriber to or  
22 customer of, the provider of electronic commu-  
23 nication service to the public or the provider of  
24 remote computing service for, or on behalf of,  
25 which the intermediary service provider directly

1           or indirectly delivers, transmits, stores, or proc-  
2           esses communications.”.

3 **SEC. 21. LIMITS ON SURVEILLANCE CONDUCTED FOR FOR-**  
4 **EIGN INTELLIGENCE PURPOSES OTHER**  
5 **THAN UNDER THE FOREIGN INTELLIGENCE**  
6 **SURVEILLANCE ACT OF 1978.**

7       (a) IN GENERAL.—Section 2511(2)(f) of title 18,  
8 United States Code, is amended to read as follows:

9       “(f)(i)(A) Nothing contained in this chapter, chapter  
10 121 or 206 of this title, or section 705 of the Communica-  
11 tions Act of 1934 (47 U.S.C. 151 et seq.) shall be deemed  
12 to affect an acquisition or activity described in clause (B)  
13 that is carried out utilizing a means other than electronic  
14 surveillance, as defined in section 101 of the Foreign In-  
15 telligence Surveillance Act of 1978 (50 U.S.C. 1801).

16       “(B) An acquisition or activity described in this  
17 clause is—

18           “(I) an acquisition by the United States Gov-  
19 ernment of foreign intelligence information from  
20 international or foreign communications that—

21               “(aa) is acquired pursuant to express stat-  
22 utory authority; or

23               “(bb) only includes information of persons  
24 who are not United States persons and are lo-  
25 cated outside the United States; or

1           “(II) a foreign intelligence activity involving a  
2 foreign electronic communications system that—

3           “(aa) is conducted pursuant to express  
4 statutory authority; or

5           “(bb) only involves the acquisition by the  
6 United States Government of information of  
7 persons who are not United States persons and  
8 are located outside the United States.

9           “(ii) The procedures in this chapter, chapter 121,  
10 and the Foreign Intelligence Surveillance Act of 1978 (50  
11 U.S.C. 1801 et seq.) shall be the exclusive means by which  
12 electronic surveillance, as defined in section 101 of such  
13 Act, and the interception of domestic wire, oral, and elec-  
14 tronic communications may be conducted.”.

15           (b) EXCLUSIVE MEANS RELATED TO COMMUNICA-  
16 TIONS RECORDS.—The Foreign Intelligence Surveillance  
17 Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive  
18 means by which electronic communications transactions  
19 records, call detail records, or other information from com-  
20 munications of United States persons or persons inside the  
21 United States are acquired for foreign intelligence pur-  
22 poses inside the United States or from a person or entity  
23 located in the United States that provides telecommuni-  
24 cations, electronic communication, or remote computing  
25 services.

1 (c) EXCLUSIVE MEANS RELATED TO LOCATION IN-  
2 FORMATION, WEB BROWSING HISTORY, AND INTERNET  
3 SEARCH HISTORY.—

4 (1) DEFINITION.—In this subsection, the term  
5 “location information” has the meaning given that  
6 term in subsection (e) of section 2702 of title 18,  
7 United States Code, as added by section 2 of this  
8 Act.

9 (2) EXCLUSIVE MEANS.—Title I and sections  
10 303, 304, 703, 704, and 705 of the Foreign Intel-  
11 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et  
12 seq., 1823, 1824, 1881b, 1881c, 1881d) shall be the  
13 exclusive means by which location information, web  
14 browsing history, and internet search history of  
15 United States persons or persons inside the United  
16 States are acquired for foreign intelligence purposes  
17 inside the United States or from a person or entity  
18 located in the United States.

19 (d) EXCLUSIVE MEANS RELATED TO FOURTH  
20 AMENDMENT-PROTECTED INFORMATION.—Title I and  
21 sections 303, 304, 703, 704, and 705 of the Foreign Intel-  
22 ligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.,  
23 1823, 1824, 1881b, 1881c, 1881d) shall be the exclusive  
24 means by which any information, records, data, or tangible  
25 things are acquired for foreign intelligence purposes from

1 a person or entity located in the United States if the com-  
2 pelled production of such information, records, data, or  
3 tangible things would require a warrant for law enforce-  
4 ment purposes.

5 (e) DEFINITION.—In this section, the term “United  
6 States person” has the meaning given that term in section  
7 101 of the Foreign Intelligence Surveillance Act of 1978  
8 (50 U.S.C. 1801).

9 **SEC. 22. LIMIT ON CIVIL IMMUNITY FOR PROVIDING INFOR-**  
10 **MATION, FACILITIES, OR TECHNICAL ASSIST-**  
11 **ANCE TO THE GOVERNMENT ABSENT A**  
12 **COURT ORDER.**

13 Section 2511(2)(a) of title 18, United States Code,  
14 is amended—

15 (1) in subparagraph (ii), by striking clause (B)  
16 and inserting the following:

17 “(B) a certification in writing—

18 “(I) by a person specified in section  
19 2518(7) or the Attorney General of the United  
20 States;

21 “(II) that the requirements for an emer-  
22 gency authorization to intercept a wire, oral, or  
23 electronic communication under section 2518(7)  
24 have been met; and



1                   “(III) that the specified assistance is re-  
2                   quired,”; and

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

5                   “(iii) For assistance provided pursuant to a certifi-  
6                   cation under subparagraph (ii)(B), the limitation on  
7                   causes of action under the last sentence of the matter fol-  
8                   lowing subparagraph (ii)(B) shall only apply to the extent  
9                   that the assistance ceased at the earliest of the time the  
10                  application for a court order was denied, the time the com-  
11                  munication sought was obtained, or 48 hours after the  
12                  interception began.”.

