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:

At the appropriate place, insert the following:

SEC. _____. PROHIBITION ON WARRANTLESS ACCESS TO THE COMMUNICATIONS AND OTHER INFORMATION OF UNITED STATES PERSONS.

(a) DEFINITION.—Section 702(f) is amended in paragraph (5), as so redesignated by section 2(a)(2) of this Act—

(1) by redesignating subparagraph (B) as subparagraph (C); and

(2) by inserting after subparagraph (A) the following:

"(B) The term ‘covered query’ means a query conducted—"
“(i) using a term associated with a
United States person; or
“(ii) for the purpose of finding the in-
formation of a United States person.”.

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

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

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

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

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

“(A) IN GENERAL.—Except as provided in
subparagraphs (B) and (C), no officer or em-
ployee of the United States may access commu-
ications content, or information the compelled
disclosure of which would require a probable
cause warrant if sought for law enforcement
purposes inside the United States, acquired
under subsection (a) and returned in response to a covered query.

“(B) Exceptions for concurrent authorization, consent, emergency situations, and certain defensive cybersecurity queries.—Subparagraph (A) shall not apply if—

“(i) the person to whom the query relates is the subject of an order or emergency authorization authorizing electronic surveillance, a physical search, or an acquisition under this section or section 105, section 304, section 703, or section 704 of this Act or a warrant issued pursuant to the Federal Rules of Criminal Procedure by a court of competent jurisdiction;

“(ii)(I) the officer or employee accessing the communications content or information has a reasonable belief that—

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

“(bb) in order to prevent or mitigate the threat described in subitem (AA), the communications content or
information must be accessed before
authorization described in clause (i)
can, with due diligence, be obtained;
and
“(II) not later than 14 days after the
communications content or information is
accessed, a description of the cir-
cumstances justifying the accessing of the
query results is provided to the Foreign In-
telligence Surveillance Court, the congres-
sional intelligence committees, the Com-
mittee on the Judiciary of the House of
Representatives, and the Committee on the
Judiciary of the Senate;
“(iii) such person or, if such person is
incapable of providing consent, a third
party legally authorized to consent on be-
half of such person, has provided consent
for the access on a case-by-case basis; or
“(iv)(I) the communications content
or information is accessed and used for the
sole purpose of identifying targeted recipi-
ents of malicious software and preventing
or mitigating harm from such malicious
software;
“(II) other than malicious software
and cybersecurity threat signatures, no
communications content or other informa-
tion are accessed or reviewed; and

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

“(C) MATTERS RELATING TO EMERGENCY
QUERIES.—

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

“(I) no communications content
or information acquired or evidence
derived from such access may be used, received in evidence, or otherwise disseminated in any investigation by or in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof; and

“(II) no communications content or information acquired or derived from such access may subsequently be used or disclosed in any other manner without the consent of the person to whom the covered query relates, except in the case that the Attorney General approves the use or disclosure of such information in order to prevent the death of or serious bodily harm to any person.

“(ii) ASSESSMENT OF COMPLIANCE.—
Not less frequently than annually, the Attorney General shall assess compliance with the requirements under clause (i).
“(D) FOREIGN INTELLIGENCE PURPOSE.—

“(i) IN GENERAL.—Except as provided in clause (ii) of this subparagraph, no officer or employee of the United States may conduct a covered query of information acquired under subsection (a) unless the query is reasonably likely to retrieve foreign intelligence information.

“(ii) EXCEPTIONS.—An officer or employee of the United States may conduct a covered query of information acquired under this section if—

“(I)(aa) the officer or employee conducting the query has a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm; and

“(bb) not later than 14 days after the query is conducted, a description of the query is provided to the Foreign Intelligence Surveillance Court, the congressional intelligence committees, the Committee on the Judiciary of the House of Representa-
tives, and the Committee on the Judiciary of the Senate;

“(II) the person to whom the query relates or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of such person, has provided consent for the query on a case-by-case basis;

“(III)(aa) the query is conducted, and the results of the query are used, for the sole purpose of identifying targeted recipients of malicious software and preventing or mitigating harm from such malicious software;

“(bb) other than malicious software and cybersecurity threat signatures, no additional contents of communications acquired as a result of the query are accessed or reviewed; and

“(cc) the query is reported to the Foreign Intelligence Surveillance Court; or
“(IV) the query is necessary to identify information that must be produced or preserved in connection with a litigation matter or to fulfill discovery obligations in a criminal matter under the laws of the United States or any State thereof.

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

“(7) QUERY RECORD SYSTEM.—The head of each agency that conducts queries shall ensure that a system, mechanism, or business practice is in place to maintain the records described in paragraph (6). Not later than 90 days after the date of enactment of the Reforming Intelligence and Securing America Act, the head of each agency that conducts queries
shall report to Congress on its compliance with this
procedure.”.

(c) CONFORMING AMENDMENTS.—

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

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