

AMENDMENT TO H.R. 7320
OFFERED BY MS. LOFGREN OF CALIFORNIA

Add, at the end of the bill, the following:

1 SEC. 22. DEFINITIONS.

2 For purposes of sections 23 through 28:

3 (1) INTELLIGENCE, INTELLIGENCE COMMU-
4 NITY, AND FOREIGN INTELLIGENCE.—The terms
5 “intelligence”, “intelligence community”, and “for-
6 eign intelligence” have the meanings given such
7 terms in section 3 of the National Security Act of
8 1947 (50 U.S.C. 3003).

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

1 **SEC. 23. PROHIBITION ON WARRANTLESS QUERIES FOR**
2 **THE COMMUNICATIONS OF UNITED STATES**
3 **PERSONS AND PERSONS LOCATED IN THE**
4 **UNITED STATES.**

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

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

19 (1) IN GENERAL.—Subsection (a) shall not
20 apply to a query relating to United States person or
21 persons reasonably believed to be located in the
22 United States at the time of the query or the time
23 of the communication or creation of the information
24 if—

25 (A) such persons or person are the subject
26 of an order or emergency authorization author-

1 izing electronic surveillance or physical search
2 under section 105 or 304 of the Foreign Intel-
3 ligence Surveillance Act of 1978 (50 U.S.C.
4 1805, 1824), or a warrant issued pursuant to
5 the Federal Rules of Criminal Procedure by a
6 court of competent jurisdiction covering the pe-
7 riod of the query;

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

10 (I) an emergency exists involving
11 an imminent threat of death or seri-
12 ous bodily harm; and

13 (II) in order to prevent or miti-
14 gate this threat, the query must be
15 conducted before authorization pursu-
16 ant to subparagraph (A) can, with
17 due diligence, be obtained; and

18 (ii) a description of the query is pro-
19 vided to the congressional intelligence com-
20 mittees (as defined in section 3 of the Na-
21 tional Security Act of 1947 (50 U.S.C.
22 3003)) in a timely manner;

23 (C) such persons or, if such person is in-
24 capable of providing consent, a third party le-
25 gally authorized to consent on behalf of the per-

1 son, has provided consent to the query on a
2 case-by-case basis; or

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

5 (ii) the query is conducted, and the
6 results of the query are used, for the sole
7 purpose of identifying targeted recipients
8 of malicious software and preventing or
9 mitigating harm from such malicious soft-
10 ware;

11 (iii) no additional contents of commu-
12 nications retrieved as a result of the query
13 are accessed or reviewed; and

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

17 (2) LIMITATIONS.—

18 (A) USE IN SUBSEQUENT PROCEEDINGS
19 AND INVESTIGATIONS.—No information re-
20 trieved pursuant to a query authorized by para-
21 graph (1)(B) or evidence derived from such
22 query may be used, received in evidence, or oth-
23 erwise disseminated in any investigation, trial,
24 hearing, or other proceeding in or before any
25 court, grand jury, department, office, agency,

1 regulatory body, legislative committee, or other
2 authority of the United States, a State, or polit-
3 ical subdivision thereof, except in a proceeding
4 or investigation that arises from the threat that
5 prompted the query.

6 (B) ASSESSMENT OF COMPLIANCE.—Not
7 less frequently than annually, the Attorney
8 General shall assess compliance with the re-
9 quirements under subparagraphs (A).

10 (c) MATTERS RELATING TO EMERGENCY QUE-
11 RIES.—

12 (1) TREATMENT OF DENIALS.—In the event
13 that a query for communications or information the
14 compelled production of which would require a prob-
15 able cause warrant if sought for law enforcement
16 purposes in the United States relating to 1 or more
17 United States persons or persons reasonably believed
18 to be located in the United States at the time of the
19 query or the time of communication, or creation of
20 the information is conducted pursuant to an emer-
21 gency authorization described in subsection
22 (b)(1)(A) and the application for such emergency
23 authorization is denied, or in any other case in
24 which the query has been conducted and no order is
25 issued approving the query—

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

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

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

24 (d) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF
25 1978.—This section shall not apply to queries of commu-

1 nications and information collected pursuant to the For-
2 eign Intelligence Surveillance Act of 1978 (50 U.S.C.
3 1801 et seq.).

4 (e) FOREIGN INTELLIGENCE PURPOSE.—Except as
5 provided in subsection (b)(1), no officer or employee of
6 the United States may conduct a query of information ac-
7 quired pursuant to Executive Order 12333 (50 U.S.C.
8 3001 note; relating to United States intelligence activi-
9 ties), or successor order, in an effort to find information
10 of or about 1 or more United States persons or persons
11 reasonably believed to be located in the United States at
12 the time of the query or the time of communication or
13 creation of the information unless the query is reasonably
14 likely to retrieve foreign intelligence information.

15 (f) DOCUMENTATION.—No officer or employee of the
16 Federal Government may conduct a query of information
17 acquired pursuant to Executive Order 12333 (50 U.S.C.
18 3001 note; relating to United States intelligence activi-
19 ties), or successor order, in an effort to find information
20 of or about 1 or more United States persons or persons
21 reasonably believed to be located in the United States at
22 the time of the query or the time of the communication
23 or creation of the information unless first an electronic
24 record is created, and a system, mechanism, or business

1 practice is in place to maintain such record, that includes
2 the following:

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

5 (2) The date of the query.

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

7 (4) A statement of facts showing that the use
8 of each query term included under paragraph (1) is
9 reasonably likely to retrieve foreign intelligence in-
10 formation.

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

22 **SEC. 24. PROHIBITION ON REVERSE TARGETING OF**
23 **UNITED STATES PERSONS AND PERSONS LO-**
24 **CATED IN THE UNITED STATES.**

25 (a) PROHIBITION ON ACQUISITION.—

1 (1) PROHIBITION WITH EXCEPTIONS.—No offi-
2 cer or employee of the United States may inten-
3 tionally target, pursuant to Executive Order 12333
4 (50 U.S.C. 3001 note; relating to United States in-
5 telligence activities), or successor order, any person
6 if a significant purpose of the acquisition is to target
7 1 or more United States persons or persons reason-
8 ably believed to be located in the United States at
9 the time of acquisition, communication, or the cre-
10 ation of the information as prohibited by Section
11 703 of the Foreign Intelligence Surveillance Act of
12 1978, as added by section 201 of this Act, unless—

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

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

21 (iii) a description of the targeting is
22 provided to the congressional intelligence
23 committees (as defined in section 3 of the
24 National Security Act of 1947 (50 U.S.C.
25 3003)) in a timely manner; or

1 (B) the United States person or persons
2 reasonably believed to be located in the United
3 States at the time of acquisition, communica-
4 tion or creation of the information has provided
5 consent to the targeting, or if such person is in-
6 capable of providing consent, a third party le-
7 gally authorized to consent on behalf of such
8 person has provided consent.

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

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

23 (1) an acquisition carried out pursuant to both
24 section 702 of the Foreign Intelligence Surveillance
25 Act of 1978 (50 U.S.C. 1881a), as amended by sec-

1 tion 103 of this Act, and section 703(b)(2) of the
2 Foreign Intelligence Surveillance Act of 1978, as
3 added by section 201 of this Act;

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

7 (3) an acquisition pursuant to a warrant issued
8 pursuant to the Federal Rules of Criminal Proce-
9 dure.

10 **SEC. 25. PROHIBITION ON INTELLIGENCE ACQUISITION OF**
11 **UNITED STATES PERSON DATA.**

12 (a) DEFINITIONS.—In this section:

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

16 (A) is linked to or is reasonably linkable to
17 a covered person; and

18 (B) does not include data that—

19 (i) is lawfully available to the public
20 through Federal, State, or local govern-
21 ment records or through widely distributed
22 media;

23 (ii) is reasonably believed to have been
24 voluntarily made available to the general
25 public by the covered person; or

1 (iii) is a specific communication or
2 transaction with a targeted individual who
3 is not a covered person.

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

6 (A) is reasonably believed to be located in
7 the United States at the time of the creation or
8 the time of acquisition of the covered data; or

9 (B) is a United States person.

10 (b) LIMITATION.—

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

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

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

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

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

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

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

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

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

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

4 (A) there is a reasonable belief that—

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

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

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

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

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

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

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

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

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

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

21 (c) MINIMIZATION PROCEDURES.—

22 (1) IN GENERAL.—The Attorney General shall
23 adopt specific procedures that are reasonably de-
24 signed to minimize the acquisition and retention of

1 covered data that is not subject to 1 or more of the
2 exceptions set forth in subsection (b).

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

7 (A) to exclude covered data not subject to
8 1 or more exceptions set forth in subsection (b)
9 from datasets prior to acquisition; and

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

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

20 (d) PROHIBITION ON USE OF DATA OBTAINED IN
21 VIOLATION OF THIS SECTION.—Covered data acquired by
22 an element of the intelligence community in violation of
23 subsection (b), and any evidence derived therefrom, may
24 not be used, received in evidence, or otherwise dissemi-
25 nated in any investigation, trial, hearing, or other pro-

1 ceeding in or before any court, grand jury, department,
2 office, agency, regulatory body, legislative committee, or
3 other authority of the United States, a State, or political
4 subdivision thereof.

5 (e) REPORTING REQUIREMENT.—

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

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

16 (A) A description of the covered person in-
17 formation in each dataset.

18 (B) An estimate of the amount of covered
19 person information in each dataset.

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

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

4 (A) the unclassified portion of the report
5 submitted pursuant to paragraph (1); and

6 (B) any notifications submitted pursuant
7 to paragraph (3).

8 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
9 tion shall authorize an acquisition otherwise prohibited by
10 sections 23 through 28, the Foreign Intelligence Surveil-
11 lance Act of 1978 (50 U.S.C. 1801 et seq.), or title 18,
12 United States Code.

13 **SEC. 26. PROHIBITION ON THE WARRANTLESS ACQUI-**
14 **SION OF DOMESTIC COMMUNICATIONS.**

15 (a) IN GENERAL.—No officer or employee of the
16 United States may intentionally acquire pursuant to Exec-
17 utive Order 12333 (50 U.S.C. 3001 note; relating to
18 United States intelligence activities), or successor order,
19 any communication as to which the sender and all in-
20 tended recipients are known to be located in the United
21 States at the time of acquisition or the time of commu-
22 nication except—

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

1 (2) if—

2 (A) there is a reasonable belief that—

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

6 (ii) in order to prevent or mitigate
7 this threat, the acquisition must be con-
8 ducted before an authorization pursuant to
9 the provisions of law cited in paragraph
10 (1) can, with due diligence, be obtained;
11 and

12 (B) a description of the acquisition is pro-
13 vided to the congressional intelligence commit-
14 tees (as defined in section 3 of the National Se-
15 curity Act of 1947 (50 U.S.C. 3003)) in a time-
16 ly manner.

17 (b) USE IN SUBSEQUENT PROCEEDINGS AND INVES-
18 TIGATIONS.—No information acquired pursuant to an
19 emergency described in subsection (a)(2) or information
20 derived from such acquisition may be used, received in evi-
21 dence, or otherwise disseminated in any investigation,
22 trial, hearing, or other proceeding in or before any court,
23 grand jury, department, office, agency, regulatory body,
24 legislative committee, or other authority of the United
25 States, a State, or political subdivision thereof, except in

1 a proceeding or investigation that arises from the threat
2 that prompted the acquisition.

3 **SEC. 27. DATA RETENTION LIMITS.**

4 (a) PROCEDURES.—Each head of an element of the
5 Intelligence Community shall develop and implement pro-
6 cedures governing the retention of information collected
7 pursuant to Executive Order 12333 (50 U.S.C. 3001 note;
8 relating to United States intelligence activities), or suc-
9 cessor order.

10 (b) REQUIREMENTS.—

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

14 (A) any information, including an
15 encrypted communication, to, from, or per-
16 taining to a United States person or person
17 reasonably believed to be located in the United
18 States at the time of acquisition, communica-
19 tion, or creation of the information that has
20 been evaluated and is not specifically known to
21 contain foreign intelligence information; and

22 (B) any unevaluated information, unless it
23 can reasonably be determined that the
24 unevaluated information does not contain com-
25 munications to or from, or information per-

1 taining to a United States person or person
2 reasonably believed to be located in the United
3 States at the time of acquisition, communica-
4 tion, or creation of the information.

5 (2) IN GENERAL.—The procedures developed
6 and implemented pursuant to subsection (a) shall
7 ensure, with respect to information described in such
8 subsection, that covered information shall be de-
9 stroyed within 5 years of collection unless the Attor-
10 ney General determines in writing that—

11 (A) the information is the subject of a
12 preservation obligation in pending administra-
13 tive, civil, or criminal litigation, in which case
14 the covered information shall be segregated, re-
15 tained, and used solely for that purpose and
16 shall be destroyed as soon as it is no longer re-
17 quired to be preserved for such litigation; or

18 (B) the information is being used in a pro-
19 ceeding or investigation in which the informa-
20 tion is directly related to and necessary to ad-
21 dress a specific threat identified in section
22 706(a)(2)(B) of the Foreign Intelligence Sur-
23 veillance Act of 1978 (50 U.S.C.
24 1881e(a)(2)(B)), as amended by section 102.

1 **SEC. 28. REPORTS ON VIOLATIONS OF LAW OR EXECUTIVE**
2 **ORDER.**

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

6 “(c) **PUBLIC AVAILABILITY.**—The Director of Na-
7 tional Intelligence shall make each report submitted under
8 subsection (a) publicly available on an internet website,
9 with such redactions as may be necessary to protect
10 sources and methods.

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

