

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: To prohibit warrantless access to the communications and other information of United States persons.

**IN THE SENATE OF THE UNITED STATES—118th Cong., 2d Sess.**

**H. R. 7888**

To reform the Foreign Intelligence Surveillance Act of 1978.

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. DURBIN

Viz:

1 At the appropriate place, insert the following:

2 **SEC. \_\_\_\_ . PROHIBITION ON WARRANTLESS ACCESS TO**  
3 **THE COMMUNICATIONS AND OTHER INFOR-**  
4 **MATION OF UNITED STATES PERSONS.**

5 (a) DEFINITION.—Section 702(f) is amended in para-  
6 graph (5), as so redesignated by section 2(a)(2) of this  
7 Act—

8 (1) by redesignating subparagraph (B) as sub-  
9 paragraph (C); and

10 (2) by inserting after subparagraph (A) the fol-  
11 lowing:

12 “(B) The term ‘covered query’ means a  
13 query conducted—

1                   “(i) using a term associated with a  
2                   United States person; or

3                   “(ii) for the purpose of finding the in-  
4                   formation of a United States person.”.

5           (b) PROHIBITION.—Section 702(f) of the Foreign In-  
6           telligence Surveillance Act of 1978 (50 U.S.C. 1881a(f))  
7           is amended—

8                   (1) by redesignating paragraph (5), as redesign-  
9                   nated by section 2(a)(1) of this Act, as paragraph  
10                  (8);

11                  (2) in paragraph (1)(A) by inserting “and the  
12                  limitations and requirements in paragraph (5)” after  
13                  “Constitution of the United States”; and

14                  (3) by inserting after paragraph (4), as added  
15                  by section 16(a)(1) of this Act, the following:

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

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

1 under subsection (a) and returned in response  
2 to a covered query.

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

8 “(i) the person to whom the query re-  
9 lates is the subject of an order or emer-  
10 gency authorization authorizing electronic  
11 surveillance, a physical search, or an acqui-  
12 sition under this section or section 105,  
13 section 304, section 703, or section 704 of  
14 this Act or a warrant issued pursuant to  
15 the Federal Rules of Criminal Procedure  
16 by a court of competent jurisdiction;

17 “(ii)(I) the officer or employee access-  
18 ing the communications content or infor-  
19 mation has a reasonable belief that—

20 “(aa) an emergency exists involv-  
21 ing an imminent threat of death or se-  
22 rious bodily harm; and

23 “(bb) in order to prevent or miti-  
24 gate the threat described in subitem  
25 (AA), the communications content or

1 information must be accessed before  
2 authorization described in clause (i)  
3 can, with due diligence, be obtained;  
4 and

5 “(II) not later than 14 days after the  
6 communications content or information is  
7 accessed, a description of the cir-  
8 cumstances justifying the accessing of the  
9 query results is provided to the Foreign In-  
10 telligence Surveillance Court, the congres-  
11 sional intelligence committees, the Com-  
12 mittee on the Judiciary of the House of  
13 Representatives, and the Committee on the  
14 Judiciary of the Senate;

15 “(iii) such person or, if such person is  
16 incapable of providing consent, a third  
17 party legally authorized to consent on be-  
18 half of such person, has provided consent  
19 for the access on a case-by-case basis; or

20 “(iv)(I) the communications content  
21 or information is accessed and used for the  
22 sole purpose of identifying targeted recipi-  
23 ents of malicious software and preventing  
24 or mitigating harm from such malicious  
25 software;

1           “(II) other than malicious software  
2           and cybersecurity threat signatures, no  
3           communications content or other informa-  
4           tion are accessed or reviewed; and

5           “(III) the accessing of query results is  
6           reported to the Foreign Intelligence Sur-  
7           veillance Court.

8           “(C) MATTERS RELATING TO EMERGENCY  
9           QUERIES.—

10           “(i) TREATMENT OF DENIALS.—In  
11           the event that communications content or  
12           information returned in response to a cov-  
13           ered query are accessed pursuant to an  
14           emergency authorization described in sub-  
15           paragraph (B)(i) and the subsequent appli-  
16           cation to authorize electronic surveillance,  
17           a physical search, or an acquisition pursu-  
18           ant to section 105(e), section 304(e), sec-  
19           tion 703(d), or section 704(d) of this Act  
20           is denied, or in any other case in which  
21           communications content or information re-  
22           turned in response to a covered query are  
23           accessed in violation of this paragraph—

24           “(I) no communications content  
25           or information acquired or evidence

1 derived from such access may be used,  
2 received in evidence, or otherwise dis-  
3 seminated in any investigation by or  
4 in any trial, hearing, or other pro-  
5 ceeding in or before any court, grand  
6 jury, department, office, agency, regu-  
7 latory body, legislative committee, or  
8 other authority of the United States,  
9 a State, or political subdivision there-  
10 of; and

11 “(II) no communications content  
12 or information acquired or derived  
13 from such access may subsequently be  
14 used or disclosed in any other manner  
15 without the consent of the person to  
16 whom the covered query relates, ex-  
17 cept in the case that the Attorney  
18 General approves the use or disclosure  
19 of such information in order to pre-  
20 vent the death of or serious bodily  
21 harm to any person.

22 “(ii) ASSESSMENT OF COMPLIANCE.—  
23 Not less frequently than annually, the At-  
24 torney General shall assess compliance  
25 with the requirements under clause (i).

1 “(D) FOREIGN INTELLIGENCE PURPOSE.—

2 “(i) IN GENERAL.—Except as pro-  
3 vided in clause (ii) of this subparagraph,  
4 no officer or employee of the United States  
5 may conduct a covered query of informa-  
6 tion acquired under subsection (a) unless  
7 the query is reasonably likely to retrieve  
8 foreign intelligence information.

9 “(ii) EXCEPTIONS.—An officer or em-  
10 ployee of the United States may conduct a  
11 covered query of information acquired  
12 under this section if—

13 “(I)(aa) the officer or employee  
14 conducting the query has a reasonable  
15 belief that an emergency exists involv-  
16 ing an imminent threat of death or se-  
17 rious bodily harm; and

18 “(bb) not later than 14 days  
19 after the query is conducted, a de-  
20 scription of the query is provided to  
21 the Foreign Intelligence Surveillance  
22 Court, the congressional intelligence  
23 committees, the Committee on the Ju-  
24 diciary of the House of Representa-

1                   tives, and the Committee on the Judi-  
2                   ciary of the Senate;

3                   “(II) the person to whom the  
4                   query relates or, if such person is in-  
5                   capable of providing consent, a third  
6                   party legally authorized to consent on  
7                   behalf of such person, has provided  
8                   consent for the query on a case-by-  
9                   case basis;

10                  “(III)(aa) the query is conducted,  
11                  and the results of the query are used,  
12                  for the sole purpose of identifying tar-  
13                  geted recipients of malicious software  
14                  and preventing or mitigating harm  
15                  from such malicious software;

16                  “(bb) other than malicious soft-  
17                  ware and cybersecurity threat signa-  
18                  tures, no additional contents of com-  
19                  munications acquired as a result of  
20                  the query are accessed or reviewed;  
21                  and

22                  “(cc) the query is reported to the  
23                  Foreign Intelligence Surveillance  
24                  Court; or



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

8                   “(6) DOCUMENTATION.—No officer or employee  
9                   of the United States may access communications  
10                  content, or information the compelled disclosure of  
11                  which would require a probable cause warrant if  
12                  sought for law enforcement purposes inside the  
13                  United States, returned in response to a covered  
14                  query unless an electronic record is created that in-  
15                  cludes a statement of facts showing that the access  
16                  is authorized pursuant to an exception specified in  
17                  paragraph (5)(B).

18                  “(7) QUERY RECORD SYSTEM.—The head of  
19                  each agency that conducts queries shall ensure that  
20                  a system, mechanism, or business practice is in place  
21                  to maintain the records described in paragraph (6).  
22                  Not later than 90 days after the date of enactment  
23                  of the Reforming Intelligence and Securing America  
24                  Act, the head of each agency that conducts queries

1 shall report to Congress on its compliance with this  
2 procedure.”.

3 (c) CONFORMING AMENDMENTS.—

4 (1) Section 603(b)(2) is amended, in the matter  
5 preceding subparagraph (A), by striking “, including  
6 pursuant to subsection (f)(2) of such section,”.

7 (2) Section 706(a)(2)(A)(i) is amended by  
8 striking “obtained an order of the Foreign Intel-  
9 ligence Surveillance Court to access such informa-  
10 tion pursuant to section 702(f)(2)” and inserting  
11 “accessed such information in accordance with sec-  
12 tion 702(b)(5)”.