

118TH CONGRESS
2D SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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

A BILL

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

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 “Security And Freedom Enhancement Act of 2024” or the
6 “SAFE Act”.

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

2

Sec. 1. Short title; table of contents.

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

Sec. 101. Query procedure reform.

Sec. 102. Quarterly reports.

Sec. 103. Accountability procedures for incidents relating to queries conducted by the Federal Bureau of Investigation.

Sec. 104. Prohibition on reverse targeting of United States persons and persons located in the United States.

Sec. 105. FISA court review of targeting decisions.

Sec. 106. Repeal of authority for the resumption of abouts collection.

Sec. 107. Extension of title VII of FISA; expiration of FISA authorities; effective dates.

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

Sec. 201. Application for an order under the Foreign Intelligence Surveillance Act of 1978.

Sec. 202. Criminal penalties for violations of FISA.

Sec. 203. Increased penalties for civil actions.

Sec. 204. Agency procedures to ensure compliance.

Sec. 205. Limit on civil immunity for providing information, facilities, or technical assistance to the Government absent a court order.

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

Sec. 301. Foreign Intelligence Surveillance Court reform.

Sec. 302. Public disclosure and declassification of certain documents.

Sec. 303. Submission of court transcripts to Congress.

Sec. 304. Contempt power of FISC and FISCR.

TITLE IV—INDEPENDENT EXECUTIVE BRANCH OVERSIGHT

Sec. 401. Periodic audit of FISA compliance by Inspector General.

Sec. 402. Intelligence community parity and communications with Privacy and Civil Liberties Oversight Board.

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

Sec. 501. Limitation on intelligence acquisition of United States person data.

Sec. 502. Limitation on law enforcement purchase of personal data from data brokers.

Sec. 503. Consistent protections for demands for data held by interactive computing services.

Sec. 504. Consistent privacy protections for data held by data brokers.

Sec. 505. Protection of data entrusted to intermediary or ancillary service providers.

TITLE VI—TRANSPARENCY

Sec. 601. Enhanced reports by Director of National Intelligence.

TITLE VII—LIMITED DELAYS IN IMPLEMENTATION

Sec. 701. Limited delays in implementation.

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. QUERY PROCEDURE REFORM.**

9 (a) MANDATORY AUDITS OF UNITED STATES PER-
10 SON QUERIES CONDUCTED BY FEDERAL BUREAU OF IN-
11 VESTIGATION.—

12 (1) IN GENERAL.—The Department of Justice
13 shall conduct an audit of a significant representative
14 sample of covered queries, as defined in paragraph
15 (6) of section 702(f) of the Foreign Intelligence Sur-
16 veillance Act of 1978 (50 U.S.C. 1881a(f)), as re-
17 designated and amended by subsection (b) of this
18 section, conducted during the 180-day period begin-
19 ning on the date of enactment of this Act, and dur-
20 ing each 180-day period thereafter.

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

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

3 (b) RESTRICTIONS RELATING TO CONDUCT OF CER-
4 TAIN QUERIES BY FEDERAL BUREAU OF INVESTIGA-
5 TION.—Section 702(f) of the Foreign Intelligence Surveil-
6 lance Act of 1978 (50 U.S.C. 1881a(f)) is amended—

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

9 (2) by inserting before paragraph (6) the fol-
10 lowing:

11 “(5) QUERYING PROCEDURES APPLICABLE TO
12 FEDERAL BUREAU OF INVESTIGATION.—For any
13 procedures adopted under paragraph (1) applicable
14 to the Federal Bureau of Investigation, the Attorney
15 General, in consultation with the Director of Na-
16 tional Intelligence, shall include the following re-
17 quirements:

18 “(A) TRAINING.—A requirement that,
19 prior to conducting any query, and on an an-
20 nual basis thereafter as a prerequisite for con-
21 tinuing to conduct queries, personnel of the
22 Federal Bureau of Investigation successfully
23 complete training on the querying procedures.

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

1 sent exigent circumstances, prior to conducting
2 certain queries, personnel of the Federal Bu-
3 reau of Investigation receive approval, at min-
4 imum, as follows:

5 “(i) Approval from the Deputy Direc-
6 tor of the Federal Bureau of Investigation
7 if the query uses a query term reasonably
8 believed to identify a United States elected
9 official, an appointee of the President or
10 the governor of a State, a United States
11 political candidate, a United States polit-
12 ical organization or a United States person
13 prominent in such organization, or a
14 United States media organization or a
15 United States person who is a member of
16 such organization.

17 “(ii) Approval from an attorney of the
18 Federal Bureau of Investigation if the
19 query uses a query term reasonably be-
20 lieved to identify a United States religious
21 organization or a United States person
22 who is prominent in such organization.

23 “(iii) Approval from an attorney of
24 the Federal Bureau of Investigation for 2

1 or more queries conducted together as a
2 batch job.

3 “(C) PRIOR WRITTEN JUSTIFICATION.—A
4 requirement that—

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

12 “(ii) for each covered query, the Fed-
13 eral Bureau of Investigation shall keep a
14 record of the query term, the date of the
15 conduct of the query, the identifier of the
16 personnel conducting the query, and such
17 written statement.

18 “(D) AFFIRMATIVE ELECTION TO INCLUDE
19 SECTION 702 INFORMATION IN QUERIES.—Any
20 system of the Federal Bureau of Investigation
21 that stores unminimized contents or noncon-
22 tents obtained through acquisitions authorized
23 under subsection (a) together with contents or
24 noncontents obtained through other lawful
25 means shall be configured in a manner that—

1 “(i) requires personnel of the Federal
2 Bureau of Investigation to affirmatively
3 elect to include such unminimized contents
4 or noncontents obtained through acquisi-
5 tions authorized under subsection (a) when
6 running a query; or

7 “(ii) includes other controls reason-
8 ably expected to prevent inadvertent que-
9 ries of such unminimized contents or non-
10 contents.”; and

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

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

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

16 “(B) The term ‘covered query’ means a
17 query conducted—

18 “(i) using a term associated with a
19 United States person or a person reason-
20 ably believed to be located in the United
21 States at the time of the query or the time
22 of the communication or creation of the in-
23 formation; or

24 “(ii) for the purpose of finding the in-
25 formation of a United States person or a

1 person reasonably believed to be located in
2 the United States at the time of the query
3 or the time of the communication or cre-
4 ation of the information.”.

5 (c) PROHIBITION ON WARRANTLESS ACCESS TO THE
6 COMMUNICATIONS AND OTHER INFORMATION OF UNITED
7 STATES PERSONS AND PERSONS LOCATED IN THE
8 UNITED STATES.—Section 702(f) of the Foreign Intel-
9 ligence Surveillance Act of 1978 (50 U.S.C. 1881a(f)) is
10 amended—

11 (1) in paragraph (1)(A) by inserting “and the
12 limitations and requirements in paragraph (2)” after
13 “Constitution of the United States”;

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

16 “(2) PROHIBITION ON WARRANTLESS ACCESS
17 TO THE COMMUNICATIONS AND OTHER INFORMA-
18 TION OF UNITED STATES PERSONS AND PERSONS
19 LOCATED IN THE UNITED STATES.—

20 “(A) IN GENERAL.—Except as provided in
21 subparagraphs (B) and (C), no officer or em-
22 ployee of the United States may access commu-
23 nications content, or information the compelled
24 disclosure of which would require a probable
25 cause warrant if sought for law enforcement

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

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

8 “(i) IN GENERAL.—Subparagraph (A)
9 shall not apply if—

10 “(I) the person to whom the
11 query relates is the subject of an
12 order or emergency authorization au-
13 thorizing electronic surveillance, a
14 physical search, or an acquisition
15 under this section or section 105, sec-
16 tion 304, section 703, or section 704
17 of this Act or a warrant issued pursu-
18 ant to the Federal Rules of Criminal
19 Procedure by a court of competent ju-
20 risdiction;

21 “(II)(aa) the officer or employee
22 accessing the communications content
23 or information has a reasonable belief
24 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 the threat described in
6 subitem (AA), the communica-
7 tions content or information
8 must be accessed before author-
9 ization described in subelause (I)
10 can, with due diligence, be ob-
11 tained; and

12 “(bb) not later than 14 days
13 after the communications content or
14 information is accessed, a description
15 of the circumstances justifying the ac-
16 cessing of the query results is pro-
17 vided to the Foreign Intelligence Sur-
18 veillance Court, the congressional in-
19 telligence committees, the Committee
20 on the Judiciary of the House of Rep-
21 resentatives, and the Committee on
22 the Judiciary of the Senate;

23 “(III) such person or, if such
24 person is incapable of providing con-
25 sent, a third party legally authorized

1 to consent on behalf of such person,
2 has provided consent for the access on
3 a case-by-case basis; or

4 “(IV)(aa) the communications
5 content or information is accessed and
6 used for the sole purpose of identi-
7 fying targeted recipients of malicious
8 software and preventing or mitigating
9 harm from such malicious software;

10 “(bb) other than malicious soft-
11 ware and cybersecurity threat signa-
12 tures, no communications content or
13 other information are accessed or re-
14 viewed; and

15 “(cc) the accessing of query re-
16 sults is reported to the Foreign Intel-
17 ligence Surveillance Court.

18 “(ii) LIMITATIONS.—

19 “(I) USE IN SUBSEQUENT PRO-
20 CEEDINGS.—No communications con-
21 tent or information accessed under
22 clause (i)(II) or information derived
23 from such access may be used, re-
24 ceived in evidence, or otherwise dis-
25 seminated in any trial, hearing, or

1 other proceeding in or before any
2 court, grand jury, department, office,
3 agency, regulatory body, legislative
4 committee, or other authority of the
5 United States, a State, or political
6 subdivision thereof, except in a pro-
7 ceeding that arises from the threat
8 that prompted the query.

9 “(II) ASSESSMENT OF COMPLI-
10 ANCE.—Not less frequently than an-
11 nually, the Attorney General shall as-
12 sess compliance with the requirements
13 under subclause (I).

14 “(C) MATTERS RELATING TO EMERGENCY
15 QUERIES.—

16 “(i) TREATMENT OF DENIALS.—In
17 the event that communications content or
18 information returned in response to a cov-
19 ered query are accessed pursuant to an
20 emergency authorization described in sub-
21 paragraph (B)(i)(I) and the subsequent
22 application to authorize electronic surveil-
23 lance, a physical search, or an acquisition
24 pursuant to section 105(e), section 304(e),
25 section 703(d), or section 704(d) of this

1 Act is denied, or in any other case in which
2 communications content or information re-
3 turned in response to a covered query are
4 accessed in violation of this paragraph—

5 “(I) no communications content
6 or information acquired or evidence
7 derived from such access may be used,
8 received in evidence, or otherwise dis-
9 seminated in any investigation by or
10 in any trial, hearing, or other pro-
11 ceeding in or before any court, grand
12 jury, department, office, agency, regu-
13 latory body, legislative committee, or
14 other authority of the United States,
15 a State, or political subdivision there-
16 of; and

17 “(II) no communications content
18 or information acquired or derived
19 from such access may subsequently be
20 used or disclosed in any other manner
21 without the consent of the person to
22 whom the covered query relates, ex-
23 cept in the case that the Attorney
24 General approves the use or disclosure
25 of such information in order to pre-

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

3 “(ii) ASSESSMENT OF COMPLIANCE.—

4 Not less frequently than annually, the At-
5 torney General shall assess compliance
6 with the requirements under clause (i).

7 “(D) FOREIGN INTELLIGENCE PURPOSE.—

8 “(i) IN GENERAL.—Except as pro-
9 vided in clause (ii) of this subparagraph,
10 no officer or employee of the United States
11 may conduct a covered query of informa-
12 tion acquired under subsection (a) unless
13 the query is reasonably likely to retrieve
14 foreign intelligence information.

15 “(ii) EXCEPTIONS.—An officer or em-
16 ployee of the United States may conduct a
17 covered query of information acquired
18 under this section if—

19 “(I)(aa) the officer or employee
20 conducting the query has a reasonable
21 belief that an emergency exists involv-
22 ing an imminent threat of death or se-
23 rious bodily harm; and

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

1 description of the query is provided to
2 the Foreign Intelligence Surveillance
3 Court, the congressional intelligence
4 committees, the Committee on the Ju-
5 diciary of the House of Representa-
6 tives, and the Committee on the Judi-
7 ciary of the Senate;

8 “(II) the person to whom the
9 query relates or, if such person is in-
10 capable of providing consent, a third
11 party legally authorized to consent on
12 behalf of such person, has provided
13 consent for the query on a case-by-
14 case basis;

15 “(III)(aa) the query is conducted,
16 and the results of the query are used,
17 for the sole purpose of identifying tar-
18 geted recipients of malicious software
19 and preventing or mitigating harm
20 from such malicious software;

21 “(bb) other than malicious soft-
22 ware and cybersecurity threat signa-
23 tures, no additional contents of com-
24 munications acquired as a result of

1 the query are accessed or reviewed;
2 and

3 “(cc) the query is reported to the
4 Foreign Intelligence Surveillance
5 Court; or

6 “(IV) the query is necessary to
7 identify information that must be pro-
8 duced or preserved in connection with
9 a litigation matter or to fulfill dis-
10 covery obligations in a criminal matter
11 under the laws of the United States
12 or any State thereof.

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

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

1 to maintain the record described in paragraph (3).
2 Not later than 90 days after the date of enactment
3 of the SAFE Act, the head of each agency that con-
4 ducts queries shall report to Congress on its compli-
5 ance with this procedure.”.

6 (d) CONFORMING AMENDMENTS.—

7 (1) Section 603(b)(2) of the Foreign Intel-
8 ligence Surveillance Act of 1978 (50 U.S.C.
9 1873(b)(2)) is amended, in the matter preceding
10 subparagraph (A), by striking “, including pursuant
11 to subsection (f)(2) of such section,”.

12 (2) Section 706(a)(2)(A)(i) of the Foreign In-
13 telligence Surveillance Act of 1978 (50 U.S.C.
14 1881e(a)(2)(A)(i)) is amended by striking “obtained
15 an order of the Foreign Intelligence Surveillance
16 Court to access such information pursuant to section
17 702(f)(2)” and inserting “accessed such information
18 in accordance with section 702(b)(2)”.

19 **SEC. 102. QUARTERLY REPORTS.**

20 Section 707 of the Foreign Intelligence Surveillance
21 Act of 1978 (50 U.S.C. 1881f) is amended by adding at
22 the end the following:

23 “(c) QUARTERLY REPORTS.—The Attorney General,
24 in consultation with the Director of National Intelligence,
25 shall submit to the congressional intelligence committees,

1 the Committee on the Judiciary of the Senate, and the
2 Committee on the Judiciary of the House of Representa-
3 tives a quarterly report, which shall include, for that quar-
4 ter, disaggregated by each agency that conducts queries
5 of information acquired under section 702, the following
6 information:

7 “(1) The total number of covered queries (as
8 defined in section 702(f)(6)) conducted of informa-
9 tion acquired under section 702.

10 “(2) The number of times an officer or em-
11 ployee of the United States accessed communications
12 contents (as defined in section 2510(8) of title 18,
13 United States Code) or information the compelled
14 disclosure of which would require a probable cause
15 warrant if sought for law enforcement purposes in
16 the United States, returned in response to such que-
17 ries.

18 “(3) The number of applications for orders re-
19 lating to an emergency authorization described in
20 subclause (I) of section 702(f)(2)(B)(i) with respect
21 to a person for which communications contents or
22 information relating to such person were accessed
23 under such subclause and the number of such orders
24 granted.

1 “(4) The number of times an exception sub-
2 clause (II), (III), or (IV) of section 702(f)(2)(B)(i)
3 was asserted, disaggregated by the subclause under
4 which an exception was asserted.”.

5 **SEC. 103. ACCOUNTABILITY PROCEDURES FOR INCIDENTS**
6 **RELATING TO QUERIES CONDUCTED BY THE**
7 **FEDERAL BUREAU OF INVESTIGATION.**

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

11 **“SEC. 709. ACCOUNTABILITY PROCEDURES FOR INCIDENTS**
12 **RELATING TO QUERIES CONDUCTED BY THE**
13 **FEDERAL BUREAU OF INVESTIGATION.**

14 “(a) IN GENERAL.—The Director of the Federal Bu-
15 reau of Investigation shall establish procedures to hold
16 employees of the Federal Bureau of Investigation account-
17 able for violations of law, guidance, and procedure gov-
18 erning queries of information acquired pursuant to section
19 702.

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

22 “(1) Centralized tracking of individual employee
23 performance incidents involving negligent violations
24 of law, guidance, and procedure described in sub-
25 section (a), over time.

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

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

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

7 “(ii) documentation of the incident in
8 the personnel file of each employee respon-
9 sible for the violation; and

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

12 “(i) possible indefinite suspension of
13 access to information acquired under this
14 Act;

15 “(ii) reassignment of each employee
16 responsible for the violation; and

17 “(iii) referral of the incident to the
18 Inspection Division of the Federal Bureau
19 of Investigation for review of potentially
20 reckless conduct.

21 “(3) Clarification of requirements for referring
22 intentional misconduct and reckless conduct to the
23 Inspection Division of the Federal Bureau of Inves-
24 tigation for investigation and disciplinary action by

1 the Office of Professional Responsibility of the Fed-
2 eral Bureau of Investigation.”.

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.) is amended by inserting after the
6 item relating to section 708 the following:

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

7 (c) REPORT REQUIRED.—

8 (1) INITIAL REPORT.—Not later than 180 days
9 after the date of enactment of this Act, the Director
10 of the Federal Bureau of Investigation shall submit
11 to the Committee on the Judiciary of the House of
12 Representatives, the Committee on the Judiciary of
13 the Senate, and the congressional intelligence com-
14 mittees (as such term is defined in section 801 of
15 the Foreign Intelligence Surveillance Act of 1978
16 (50 U.S.C. 1885)) a report detailing the procedures
17 established under section 709 of the Foreign Intel-
18 ligence Surveillance Act of 1978, as added by sub-
19 section (a).

20 (2) ANNUAL REPORT.—Not later than 1 year
21 after the date of enactment of this Act, and annually
22 thereafter, the Federal Bureau of Investigation shall
23 submit to the Committee on the Judiciary of the
24 House of Representatives, the Committee on the Ju-

1 diciary of the Senate, and the congressional intel-
2 ligence committees (as such term is defined in sec-
3 tion 801 of the Foreign Intelligence Surveillance Act
4 of 1978 (50 U.S.C. 1885)) a report on any discipli-
5 nary actions taken pursuant to the procedures estab-
6 lished under section 709 of the Foreign Intelligence
7 Surveillance Act of 1978, as added by subsection
8 (a), including a description of the circumstances sur-
9 rounding each such disciplinary action, and the re-
10 sults of each such disciplinary action.

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

15 **SEC. 104. 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) is amended—

20 (1) in subsection (b)(2)—

21 (A) by striking “may not intentionally”
22 and inserting the following: “may not—
23 “(A) intentionally”; and

24 (B) in subparagraph (A), as designated by
25 subparagraph (A) of this paragraph, by striking

1 “if the purpose of such acquisition is to target
2 a particular, known person reasonably believed
3 to be in the United States;” and inserting the
4 following: “if a significant purpose of such ac-
5 quisition is to target 1 or more United States
6 persons or persons reasonably believed to be lo-
7 cated in the United States at the time of acqui-
8 sition or communication, unless—

9 “(i)(I) there is a reasonable belief that
10 an emergency exists involving an imminent
11 threat of death or serious bodily harm;

12 “(II) the information is necessary to
13 mitigate that threat;

14 “(III) a description of the targeting is
15 provided to the Foreign Intelligence Sur-
16 veillance Court, the congressional intel-
17 ligence committees, the Committee on the
18 Judiciary of the Senate, and the Com-
19 mittee on the Judiciary of the House of
20 Representatives in a timely manner; and

21 “(IV) any information acquired from
22 such targeting is used, received in evi-
23 dence, or otherwise disseminated solely in
24 an investigation by or in a trial, hearing,
25 or other proceeding in or before a court,

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

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

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

17 “(A) ensure that—

18 “(i) any acquisition authorized under
19 subsection (a) is limited to targeting per-
20 sons reasonably believed to be non-United
21 States persons located outside the United
22 States; and

23 “(ii) except as provided in subsection
24 (b)(2), targeting 1 or more United States
25 persons or persons reasonably believed to

1 getting persons reasonably believed to
2 be non-United States persons located
3 outside the United States; and

4 “(II) except as provided in sub-
5 section (b)(2), a significant purpose of
6 an acquisition is not to target 1 or
7 more United States persons or per-
8 sons reasonably believed to be in the
9 United States at the time of acqui-
10 sition or communication; and”.

11 **SEC. 105. FISA COURT REVIEW OF TARGETING DECISIONS.**

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

14 (1) in subsection (h)(2)—

15 (A) in subparagraph (D)(ii), by striking
16 “and” at the end;

17 (B) in subparagraph (E), by striking the
18 period at the end and inserting “; and”; and

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

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

25 (2) in subsection (j)(1)—

1 (A) by striking “subsection (g)” each place
2 it appears and inserting “subsection (h)”; and

3 (B) in subparagraph (A), as amended by
4 subparagraph (A) of this paragraph, by insert-
5 ing “, including reviewing the random sample of
6 targeting decisions and written justifications
7 submitted under subsection (h)(2)(F),” after
8 “subsection (h)”.

9 **SEC. 106. REPEAL OF AUTHORITY FOR THE RESUMPTION**
10 **OF ABOUTS COLLECTION.**

11 (a) IN GENERAL.—Section 702(b)(5) of the Foreign
12 Intelligence Surveillance Act of 1978 (50 U.S.C.
13 1881a(b)(5)) is amended by striking “, except as provided
14 under section 103(b) of the FISA Amendments Reauthor-
15 ization Act of 2017”.

16 (b) CONFORMING AMENDMENTS.—

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

21 (A) in the subsection heading, by striking
22 “REVIEWS, AND REPORTING” and inserting
23 “AND REVIEWS”; and

24 (B) by striking paragraph (4).

1 (2) FISA AMENDMENTS REAUTHORIZATION ACT
2 OF 2017.—Section 103 of the FISA Amendments Re-
3 authorization Act of 2017 (Public Law 115–118;
4 132 Stat. 10) is amended—

5 (A) by striking subsection (b) (50 U.S.C.
6 1881a note); and

7 (B) by striking “(a) IN GENERAL.—”.

8 **SEC. 107. EXTENSION OF TITLE VII OF FISA; EXPIRATION**
9 **OF FISA AUTHORITIES; EFFECTIVE DATES.**

10 (a) EFFECTIVE DATES.—Section 403(b) of the FISA
11 Amendments Act of 2008 (Public Law 110–261; 122 Stat.
12 2474) is amended—

13 (1) in paragraph (1) (50 U.S.C. 1881 note)—

14 (A) by striking “April 19, 2024” and in-
15 serting “December 31, 2027”; and

16 (B) by striking “, as amended by section
17 101(a) and by the FISA Amendments Reau-
18 thorization Act of 2017,” and inserting “, as
19 most recently amended,”; and

20 (2) in paragraph (2) (18 U.S.C. 2511 note), in
21 the matter preceding subparagraph (A), by striking
22 “April 19, 2024” and inserting “December 31,
23 2027”.

1 (b) CONFORMING AMENDMENTS.—Section 404(b) of
2 the FISA Amendments Act of 2008 (Public Law 110–261;
3 122 Stat. 2476), is amended—

4 (1) in paragraph (1)—

5 (A) in the heading, by striking “APRIL 19,
6 2024” and inserting “DECEMBER 31, 2027”; and

7 (B) by striking “, as amended by section
8 101(a) and by the FISA Amendments Reau-
9 thorization Act of 2017,” and inserting “, as
10 most recently amended,”;

11 (2) in paragraph (2), by striking “, as amended
12 by section 101(a) and by the FISA Amendments Re-
13 authorization Act of 2017,” and inserting “, as most
14 recently amended,”; and

15 (3) in paragraph (4)—

16 (A) by striking “, as added by section
17 101(a) and amended by the FISA Amendments
18 Reauthorization Act of 2017,” both places it
19 appears and inserting “, as added by section
20 101(a) and as most recently amended,”; and

21 (B) by striking “, as amended by section
22 101(a) and by the FISA Amendments Reau-
23 thorization Act of 2017,” both places it appears
24 and inserting “, as most recently amended,”.

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

6 **SEC. 201. APPLICATION FOR AN ORDER UNDER THE FOR-**
7 **EIGN INTELLIGENCE SURVEILLANCE ACT OF**
8 **1978.**

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

11 (1) TITLE I.—Subsection (a)(3) of section 104
12 of the Foreign Intelligence Surveillance Act of 1978
13 (50 U.S.C. 1804) is amended by striking “a state-
14 ment of” and inserting “a sworn statement of”.

15 (2) TITLE III.—Subsection (a)(3) of section 303
16 of the Foreign Intelligence Surveillance Act of 1978
17 (50 U.S.C. 1823) is amended by striking “a state-
18 ment of” and inserting “a sworn statement of”.

19 (3) SECTION 703.—Subsection (b)(1)(C) of sec-
20 tion 703 of the Foreign Intelligence Surveillance Act
21 of 1978 (50 U.S.C. 1881b) is amended by striking
22 “a statement of” and inserting “a sworn statement
23 of”.

24 (4) SECTION 704.—Subsection (b)(3) of section
25 704 of the Foreign Intelligence Surveillance Act of

1 1978 (50 U.S.C. 1881c) is amended by striking “a
2 statement of” and inserting “a sworn statement of”.

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

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

9 (1) TITLE I.—Subsection (a) of section 104 of
10 the Foreign Intelligence Surveillance Act of 1978
11 (50 U.S.C. 1804) is amended—

12 (A) in paragraph (8), by striking “; and”
13 and inserting a semicolon;

14 (B) in paragraph (9), by striking the pe-
15 riod at the end and inserting a semicolon; and

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

17 “(10) with respect to a target who is a United
18 States person, a statement summarizing the inves-
19 tigative techniques carried out before making the ap-
20 plication;”.

21 (2) APPLICABILITY.—The amendments made
22 by this subsection shall apply with respect to appli-
23 cations made on or after the date that is 120 days
24 after the date of enactment of this Act.

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

3 (1) APPLICATIONS FOR EXTENSION OF ORDERS
4 UNDER TITLE I.—Subsection (a) of section 104 of
5 the Foreign Intelligence Surveillance Act of 1978
6 (50 U.S.C. 1804), as amended by this Act, is fur-
7 ther amended by adding at the end the following:

8 “(11) in the case of an application for an exten-
9 sion of an order under this title for a surveillance
10 targeted against a United States person, a summary
11 statement of the foreign intelligence information ob-
12 tained pursuant to the original order (and any pre-
13 ceding extension thereof) as of the date of the appli-
14 cation for the extension, or a reasonable explanation
15 of the failure to obtain such information;”.

16 (2) APPLICATIONS FOR EXTENSION OF ORDERS
17 UNDER TITLE III.—Subsection (a) of section 303 of
18 the Foreign Intelligence Surveillance Act of 1978
19 (50 U.S.C. 1823) is amended—

20 (A) in paragraph (7), by striking “; and”
21 and inserting a semicolon;

22 (B) in paragraph (8), by striking the pe-
23 riod at the end and inserting a semicolon; and

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

1 “(9) in the case of an application for an exten-
2 sion of an order under this title in which the target
3 of the physical search is a United States person, a
4 summary statement of the foreign intelligence infor-
5 mation obtained pursuant to the original order (and
6 any preceding extension thereof) as of the date of
7 the application for the extension, or a reasonable ex-
8 planation of the failure to obtain such information;”.

9 (3) APPLICABILITY.—The amendments made
10 by this subsection shall apply with respect to appli-
11 cations made on or after the date that is 120 days
12 after the date of enactment of this Act.

13 (d) REQUIREMENT FOR JUSTIFICATION OF UNDER-
14 LYING CRIMINAL OFFENSE IN CERTAIN APPLICATIONS.—

15 (1) TITLE I.—Subsection (a)(3)(A) of section
16 104 of the Foreign Intelligence Surveillance Act of
17 1978 (50 U.S.C. 1804) is amended by inserting be-
18 fore the semicolon at the end the following: “, and,
19 in the case of a target that is a United States per-
20 son alleged to be acting as an agent of a foreign
21 power (as described in section 101(b)(2)(B)), that a
22 violation of the criminal statutes of the United
23 States as referred to in section 101(b)(2)(B) has oc-
24 curred or will occur”.

1 (2) TITLE III.—Subsection (a)(3)(A) of section
2 303 of the Foreign Intelligence Surveillance Act of
3 1978 (50 U.S.C. 1823) is amended by inserting be-
4 fore the semicolon at the end the following: “, and,
5 in the case of a target that is a United States per-
6 son alleged to be acting as an agent of a foreign
7 power (as described in section 101(b)(2)(B)), that a
8 violation of the criminal statutes of the United
9 States as referred to in section 101(b)(2)(B) has oc-
10 curred or will occur”.

11 (3) APPLICABILITY.—The amendments made
12 by this subsection shall apply with respect to appli-
13 cations made on or after the date that is 120 days
14 after the date of enactment of this Act.

15 (e) REQUIRED DISCLOSURE OF RELEVANT INFORMA-
16 TION IN FOREIGN INTELLIGENCE SURVEILLANCE ACT OF
17 1978 APPLICATIONS.—

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

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

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

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

8 “(1) all information in the possession of the
9 Government that is material to determining whether
10 the application satisfies the applicable requirements
11 under this Act, including any exculpatory informa-
12 tion; and

13 “(2) all information in the possession of the
14 Government that might reasonably—

15 “(A) call into question the accuracy of the
16 application or the reasonableness of any assess-
17 ment in the application conducted by the de-
18 partment or agency on whose behalf the appli-
19 cation is made; or

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

1 (2) CLERICAL AMENDMENT.—The table of con-
2 tents for the Foreign Intelligence Surveillance Act of
3 1978 is amended by adding at the end the following:

 “TITLE IX—REQUIRED DISCLOSURE OF RELEVANT
 INFORMATION

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

4 (f) CERTIFICATION REGARDING ACCURACY PROCE-
5 DURES.—

6 (1) CERTIFICATION REGARDING ACCURACY PRO-
7 CEDURES.—Title IX of the Foreign Intelligence Sur-
8 veillance Act of 1978, as added by subsection (e) of
9 this section, is amended by adding at the end the
10 following:

11 **“SEC. 902. CERTIFICATION REGARDING ACCURACY PROCE-**
12 **DURES.**

13 “(a) DEFINITION OF ACCURACY PROCEDURES.—In
14 this section, the term ‘accuracy procedures’ means specific
15 procedures, adopted by the Attorney General, to ensure
16 that an application for a court order under this Act, in-
17 cluding any application for renewal of an existing order,
18 is accurate and complete, including procedures that en-
19 sure, at a minimum, that—

20 “(1) the application reflects all information that
21 might reasonably call into question the accuracy of
22 the information or the reasonableness of any assess-

1 ment in the application, or otherwise raises doubts
2 about the requested findings;

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

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

10 “(4) the applicant coordinates with the appro-
11 priate elements of the intelligence community (as de-
12 fined in section 3 of the National Security Act of
13 1947 (50 U.S.C. 3003)), concerning any prior or ex-
14 isting relationship with the target of any surveil-
15 lance, search, or other means of investigation, and
16 discloses any such relationship in the application;

17 “(5) before any application targeting a United
18 States person (as defined in section 101) is made,
19 the applicant Federal officer shall document that the
20 officer has collected and reviewed for accuracy and
21 completeness supporting documentation for each fac-
22 tual assertion in the application; and

23 “(6) the applicant Federal agency establish
24 compliance and auditing mechanisms to address, on
25 an annual basis, the efficacy of the accuracy proce-

1 dures that have been adopted and report such find-
2 ings to the Attorney General.

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

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

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

12 “(A) supporting documentation for each
13 factual assertion contained in the application;

14 “(B) all information that might reasonably
15 call into question the accuracy of the informa-
16 tion or the reasonableness of any assessment in
17 the application, or otherwise raises doubts
18 about the requested findings; and

19 “(C) all material information that might
20 reasonably call into question the reliability and
21 reporting of any information from any confiden-
22 tial human source that is used in the applica-
23 tion.

24 “(c) NECESSARY FINDING FOR COURT ORDERS.—A
25 judge may not enter an order under this Act unless the

1 judge finds, in addition to any other findings required
2 under this Act, that the accuracy procedures described in
3 the application for the order, as required under subsection
4 (b)(1), are actually accuracy procedures as defined in this
5 section.”.

6 (2) TECHNICAL AMENDMENT.—The table of
7 contents for the Foreign Intelligence Surveillance
8 Act of 1978, as amended by subsection (e) of this
9 section, is amended by adding at the end the fol-
10 lowing:

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

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

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

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

21 “(2) with regard to information gathered from
22 the content of a media source, the application in-
23 cludes an explanation of the investigative techniques
24 used to corroborate the information; and

1 “(3) with regard to information gathered by a
2 political campaign, such information is not the sole
3 source of the information used to justify the appli-
4 cant’s belief described in subsection (a)(3).”.

5 (h) LIMITATION ON ISSUANCE OF ORDER.—Section
6 105(a) of the Foreign Intelligence Surveillance Act of
7 1978 (50 U.S.C. 1805(a)) is amended—

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

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

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

13 “(5) for an application that is based, in whole
14 or in part, on information obtained from the content
15 of a media source or information gathered by a po-
16 litical campaign—

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

20 “(B) with regard to information gathered
21 from the content of a media source, the applica-
22 tion includes an explanation of the investigative
23 techniques used to corroborate the information;
24 and

1 “(C) with regard to information gathered
2 by a political campaign, such information is not
3 the sole source of the information used to jus-
4 tify the applicant’s belief described in section
5 104(a)(3).”.

6 **SEC. 202. CRIMINAL PENALTIES FOR VIOLATIONS OF FISA.**

7 (a) IN GENERAL.—Section 109 of the Foreign Intel-
8 ligence Surveillance Act of 1978 (50 U.S.C. 1809) is
9 amended—

10 (1) in subsection (a)—

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

13 (B) in paragraph (1)—

14 (i) by inserting “intentionally” before
15 “engages”; and

16 (ii) by striking “or” at the end;

17 (C) in paragraph (2)—

18 (i) by inserting “intentionally” before
19 “disclose”; and

20 (ii) by striking the period at the end
21 and inserting a semicolon; and

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

23 “(3) knowingly submits any document to or
24 makes any false statement before the court estab-
25 lished under section 103(a) or the court established

1 under section 103(b), knowing such document or
2 statement to contain—

3 “(A) a false material declaration; or

4 “(B) a material omission; or

5 “(4) knowingly discloses the existence of an ap-
6 plication for an order authorizing surveillance under
7 this title, or any information contained therein, to
8 any person not authorized to receive such informa-
9 tion, except insofar as such disclosure is authorized
10 by statute or executive order setting forth permis-
11 sible disclosures by whistleblowers.”; and

12 (2) in subsection (c), by striking “five” and in-
13 serting “8”.

14 (b) **RULE OF CONSTRUCTION.**—This section and the
15 amendments made by this section may not be construed
16 to interfere with the enforcement of section 798 of title
17 18, United States Code, or any other provision of law re-
18 garding the unlawful disclosure of classified information.

19 **SEC. 203. INCREASED PENALTIES FOR CIVIL ACTIONS.**

20 (a) **INCREASED PENALTIES.**—Section 110 of the
21 Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.
22 1810) is amended by striking subsection (a) and inserting
23 the following:

24 “(a) actual damages, but not less than liquidated
25 damages equal to the greater of—

1 Act of 1978 (50 U.S.C. 1871 et seq.) is amended by add-
2 ing at the end the following:

3 **“SEC. 605. AGENCY PROCEDURES TO ENSURE COMPLI-**
4 **ANCE.**

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

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

11 “(2) for taking appropriate adverse personnel
12 action against any officer or employee of the depart-
13 ment or agency who engages in a violation described
14 in paragraph (1), including more severe adverse per-
15 sonnel actions for any subsequent violation by such
16 officer or employee.”.

17 (b) CLERICAL AMENDMENT.—The table of contents
18 for the Foreign Intelligence Surveillance Act of 1978 is
19 amended by inserting after the item relating to section
20 604 the following:

“Sec. 605. Agency procedures to ensure compliance.”.

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

1 shall report to Congress on the implementation of such
2 procedures.

3 **SEC. 205. LIMIT ON CIVIL IMMUNITY FOR PROVIDING IN-**
4 **FORMATION, FACILITIES, OR TECHNICAL AS-**
5 **SISTANCE TO THE GOVERNMENT ABSENT A**
6 **COURT ORDER.**

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

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

11 “(B) a certification in writing—

12 “

13 “(I) by a person specified in section
14 2518(7) or the Attorney General of the
15 United States;

16 “(II) that the requirements for an
17 emergency authorization to intercept a
18 wire, oral, or electronic communication
19 under section 2518(7) have been met; and

20 “(III) that the specified assistance is
21 required,”; and

22 (2) by striking subparagraph (iii) and inserting
23 the following:

24 “(iii) For assistance provided pursu-
25 ant to a certification under subparagraph

1 (ii)(B), the limitation on causes of action
2 under the last sentence of the matter fol-
3 lowing that subparagraph shall only apply
4 to the extent that the assistance ceased at
5 the earliest of the time the application for
6 a court order was denied, the time the
7 communication sought was obtained, or 48
8 hours after the interception began.”.

9 **TITLE III—REFORMS RELATING**
10 **TO PROCEEDINGS BEFORE**
11 **THE FOREIGN INTELLIGENCE**
12 **SURVEILLANCE COURT AND**
13 **OTHER COURTS**

14 **SEC. 301. FOREIGN INTELLIGENCE SURVEILLANCE COURT**
15 **REFORM.**

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

1 the application has expired, or that judge is otherwise no
2 longer serving on the court.”.

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

5 (1) EXPANSION OF APPOINTMENT AUTHOR-
6 ITY.—

7 (A) IN GENERAL.—Section 103(i)(2) of the
8 Foreign Intelligence Surveillance Act of 1978
9 (50 U.S.C. 1803(i)(2)) is amended—

10 (i) by striking subparagraph (A) and
11 inserting the following:

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

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

24 “(ii) presents significant concerns
25 with respect to the activities of a United

1 States person that are protected by the
2 first amendment to the Constitution of the
3 United States;

4 “(iii) presents or involves a sensitive
5 investigative matter;

6 “(iv) presents a request for approval
7 of a new program, a new technology, or a
8 new use of existing technology;

9 “(v) presents a request for reauthor-
10 ization of programmatic surveillance; or

11 “(vi) otherwise presents novel or sig-
12 nificant civil liberties issues; and”;

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

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

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

24 “(A) an investigative matter involving the
25 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 paragraph
19 (1) of this subsection, 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 court estab-
11 lished under subsection (a), an amicus cu-
12 riae appointed under paragraph (2) may
13 petition the court to certify for review to
14 the court established under subsection (b)
15 a question of law pursuant to subsection
16 (j).

17 “(ii) WRITTEN STATEMENT OF REA-
18 SONS.—If the court established under sub-
19 section (a) denies a petition under this
20 subparagraph, the court shall provide for
21 the record a written statement of the rea-
22 sons for the denial.

23 “(iii) APPOINTMENT.—Upon certifi-
24 cation of any question of law pursuant to
25 this subparagraph, the court established

1 under subsection (b) shall appoint the ami-
2 cus curiae to assist the court in its consid-
3 eration of the certified question, unless the
4 court issues a finding that such appoint-
5 ment is not appropriate.

6 “(B) FISA COURT OF REVIEW DECI-
7 SIONS.—An amicus curiae appointed under
8 paragraph (2) may petition the court estab-
9 lished under subsection (b) to certify for review
10 to the Supreme Court of the United States any
11 question of law pursuant to section 1254(2) of
12 title 28, United States Code.

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

21 (3) ACCESS TO INFORMATION.—

22 (A) APPLICATION AND MATERIALS.—Sec-
23 tion 103(i)(6) of the Foreign Intelligence Sur-
24 veillance Act of 1978 (50 U.S.C. 1803(i)(6)) is

1 “(bb) an unredacted copy of
2 each relevant decision made by
3 the court established under sub-
4 section (a) or the court estab-
5 lished under subsection (b) in
6 which the court decides a ques-
7 tion of law, without regard to
8 whether the decision is classified;
9 and

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

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

21 “(ii) SUPPORTING DOCUMENTATION
22 REGARDING ACCURACY.—The court estab-
23 lished under subsection (a), upon the mo-
24 tion of an amicus curiae appointed under
25 paragraph (2) or upon its own motion,

1 may require the Government to make
2 available the supporting documentation de-
3 scribed in section 902.”.

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

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

10 (ii) by striking subparagraph (C) and
11 inserting the following:

12 “(C) CLASSIFIED INFORMATION.—An ami-
13 cus curiae designated or appointed by the court
14 shall have access, to the extent such informa-
15 tion is available to the Government, to
16 unredacted copies of each opinion, order, tran-
17 script, pleading, or other document of the court
18 established under subsection (a) and the court
19 established under subsection (b), including, if
20 the individual is eligible for access to classified
21 information, any classified documents, informa-
22 tion, and other materials or proceedings.”.

23 (C) CONSULTATION AMONG AMICI CU-
24 RIAE.—Section 103(i)(6) of the Foreign Intel-

1 ligence Surveillance Act of 1978 (50 U.S.C.
2 1803(i)(6)) is amended—

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

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

7 “(D) CONSULTATION AMONG AMICI CU-
8 RIAE.—An amicus curiae appointed under para-
9 graph (2) by the court established under sub-
10 section (a) or the court established under sub-
11 section (b) may consult with 1 or more of the
12 other individuals designated by the court to
13 serve as amicus curiae pursuant to paragraph
14 (1) of this subsection regarding any of the in-
15 formation relevant to any assigned pro-
16 ceeding.”.

17 (4) EFFECTIVE DATE.—The amendments made
18 by this subsection shall take effect on the date of en-
19 actment of this Act and shall apply with respect to
20 proceedings under the Foreign Intelligence Surveil-
21 lance Act of 1978 (50 U.S.C. 1801 et seq.) that take
22 place on or after, or are pending on, that date.

1 **SEC. 302. PUBLIC DISCLOSURE AND DECLASSIFICATION OF**
2 **CERTAIN DOCUMENTS.**

3 (a) SUBMISSION TO CONGRESS.—Section 601(c)(1)
4 of the Foreign Intelligence Surveillance Act of 1978 (50
5 U.S.C. 1871(c)) is amended by inserting “, including de-
6 classified copies that have undergone review under section
7 602” before “; and”.

8 (b) TIMELINE FOR DECLASSIFICATION REVIEW.—
9 Section 602(a) of the Foreign Intelligence Surveillance
10 Act of 1978 (50 U.S.C. 1872(a)) is amended—

11 (1) by inserting “, to be concluded not later
12 than 180 days after the issuance of such decision,
13 order, or opinion,” after “(as defined in section
14 601(e))”; and

15 (2) by inserting “or results in a change of ap-
16 plication of any provision of this Act or a novel ap-
17 plication of any provision of this Act” after “law”.

18 **SEC. 303. SUBMISSION OF COURT TRANSCRIPTS TO CON-**
19 **GRESS.**

20 Section 601(c) of the Foreign Intelligence Surveil-
21 lance Act of 1978 (50 U.S.C. 1871(c)), as amended by
22 section 302 of this Act, is amended—

23 (1) in paragraph (1), by striking “; and” and
24 inserting a semicolon;

25 (2) in paragraph (2), by striking the period at
26 the end and inserting “; and”; and

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

2 “(3) for any matter at which a court reporter
3 is present and creates a transcript of a hearing or
4 oral argument before the Foreign Intelligence Sur-
5 veillance Court or the Foreign Intelligence Surveil-
6 lance Court of Review, a copy of each such tran-
7 script not later than 45 days after the government’s
8 receipt of the transcript or the date on which the
9 matter concerning such hearing or oral argument is
10 resolved, whichever is later.”.

11 **SEC. 304. CONTEMPT POWER OF FISC AND FISCR.**

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

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

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

19 **“§ 404. Definitions**

20 “For purposes of this chapter—

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

1 “(2) the terms ‘Foreign Intelligence Surveil-
2 lance Court’ and ‘Foreign Intelligence Surveillance
3 Court of Review’ have the meanings given those
4 terms in section 601(e) of the Foreign Intelligence
5 Surveillance Act of 1978 (50 U.S.C. 1871(e)).”.

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

 “404. Definitions.”.

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

19 **TITLE IV—INDEPENDENT EXEC-**
20 **UTIVE BRANCH OVERSIGHT**

21 **SEC. 401. PERIODIC AUDIT OF FISA COMPLIANCE BY IN-**
22 **SPECTOR GENERAL.**

23 (a) REPORT REQUIRED.—Title VI of the Foreign In-
24 telligence Surveillance Act of 1978 (50 U.S.C. 1871 et

1 seq.), as amended by section 204 of this Act, is amended
2 by adding at the end the following:

3 **“SEC. 606. PERIODIC AUDIT OF FISA COMPLIANCE BY IN-**
4 **SPECTOR GENERAL.**

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

9 “(1) conduct an audit of alleged or potential
10 violations and failures to comply with the require-
11 ments of this Act, and any procedures established
12 pursuant to this Act, which shall include an analysis
13 of the accuracy and completeness of applications and
14 certifications for orders submitted under each of sec-
15 tions 105, 303, 402, 502, 702, 703, and 704; and

16 “(2) submit to the Select Committee on Intel-
17 ligence of the Senate, the Committee on the Judici-
18 ary of the Senate, the Permanent Select Committee
19 on Intelligence of the House of Representatives, and
20 the Committee on the Judiciary of the House of
21 Representatives a report on the audit required under
22 paragraph (1).”.

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

1 amended by section 204 of this Act, is amended by insert-
2 ing after the item relating to section 605 the following:

“Sec. 606. Periodic audit of FISA compliance by Inspector General.”.

3 **SEC. 402. INTELLIGENCE COMMUNITY PARITY AND COMMU-**
4 **NICATIONS WITH PRIVACY AND CIVIL LIB-**
5 **ERTIES OVERSIGHT BOARD.**

6 (a) WHISTLEBLOWER PROTECTIONS FOR MEMBERS
7 OF INTELLIGENCE COMMUNITY FOR COMMUNICATIONS
8 WITH PRIVACY AND CIVIL LIBERTIES OVERSIGHT
9 BOARD.—Section 1104 of the National Security Act of
10 1947 (50 U.S.C. 3234) is amended—

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

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

19 (b) PARITY IN PAY FOR PRIVACY AND CIVIL LIB-
20 ERTIES OVERSIGHT BOARD STAFF AND THE INTEL-
21 LIGENCE COMMUNITY.—Section 1061(j)(1) of the Intel-
22 ligence Reform and Terrorism Prevention Act of 2004 (42
23 U.S.C. 2000ee(j)(1)) is amended by striking “except that”
24 and all that follows through the period at the end and
25 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 **TITLE V—PROTECTIONS FOR**
6 **UNITED STATES PERSONS**
7 **WHOSE SENSITIVE INFORMA-**
8 **TION IS PURCHASED BY IN-**
9 **TELLIGENCE AND LAW EN-**
10 **FORCEMENT AGENCIES**

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

13 (a) DEFINITIONS.—In this section:

14 (1) APPROPRIATE COMMITTEES OF CON-
15 GRESS.—The term “appropriate committees of Con-
16 gress” means—

17 (A) the congressional intelligence commit-
18 tees (as defined in section 3 of the National Se-
19 curity Act of 1947 (50 U.S.C. 3003));

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

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

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

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

6 (B) does not include data that—

7 (i) is lawfully available to the public
8 through Federal, State, or local govern-
9 ment records or through widely distributed
10 media;

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

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

17 (3) COVERED PERSON.—The term “covered
18 person” means an individual who—

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

22 (B) is a United States person.

23 (4) INTELLIGENCE COMMUNITY.—The term
24 “intelligence community” has the meaning given

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

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

8 (b) LIMITATION.—

9 (1) IN GENERAL.—Subject to paragraphs (2)
10 through (7), an element of the intelligence commu-
11 nity may not acquire a dataset that includes covered
12 data.

13 (2) AUTHORIZATION PURSUANT TO COURT
14 ORDER.—An element of the intelligence community
15 may acquire covered data if the collection has been
16 authorized by an order or emergency authorization
17 issued pursuant to the Foreign Intelligence Surveil-
18 lance Act of 1978 (50 U.S.C. 1801 et seq.) or title
19 18, United States Code, by a court of competent ju-
20 risdiction covering the period of the acquisition, sub-
21 ject to the use, dissemination, querying, retention,
22 and other minimization limitations required by such
23 authorization.

24 (3) AUTHORIZATION FOR EMPLOYMENT-RE-
25 LATED USE.—An element of the intelligence commu-

1 nity may acquire covered data about an employee of,
2 or applicant for employment by, an element of the
3 intelligence community for employment-related pur-
4 poses, provided that—

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

7 (B) the covered data is destroyed at such
8 time as it is no longer necessary for such pur-
9 poses.

10 (4) EXCEPTION FOR COMPLIANCE PURPOSES.—

11 An element of the intelligence community may ac-
12 quire covered data for the purpose of supporting
13 compliance with collection limitations and minimiza-
14 tion requirements imposed by statute, guidelines,
15 procedures, or the Constitution of the United States,
16 provided that—

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

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

22 (5) EXCEPTION FOR LIFE OR SAFETY.—An ele-

23 ment of the intelligence community may acquire cov-
24 ered data if there is a reasonable belief than an
25 emergency exists involving an imminent threat of

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

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

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

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

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

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

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

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

1 quire a dataset that includes covered data if the cov-
2 ered data is not reasonably segregable prior to ac-
3 quisition, provided that the element of the intel-
4 ligence community complies with the minimization
5 procedures in subsection (c).

6 (c) MINIMIZATION PROCEDURES.—

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

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

17 (A) to exclude covered data not subject to
18 1 or more exceptions set forth in subsection (b)
19 from datasets prior to acquisition; and

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

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

7 (4) QUERYING.—

8 (A) IN GENERAL.—Except as provided in
9 subparagraphs (B) and (C), no officer or em-
10 ployee of an element of the intelligence commu-
11 nity may conduct a query of covered data, in-
12 cluding covered data already subjected to mini-
13 mization, in an effort to find records of or
14 about a particular covered person.

15 (B) EXCEPTIONS.—Subparagraph (A)
16 shall not apply to a query related to a par-
17 ticular covered person if—

18 (i) such covered person is the subject
19 of a court order or emergency authoriza-
20 tion issued under the Foreign Intelligence
21 Surveillance Act of 1978 (50 U.S.C. 1801
22 et seq.) or title 18, United States Code,
23 that would authorize the element of the in-
24 telligence community to compel the produc-

1 tion of the covered data, during the effec-
2 tive period of that order;

3 (ii) the purpose of the query is to re-
4 trieve information about an employee of, or
5 applicant for employment by, an element of
6 the intelligence community, provided that
7 any covered data accessed through such
8 query is used only for such purpose;

9 (iii) the query is conducted for the
10 purpose of supporting compliance with col-
11 lection limitations and minimization re-
12 quirements imposed by statute, guidelines,
13 procedures, or the Constitution of the
14 United States, provided that any covered
15 data accessed through such query is used
16 only for such purpose;

17 (iv) the officer or employee of an ele-
18 ment of the intelligence community car-
19 rying out the query has a reasonable belief
20 that an emergency exists involving an im-
21 minent threat of death or serious bodily
22 harm, and that in order to prevent or miti-
23 gate such threat, the query must be con-
24 ducted before a court order can, with due
25 diligence, be obtained, provided that any

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

3 (v) such covered person or, if such
4 person is incapable of providing consent, a
5 third party legally authorized to consent on
6 behalf of the person has consented to the
7 query, provided that any use of covered
8 data accessed through such query is lim-
9 ited to the purposes for which the consent
10 was provided.

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

14 (i) each query shall be reasonably de-
15 signed to exclude personal data of covered
16 persons, unless the query is subject to an
17 exception set forth in paragraph (4); and

18 (ii) any personal data of covered per-
19 sons returned pursuant to a query that is
20 not subject to an exception set forth in
21 paragraphs (2) through (7) of subsection
22 (b) shall not be reviewed and shall imme-
23 diately be destroyed.

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

1 an element of the intelligence community in violation of
2 subsection (b), and any evidence derived therefrom, may
3 not be used, received in evidence, or otherwise dissemi-
4 nated in any investigation by or in any trial, hearing, or
5 other proceeding in or before any court, grand jury, de-
6 partment, office, agency, regulatory body, legislative com-
7 mittee, or other authority of the United States, a State,
8 or political subdivision thereof.

9 (e) REPORTING REQUIREMENT.—

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

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

20 (A) A description of the covered person in-
21 formation in each dataset.

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

24 (3) NOTIFICATIONS.—After submitting the re-
25 port required by paragraph (1), the Director shall,

1 in coordination with the Under Secretary of Defense
2 for Intelligence and Security, notify the appropriate
3 committees of Congress of any changes to the infor-
4 mation contained in such report.

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

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

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

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

16 **SEC. 502. LIMITATION ON LAW ENFORCEMENT PURCHASE**
17 **OF PERSONAL DATA FROM DATA BROKERS.**

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

20 “(e) PROHIBITION ON OBTAINING IN EXCHANGE FOR
21 ANYTHING OF VALUE PERSONAL DATA BY LAW EN-
22 FORCEMENT AGENCIES.—

23 “(1) DEFINITIONS.—In this subsection and
24 subsection (f)—

1 “(A) the term ‘covered governmental enti-
2 ty’ means a law enforcement agency of a gov-
3 ernmental entity;

4 “(B) the term ‘covered organization’
5 means a person who—

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

7 “(ii) is not an individual;

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

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

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

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

21 “(E) the term ‘electronic device’ has the
22 meaning given the term ‘computer’ in section
23 1030(e);

24 “(F) the term ‘lawfully obtained public
25 data’ means personal data obtained by a par-

1 ticular covered organization that the covered or-
2 ganization—

3 “(i) reasonably understood to have
4 been voluntarily made available to the gen-
5 eral public by the covered person; and

6 “(ii) obtained in compliance with all
7 applicable laws, regulations, contracts, pri-
8 vacy policies, and terms of service;

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

16 “(H) the term ‘personal data’—

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

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

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

4 “(iii) does not include—

5 “(I) data that is lawfully avail-
6 able through Federal, State, or local
7 government records or through widely
8 distributed media; or

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

12 “(2) LIMITATION.—

13 “(A) IN GENERAL.—

14 “(i) PROHIBITION.—Subject to
15 clauses (ii) through (x), a covered govern-
16 mental entity may not obtain in exchange
17 for anything of value covered personal data
18 if—

19 “(I) the covered personal data is
20 directly or indirectly obtained from a
21 covered organization; or

22 “(II) the covered personal data is
23 derived from covered personal data
24 that was directly or indirectly ob-
25 tained from a covered organization.

1 “(ii) EXCEPTION FOR CERTAIN COM-
2 PILATIONS OF DATA.—A covered govern-
3 mental entity may obtain in exchange for
4 something of value covered personal data
5 as part of a larger compilation of data
6 which includes personal data about persons
7 who are not covered persons, if—

8 “(I) the covered governmental
9 entity is unable through reasonable
10 means to exclude covered personal
11 data from the larger compilation ob-
12 tained; and

13 “(II) the covered governmental
14 entity minimizes any covered personal
15 data from the larger compilation, in
16 accordance with subsection (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 covered governmental entity under a pro-
22 gram 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 covered governmental entity from a cov-
11 ered organization in accordance with com-
12 pulsory legal process that—

13 “(I) is established by a Federal
14 or State statute; and

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

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

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

3 “(I) obtained by the covered gov-
4 ernmental entity for employment-re-
5 lated purposes;

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

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

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

17 “(I) obtained by a covered gov-
18 ernmental entity for purposes of con-
19 ducting a background check of the
20 covered person with the written con-
21 sent of the covered person;

22 “(II) accessed and used by the
23 covered governmental entity only for
24 background check-related purposes;
25 and

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

5 “(vii) EXCEPTION FOR LAWFULLY OB-
6 TAINED PUBLIC DATA.—Clause (i) shall
7 not apply to covered personal data that is
8 obtained by a covered governmental entity
9 if—

10 “(I) the covered personal data is
11 lawfully obtained public data; or

12 “(II) the covered personal data is
13 derived from covered personal data
14 that solely consists of lawfully ob-
15 tained public data.

16 “(viii) EXCEPTION FOR LIFE OR
17 SAFETY.—Clause (i) shall not apply to cov-
18 ered personal data that is obtained by a
19 covered governmental entity if there is a
20 reasonable belief that an emergency exists
21 involving an imminent threat of death or
22 serious bodily harm to a covered person
23 and the covered data is necessary to miti-
24 gate that threat, provided that—

1 “(I) access to and use of the cov-
2 ered personal data is limited to ad-
3 dressing the threat; and

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

7 “(ix) EXCEPTION FOR COMPLIANCE
8 PURPOSES.—Clause (i) shall not apply to
9 covered personal data that is obtained by
10 a covered governmental entity for the pur-
11 pose of supporting compliance with collec-
12 tion limitations and minimization require-
13 ments imposed by statute, guidelines, pro-
14 cedures, or the Constitution of the United
15 States, provided that—

16 “(I) access to and use of the cov-
17 ered personal data is limited to such
18 purpose; and

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

22 “(x) EXCEPTION FOR CONSENT.—
23 Clause (i) shall not apply to covered per-
24 sonal data that is obtained by a covered
25 governmental entity if—

1 “(I) each covered person linked
2 or reasonably linkable to the covered
3 personal data, or, if such covered per-
4 son is incapable of providing consent,
5 a third party legally authorized to
6 consent on behalf of the covered per-
7 son, has provided consent to the ac-
8 quisition and use of the data on a
9 case-by-case basis;

10 “(II) access to and use of the
11 covered personal data is limited to the
12 purposes for which the consent was
13 provided; and

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

17 “(B) INDIRECTLY ACQUIRED RECORDS
18 AND INFORMATION.—The limitation under sub-
19 paragraph (A) shall apply without regard to
20 whether the covered organization possessing the
21 covered personal data is the covered organiza-
22 tion that initially obtained or collected, or is the
23 covered organization that initially received the
24 disclosure of, the covered personal data.

1 “(3) LIMIT ON SHARING BETWEEN AGEN-
2 CIES.—An agency of a governmental entity that is
3 not a covered governmental entity may not provide
4 to a covered governmental entity covered personal
5 data that was obtained in a manner that would vio-
6 late paragraph (2) if the agency of a governmental
7 entity were a covered governmental entity, unless the
8 covered governmental entity would have been per-
9 mitted to obtain the covered personal data under an
10 exception set forth in paragraph (2)(A).

11 “(4) PROHIBITION ON USE OF DATA OBTAINED
12 IN VIOLATION OF THIS SECTION.—

13 “(A) IN GENERAL.—Covered personal data
14 obtained by or provided to a covered govern-
15 mental entity in violation of paragraph (2) or
16 (3), and any evidence derived therefrom, may
17 not be used, received in evidence, or otherwise
18 disseminated by, on behalf of, or upon a motion
19 or other action by a covered governmental enti-
20 ty in any investigation by or in any trial, hear-
21 ing, or other proceeding in or before any court,
22 grand jury, department, officer, agency, regu-
23 latory body, legislative committee, or other au-
24 thority of the United States, a State, or a polit-
25 ical subdivision thereof.

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

7 “(f) MINIMIZATION PROCEDURES.—

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

14 “(2) ACQUISITION AND RETENTION.—The pro-
15 cedures adopted under paragraph (1) shall require
16 covered governmental entities to exhaust all reason-
17 able means—

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

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

1 pilation is obtained and before operational use
2 of the compilation or inclusion of the compila-
3 tion in a dataset intended for operational use.

4 “(3) DESTRUCTION.—The procedures adopted
5 under paragraph (1) shall require that, if a covered
6 governmental entity identifies covered personal data
7 in a compilation described in clause (ii) of subsection
8 (e)(2)(A) not subject to 1 or more exceptions set
9 forth in clauses (iii) through (x) of such subsection,
10 the covered governmental entity shall promptly de-
11 stroy the covered personal data and any dissemina-
12 tion of information derived from the covered per-
13 sonal data shall be prohibited.

14 “(4) QUERYING.—

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

22 “(B) EXCEPTIONS.—Subparagraph (A)
23 shall not apply to a query related to a par-
24 ticular covered person if—

1 “(i) such covered person is the subject
2 of a court order or emergency authoriza-
3 tion issued under this title that would au-
4 thorize the covered governmental entity to
5 compel the production of the covered per-
6 sonal data, during the effective period of
7 that order;

8 “(ii) the purpose of the query is to re-
9 trieve information obtained by a covered
10 governmental entity under a program es-
11 tablished by an Act of Congress under
12 which a portion of a penalty or a similar
13 payment or bounty is paid to an individual
14 who discloses information about an unlaw-
15 ful activity to the Government, such as the
16 program authorized under section 7623 of
17 the Internal Revenue Code of 1986 (relat-
18 ing to awards to whistleblowers in cases of
19 underpayments or fraud), provided that
20 any covered personal data accessed
21 through such query is used only for such
22 purpose;

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

1 governmental entity that has been obtained
2 by the covered governmental entity for em-
3 ployment-related purposes, provided that
4 any covered personal data accessed
5 through such query is used only for such
6 purposes;

7 “(iv) the purpose of the query is to re-
8 trieve information obtained by a covered
9 governmental entity for purposes of con-
10 ducting a background check of the covered
11 person with the written consent of the cov-
12 ered person, provided that any covered per-
13 sonal data accessed through such query is
14 used only for such purposes;

15 “(v) the purpose of the query is to re-
16 trieve, and the query is reasonably de-
17 signed to retrieve, only lawfully obtained
18 public data, and only lawfully obtained
19 public data is accessed and used as a re-
20 sult of the query;

21 “(vi) the officer or employee of a cov-
22 ered governmental entity carrying out the
23 query has a reasonable belief that an emer-
24 gency exists involving an imminent threat
25 of death or serious bodily harm, and in

1 order to prevent or mitigate that threat,
2 the query must be conducted before a
3 court order can, with due diligence, be ob-
4 tained, provided that any covered personal
5 data accessed through such query is used
6 only for such purpose;

7 “(vii) the query is conducted for the
8 purpose of supporting compliance with col-
9 lection limitations and minimization re-
10 quirements imposed by statute, guidelines,
11 procedures, or the Constitution of the
12 United States, provided that any covered
13 personal data accessed through such query
14 is used only for such purpose; or

15 “(viii) such covered person or, if such
16 covered person is incapable of providing
17 consent, a third party legally authorized to
18 consent on behalf of the covered person
19 has consented to the query, provided that
20 any use of covered personal data accessed
21 through such query is limited to the pur-
22 poses for which the consent was provided.

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

1 “(i) each query shall be reasonably de-
2 signed to exclude personal data of covered
3 persons, unless the query is subject to an
4 exception set forth in subparagraph (B);
5 and

6 “(ii) any personal data of covered per-
7 sons returned pursuant to a query that is
8 not subject to an exception set forth in
9 clauses (ii) through (iii) of subsection
10 (e)(2)(A) shall not be reviewed and shall
11 immediately be destroyed.”.

12 **SEC. 503. CONSISTENT PROTECTIONS FOR DEMANDS FOR**
13 **DATA HELD BY INTERACTIVE COMPUTING**
14 **SERVICES.**

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

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

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

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

22 “(5) the term ‘online service provider’ means a
23 provider of electronic communication service, a pro-
24 vider of remote computing service, any information
25 service, system, or access software provider that pro-

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

6 (b) REQUIRED DISCLOSURE.—Section 2703 of title
7 18, United States Code, is amended—

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

11 (2) in subsection (c)—

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

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

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

1 (c) LIMITATION ON VOLUNTARY DISCLOSURE.—Sec-
2 tion 2702(a) of title 18, United States Code, is amended—

3 (1) in paragraph (1), by striking “a person or
4 entity providing an electronic communication service
5 to the public” and inserting “an online service pro-
6 vider”;

7 (2) in paragraph (2), by striking “a person or
8 entity providing remote computing service to the
9 public” and inserting “an online service provider”;
10 and

11 (3) in paragraph (3), by striking “a provider of
12 remote computing service or electronic communica-
13 tion service to the public” and inserting “an online
14 service provider”.

15 **SEC. 504. CONSISTENT PRIVACY PROTECTIONS FOR DATA**
16 **HELD BY DATA BROKERS.**

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

19 “(i) COVERED PERSONAL DATA.—

20 “(1) DEFINITIONS.—In this subsection, the
21 terms ‘covered personal data’ and ‘covered organiza-
22 tion’ have the meanings given such terms in section
23 2702(e).

24 “(2) LIMITATION.—Unless a governmental enti-
25 ty obtains an order in accordance with paragraph

1 (3), the governmental entity may not require a cov-
2 ered organization that is not an online service pro-
3 vider to disclose covered personal data if a court
4 order would be required for the governmental entity
5 to require an online service provider to disclose such
6 covered personal data that is a record of a customer
7 or subscriber of the online service provider.

8 “(3) ORDERS.—

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

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

1 **SEC. 505. PROTECTION OF DATA ENTRUSTED TO INTER-**
2 **MEDIARY OR ANCILLARY SERVICE PRO-**
3 **VIDERS.**

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

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

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

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

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

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

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

23 “(4) an intermediary or ancillary service pro-
24 vider may not knowingly disclose—

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

1 by that intermediary or ancillary service pro-
2 vider; or

3 “(B) to any governmental entity a record
4 or other information pertaining to a subscriber
5 to or customer of, a recipient of a communica-
6 tion from a subscriber to or customer of, or the
7 sender of a communication to a subscriber to or
8 customer of, the online service provider for, or
9 on behalf of, which the intermediary or ancil-
10 lary service provider directly or indirectly deliv-
11 ers, transmits, stores, or processes communica-
12 tions or any other covered personal data (as de-
13 fined in subsection (e)).”.

14 **TITLE VI—TRANSPARENCY**

15 **SEC. 601. ENHANCED REPORTS BY DIRECTOR OF NATIONAL** 16 **INTELLIGENCE.**

17 (a) IN GENERAL.—Section 603(b) of the Foreign In-
18 telligence Surveillance Act of 1978 (50 U.S.C. 1873(b))
19 is amended—

20 (1) in paragraph (2)(C), by striking the semi-
21 colon and inserting “; and”;

22 (2) by redesignating paragraphs (3) through
23 (7) as paragraphs (6) through (10), respectively;

24 (3) by inserting after paragraph (2) the fol-
25 lowing:

1 “(3) a description of the subject matter of each
2 of the certifications provided under section 702(h);

3 “(4) statistics revealing the number of persons
4 targeted and the number of selectors used under sec-
5 tion 702(a), disaggregated by the certification under
6 which the person was targeted;

7 “(5) the total number of directives issued pur-
8 suant to section 702(i)(1), disaggregated by each
9 type of electronic communication service provider de-
10 scribed in section 701(b)(4);”;

11 (4) in paragraph (9), as so redesignated, by
12 striking “and” at the end;

13 (5) in paragraph (10), as so redesignated, by
14 striking the period at the end and inserting a semi-
15 colon; and

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

17 “(11)(A) the total number of disseminated in-
18 telligence reports derived from collection pursuant to
19 section 702 containing the identities of United
20 States persons, regardless of whether the identities
21 of the United States persons were openly included or
22 masked;

23 “(B) the total number of disseminated intel-
24 ligence reports derived from collection not authorized
25 by this Act and conducted under procedures ap-

1 proved by the Attorney General containing the identities of United States persons, regardless of whether the identities of the United States persons were openly included or masked;

2
3
4
5 “(C) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were masked;

6
7
8
9
10 “(D) the total number of disseminated intelligence reports derived from collection not authorized by this Act and conducted under procedures approved by the Attorney General containing the identities of United States persons in which the identities of the United States persons were masked;

11
12
13
14
15
16 “(E) the total number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of United States persons in which the identities of the United States persons were openly included; and

17
18
19
20
21 “(F) the total number of disseminated intelligence reports derived from collection not authorized by this Act and conducted under procedures approved by the Attorney General containing the identities of United States persons in which the identities of United States persons in which the identities

1 ties of the United States persons were openly in-
2 cluded;

3 “(12) the number of queries conducted in an ef-
4 fort to find communications or information of or
5 about 1 or more United States persons or persons
6 reasonably believed to be located in the United
7 States at the time of the query or the time of the
8 communication or creation of the information, where
9 such communications or information were obtained
10 under procedures approved by the Attorney General
11 and without a court order, subpoena, or other legal
12 process established by statute;

13 “(13) the number of criminal proceedings in
14 which the Federal Government or a government of
15 a State or political subdivision thereof entered into
16 evidence or otherwise used or disclosed in a criminal
17 proceeding any information obtained or derived from
18 an acquisition conducted under procedures approved
19 by the Attorney General and without a court order,
20 subpoena, or other legal process established by stat-
21 ute; and

22 “(14) a good faith estimate of what percentage
23 of the communications that are subject to the proce-
24 dures described in section 309(b)(3) of the Intel-

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

3 “(A) are retained for more than 5 years;
4 and

5 “(B) are retained for more than 5 years
6 because, in whole or in part, the communica-
7 tions are encrypted.”.

8 (b) REPEAL OF NONAPPLICABILITY TO FEDERAL
9 BUREAU OF INVESTIGATION OF CERTAIN REQUIRE-
10 MENTS.—Section 603(d) of the Foreign Intelligence Sur-
11 veillance Act of 1978 (50 U.S.C. 1873(d)) is amended—

12 (1) by striking paragraph (2); and

13 (2) by redesignating paragraph (3) as para-
14 graph (2).

15 (c) CONFORMING AMENDMENT.—Section 603(d)(1)
16 of the Foreign Intelligence Surveillance Act of 1978 (50
17 U.S.C. 1873(d)(1)) is amended by striking “paragraphs
18 (3), (5), or (6)” and inserting “paragraph (6), (8), or
19 (9)”.

20 **TITLE VII—LIMITED DELAYS IN** 21 **IMPLEMENTATION**

22 **SEC. 701. LIMITED DELAYS IN IMPLEMENTATION.**

23 (a) DEFINITION.—In this section, the term “appro-
24 priate committees of Congress” 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 Sen-
5 ate; and

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

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

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

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