

112TH CONGRESS
1ST SESSION

S. _____

To improve the provisions relating to the privacy of electronic communications.

IN THE SENATE OF THE UNITED STATES

Mr. LEAHY introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To improve the provisions relating to the privacy of electronic communications.

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.**

4 This Act may be cited as the “Electronic Communica-
5 tions Privacy Act Amendments Act of 2011”.

6 **SEC. 2. PROHIBITION ON DISCLOSURE OF CONTENT.**

7 Section 2702(a)(3) of title 18, United States Code,
8 is amended to read as follows:

9 “(3) a provider of electronic communication
10 service, remote computing service, or geolocation in-
11 formation service to the public shall not knowingly

1 divulge to any governmental entity the contents of
2 any communication described in section 2703(a), or
3 any record or other information pertaining to a sub-
4 scriber or customer of such provider or service.”.

5 **SEC. 3. ELIMINATION OF 180 DAY RULE AND SEARCH WAR-**
6 **RANT REQUIREMENT; REQUIRED DISCLO-**
7 **SURE OF CUSTOMER RECORDS.**

8 (a) IN GENERAL.—Section 2703 of title 18, United
9 States Code, is amended—

10 (1) by striking subsections (a), (b), and (c) and
11 inserting the following:

12 “(a) CONTENTS OF WIRE OR ELECTRONIC COMMU-
13 NICATIONS IN ELECTRONIC STORAGE.—

14 “(1) IN GENERAL.—A governmental entity may
15 require the disclosure by a provider of electronic
16 communication service, remote computing service, or
17 geolocation information service of the contents of a
18 wire or electronic communication that is in electronic
19 storage with or otherwise held or maintained by the
20 provider if the governmental entity obtains a war-
21 rant issued and executed in accordance with the
22 Federal Rules of Criminal Procedure (or, in the case
23 of a State court, issued using State warrant proce-
24 dures) that is issued by a court of competent juris-
25 diction directing the disclosure.

1 “(A) obtains a warrant issued and exe-
2 cuted in accordance with the Federal Rules of
3 Criminal Procedure (or, in the case of a State
4 court, issued using State warrant procedures)
5 that is issued by a court of competent jurisdic-
6 tion directing the disclosure;

7 “(B) obtains a court order directing the
8 disclosure under subsection (c);

9 “(C) has the consent of the subscriber or
10 customer to the disclosure; or

11 “(D) submits a formal written request rel-
12 evant to a law enforcement investigation con-
13 cerning telemarketing fraud for the name, ad-
14 dress, and place of business of a subscriber or
15 customer of the provider or service that is en-
16 gaged in telemarketing (as defined in section
17 2325).

18 “(2) SUBPOENAS.—

19 “(A) IN GENERAL.—A governmental entity
20 may require a provider of electronic commu-
21 nication service, remote computing service, or
22 geolocation information service to disclose infor-
23 mation described in subparagraph (B) if the
24 governmental entity obtains—

1 “(i) an administrative subpoena under
2 a Federal or State statute; or

3 “(ii) a Federal or State grand jury
4 subpoena or trial subpoena.

5 “(B) REQUIREMENTS.—The information
6 described in this subparagraph is—

7 “(i) the name of the subscriber or
8 customer;

9 “(ii) the address of the subscriber or
10 customer;

11 “(iii) the local and long distance tele-
12 phone connection records, or records of
13 session times and durations, of the sub-
14 scriber or customer;

15 “(iv) length of service (including start
16 date) and types of service utilized by the
17 subscriber or customer;

18 “(v) telephone or instrument number
19 or other subscriber number or identity, in-
20 cluding any temporarily assigned network
21 address, of the subscriber or customer; and

22 “(vi) means and source of payment
23 for such service (including any credit card
24 or bank account number) of the subscriber
25 or customer.

1 “(3) NOTICE NOT REQUIRED.—A governmental
2 entity that receives records or information under
3 this subsection is not required to provide notice to
4 a subscriber or customer.”; and

5 (2) by redesignating subsections (d) through (g)
6 as subsections (c) through (f), respectively.

7 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

8 (1) SECTION 2258A.—Section 2258A(h)(1) of
9 title 18, United States Code, is amended by striking
10 “section 2703(f)” and inserting “section 2703(e)”.

11 (2) SECTION 2703.—Section 2703(c) of title 18,
12 United States Code, as redesignated by subsection
13 (a), is amended—

14 (A) by striking “A court order for disclo-
15 sure under subsection (b) or (c)” and inserting
16 “A court order for disclosure under subsection
17 (b)(1)(B) or (g)(3)(A)(ii)”;

18 (B) by striking “the contents of a wire or
19 electronic communication, or the records or
20 other information sought,” and inserting “the
21 records, other information, or historical
22 geolocation information sought”.

23 (3) SECTION 2707.—Section 2707(a) of title 18,
24 United States Code, is amended by striking “section
25 2703(e)” and inserting “section 2703(d)”.

1 (4) SECTION 3486.—Section 3486(a)(1)(C)(i) of
2 title 18, United States Code, is amended by striking
3 “section 2703(c)(2)” and inserting “section
4 2703(b)(2)(B)”.

5 **SEC. 4. DELAYED NOTICE.**

6 Section 2705 of title 18, United States Code, is
7 amended to read as follows:

8 **“§ 2705. Delayed notice**

9 “(a) DELAY OF NOTIFICATION.—

10 “(1) IN GENERAL.—A governmental entity that
11 is seeking a warrant under section 2703(a) may in-
12 clude in the application for the warrant a request for
13 an order delaying the notification required under
14 section 2703(a) for a period of not more than 90
15 days.

16 “(2) DETERMINATION.—A court shall grant a
17 request for delayed notification made under para-
18 graph (1) if the court determines that there is rea-
19 son to believe that notification of the existence of the
20 warrant may result in—

21 “(A) endangering the life or physical safety
22 of an individual;

23 “(B) flight from prosecution;

24 “(C) destruction of or tampering with evi-
25 dence;

1 “(D) intimidation of potential witnesses;

2 “(E) otherwise seriously jeopardizing an
3 investigation or unduly delaying a trial; or

4 “(F) endangering national security.

5 “(3) EXTENSION.—Upon request by a govern-
6 mental entity, a court may grant 1 or more exten-
7 sions of the delay of notification granted under para-
8 graph (2) of not more than 90 days.

9 “(4) EXPIRATION OF THE DELAY OF NOTIFICA-
10 TION.—Upon expiration of the period of delay of no-
11 tification under paragraph (2) or (3), the govern-
12 mental entity shall serve upon, or deliver to by reg-
13 istered or first-class mail, electronic mail or other
14 means reasonably calculated to be effective as speci-
15 fied by the court approving the search warrant, the
16 customer or subscriber—

17 “(A) a copy of the warrant; and

18 “(B) notice that informs the customer or
19 subscriber—

20 “(i) that information maintained for
21 the customer or subscriber by the provider
22 of electronic communication service, remote
23 computing service, or geolocation informa-
24 tion service named in the process or re-

1 quest was supplied to, or requested by, the
2 governmental entity;

3 “(ii) of the date on which the request
4 to the provider for information was made
5 by the governmental entity and the date on
6 which the information was provided by the
7 provider to the governmental entity;

8 “(iii) that notification of the customer
9 or subscriber was delayed;

10 “(iv) the identity of the court author-
11 izing the delay; and

12 “(v) of the provision of this chapter
13 under which the delay was authorized.

14 “(b) PRECLUSION OF NOTICE TO SUBJECT OF GOV-
15 ERNMENTAL ACCESS.—

16 “(1) IN GENERAL.—A governmental entity that
17 is obtaining the contents of a communication or in-
18 formation or records under section 2703 or
19 geolocation information under section 2713 may
20 apply to a court for an order directing a provider of
21 electronic communication service, remote computing
22 service, or geolocation information service to which
23 a warrant, order, subpoena, or other directive under
24 section 2703 or 2713 is directed not to notify any
25 other person of the existence of the warrant, order,

1 subpoena, or other directive for a period of not more
2 than 90 days.

3 “(2) DETERMINATION.—A court shall grant a
4 request for an order made under paragraph (1) if
5 the court determines that there is reason to believe
6 that notification of the existence of the warrant,
7 order, subpoena, or other directive may result in—

8 “(A) endangering the life or physical safety
9 of an individual;

10 “(B) flight from prosecution;

11 “(C) destruction of or tampering with evi-
12 dence;

13 “(D) intimidation of potential witnesses;

14 “(E) otherwise seriously jeopardizing an
15 investigation or unduly delaying a trial; or

16 “(F) endangering national security.

17 “(3) EXTENSION.—Upon request by a govern-
18 mental entity, a court may grant 1 or more exten-
19 sions of an order granted under paragraph (2) of
20 not more than 90 days.”.

21 **SEC. 5. LOCATION INFORMATION PRIVACY.**

22 (a) IN GENERAL.—Chapter 121 of title 18, United
23 States Code, is amended by adding at the end the fol-
24 lowing:

1 **“§ 2713. Location tracking of electronic communica-**
2 **tions device**

3 “(a) PROHIBITION.—Except as provided in sub-
4 section (b), (c), or (d), no governmental entity may access
5 or use an electronic communications device to acquire
6 geolocation information.

7 “(b) ACQUISITION PURSUANT TO A WARRANT OR
8 COURT ORDER.—A governmental entity may access or use
9 an electronic communications device to acquire geolocation
10 information if the governmental entity obtains—

11 “(1) a warrant issued and executed in accord-
12 ance with the Federal Rules of Criminal Procedure
13 relating to tracking devices (or, in the case of a
14 State court, issued using State warrant procedures),
15 issued by a court of competent jurisdiction author-
16 izing the accessing or use of an electronic commu-
17 nications device to acquire geolocation information;
18 or

19 “(2) a court order under title I or title VII of
20 the Foreign Intelligence Surveillance Act of 1978
21 (50 U.S.C. 1801 et seq. and 1881 et seq.) author-
22 izing the accessing or use of an electronic commu-
23 nications device to acquire geolocation information.

24 “(c) PERMITTED ACQUISITIONS WITHOUT COURT
25 ORDER.—A governmental entity may access or use an

1 electronic communications device to acquire geolocation
2 information—

3 “(1) as permitted under section 222(d)(4) of
4 the Communications Act of 1934 (47 U.S.C.
5 222(d)(4)) in order to respond to a call for emer-
6 gency services by a user of an electronic communica-
7 tions device; or

8 “(2) with the express consent of the owner or
9 user of the electronic communications device con-
10 cerned.

11 “(d) EMERGENCY ACQUISITION OF GEOLOCATION
12 INFORMATION.—

13 “(1) IN GENERAL.—Subject to paragraph (2),
14 an investigative or law enforcement officer specially
15 designated by the Attorney General, the Deputy At-
16 torney General, the Associate Attorney General, any
17 Assistant Attorney General, any acting Assistant At-
18 torney General, any United States attorney, any act-
19 ing United States attorney, or the principal pros-
20 ecuting attorney of any State or political subdivision
21 thereof acting pursuant to a statute of that State
22 may access or use an electronic communications de-
23 vice to acquire geolocation information if the inves-
24 tigative or law enforcement officer reasonably deter-
25 mines that—

1 “(A) an emergency situation exists that—

2 “(i) involves—

3 “(I) immediate danger of death
4 or serious bodily injury to any person;

5 “(II) conspiratorial activities
6 characteristic of organized crime; or

7 “(III) an immediate threat to na-
8 tional security; and

9 “(ii) requires the accessing or use of
10 an electronic communications device to ac-
11 quire geolocation information before an
12 order authorizing the acquisition may, with
13 due diligence, be obtained; and

14 “(B) there are grounds upon which an
15 order could be entered under this section to au-
16 thorize the accessing or use of an electronic
17 communications device to acquire geolocation
18 information.

19 “(2) ORDER AND TERMINATION.—If an inves-
20 tigative or law enforcement officer accesses or uses
21 an electronic communications device to acquire
22 geolocation information under paragraph (1)—

23 “(A) not later than 48 hours after the ac-
24 tivity to acquire the geolocation information has
25 occurred, or begins to occur, the investigative or

1 law enforcement officer shall seek a warrant or
2 order described in subsection (b) approving the
3 acquisition; and

4 “(B) unless a warrant or order described
5 in subsection (b) is issued approving the acqui-
6 sition, the activity to acquire the geolocation in-
7 formation shall terminate immediately at the
8 earlier of the time—

9 “(i) the information sought is ob-
10 tained;

11 “(ii) the application for the warrant
12 or order is denied; or

13 “(iii) at which 48 hours have elapsed
14 since the activity to acquire the geolocation
15 information began to occur.

16 “(3) VIOLATION AND SUPPRESSION OF EVI-
17 DENCE.—

18 “(A) IN GENERAL.—In a circumstance de-
19 scribed in subparagraph (B), a court may de-
20 termine that—

21 “(i) no information obtained, or evi-
22 dence derived from, geolocation informa-
23 tion acquired as part of the accessing or
24 use of an electronic communications device
25 to acquire geolocation information may be

1 received into evidence or otherwise dis-
2 closed in any trial, hearing, or other pro-
3 ceeding in or before any court, grand jury,
4 department, office, agency, regulatory
5 body, legislative committee, or other au-
6 thority of the United States, a State, or
7 political subdivision thereof; and

8 “(ii) no information concerning any
9 person acquired from the geolocation infor-
10 mation may be used or disclosed in any
11 other manner, without the consent of the
12 person.

13 “(B) CIRCUMSTANCES.—A circumstance
14 described in this subparagraph is any instance
15 in which—

16 “(i) an investigative or law enforce-
17 ment officer does not—

18 “(I) obtain a warrant or order
19 described in subsection (b) within 48
20 hours of commencing the accessing or
21 use of the electronic communications
22 device; or

23 “(II) terminate the activity to ac-
24 quire geolocation information in ac-
25 cordance with paragraph (2)(B); or

1 “(ii) a court denies the application for
2 a warrant or order approving the accessing
3 or use of an electronic communications de-
4 vice to acquire geolocation information.

5 “(e) ASSISTANCE AND COMPENSATION.—

6 “(1) IN GENERAL.—A warrant described in
7 subsection (b)(1) authorizing the accessing or use of
8 an electronic communications device to acquire
9 geolocation information shall, upon request of the
10 applicant, direct that a provider of electronic com-
11 munication service, remote computing service, or
12 geolocation information service shall provide to the
13 applicant forthwith all information, facilities, and
14 technical assistance necessary to accomplish the ac-
15 quisition unobtrusively and with a minimum of inter-
16 ference with the services that the provider is pro-
17 viding to or through the electronic communications
18 device in question.

19 “(2) COMPENSATION.—Any provider of elec-
20 tronic communication service, remote computing
21 service, or geolocation information service providing
22 information, facilities, or technical assistance under
23 a directive under paragraph (1) shall be com-
24 pensated by the applicant for reasonable expenses

1 incurred in providing the information, facilities, or
2 assistance.

3 “(f) NO CAUSE OF ACTION AGAINST A PROVIDER.—
4 No cause of action shall lie in any court against any pro-
5 vider of electronic communication service, remote com-
6 puting service, or geolocation information service, or an
7 officer, employee, or agent of the provider or other speci-
8 fied person for providing information, facilities, or assist-
9 ance necessary to accomplish an acquisition of geolocation
10 information authorized under this section.”.

11 (b) TECHNICAL AND CONFORMING AMENDMENTS.—
12 Title 18 of the United States Code is amended—

13 (1) in the table of sections for chapter 121, by
14 adding at the end the following:

“2713. Location tracking of electronic communications device.”;

15 (2) in section 2703—

16 (A) in subsection (d), as redesignated by
17 section 3, by inserting “geolocation information
18 service, or remote computing service,” after
19 “electronic communication service,”;

20 (B) in subsection (e)(1), as redesignated
21 by section 3, by striking “electronic communica-
22 tion services or a” and inserting “electronic
23 communication service, geolocation information
24 service, or”;

1 (C) in subsection (f), as redesignated by
2 section 3—

3 (i) by inserting “, geolocation infor-
4 mation service,” after “electronic commu-
5 nication service”; and

6 (ii) by inserting “, geolocation infor-
7 mation,” after “contents of communica-
8 tions”;

9 (3) in section 2711—

10 (A) in paragraph (3), by striking “and” at
11 the end;

12 (B) in paragraph (4), by striking the pe-
13 riod at the end and inserting a semicolon; and

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

15 “(5) the term ‘electronic communications de-
16 vice’ means any device that enables access to or use
17 of an electronic communications system, electronic
18 communication service, remote computing service, or
19 geolocation information service;

20 “(6) the term ‘geolocation information’—

21 “(A) means any information concerning
22 the location of an electronic communications de-
23 vice that is in whole or in part generated by or
24 derived from the operation or use of the elec-
25 tronic communications device;

1 “(B) does not include—
2 “(i) information described in section
3 2703(b)(2)(B); or
4 “(ii) the contents of a communication;
5 “(7) the term ‘geolocation information service’
6 means the provision of a global positioning service or
7 other mapping, locational, or directional information
8 service;
9 “(8) the term ‘electronic communication identi-
10 fiable information’ means the—
11 “(A) name of a person or entity;
12 “(B) address of a person or entity;
13 “(C) records of session times and dura-
14 tions of a person or entity;
15 “(D) length of service and types of service
16 used by a person or entity;
17 “(E) telephone or instrument number or
18 other subscriber number or identity (including
19 any temporarily assigned network address) of a
20 person or entity; and
21 “(F) dialing, routing, addressing, and sig-
22 naling information associated with each commu-
23 nication to or from the subscriber account of a
24 person or entity (including the date, time, and

1 duration of the communications, without geo-
2 graphical limit);

3 “(9) the term ‘toll billing records’ means the—

4 “(A) name of a person or entity;

5 “(B) address of a person or entity;

6 “(C) length of service of a person or entity;

7 and

8 “(D) local and long distance billing records
9 of a person or entity; and

10 “(10) the term ‘customer’ means any person, or
11 authorized representative of that person, who used
12 or is using any service provided by an electronic
13 communication service, remote computing service, or
14 geolocation information service, regardless of wheth-
15 er the service was, or is, being provided for a mone-
16 tary fee.”; and

17 (4) in section 3127—

18 (A) in paragraph (1), by striking “and
19 ‘contents’ have” and inserting “‘contents’, and
20 ‘geolocation information’ have”;

21 (B) in paragraph (3), by inserting “ or
22 geolocation information,” after “contents of any
23 communication”; and

1 (C) in paragraph (4), by inserting “or
2 geolocation information” after “contents of any
3 communication”.

4 **SEC. 6. REQUIRED DISCLOSURE OF LOCATION INFORMA-**
5 **TION AND WARRANT REQUIREMENT.**

6 Section 2703 of title 18, United States Code, as
7 amended by section 3, is amended by adding at the end
8 the following:

9 “(g) LOCATION INFORMATION.—

10 “(1) IN GENERAL.—Except as provided in para-
11 graph (2), a governmental entity may not require a
12 provider of electronic communication service, remote
13 computing service, or geolocation information service
14 to disclose geolocation information contempora-
15 neously or prospectively.

16 “(2) EXCEPTIONS.—

17 “(A) WARRANTS.—A governmental entity
18 may require a provider of electronic commu-
19 nication service, remote computing service, or
20 geolocation information service to disclose
21 geolocation information contemporaneously or
22 prospectively pursuant to a warrant issued and
23 executed in accordance with the Federal Rules
24 of Criminal Procedure (or, in the case of a
25 State court, issued using State warrant proce-

1 competent jurisdiction directing the disclo-
2 sure;

3 “(ii) obtains a court order directing
4 the disclosure under subsection (c); or

5 “(iii) has the consent of the subscriber
6 or customer to the disclosure.

7 “(B) NOTICE NOT REQUIRED.—A govern-
8 mental entity that receives historical geolocation
9 information under subparagraph (A) is not re-
10 quired to provide notice to a subscriber or cus-
11 tomer.”.

12 **SEC. 7. VOLUNTARY DISCLOSURES TO PROTECT CYBERSE-**
13 **CURITY.**

14 Section 2702 of title 18, United States Code is
15 amended—

16 (1) in subsection (b)(5), by inserting “, cyberse-
17 curity,” after “rights”;

18 (2) in subsection (c)(3), by inserting “, cyberse-
19 curity,” after “rights”; and

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

21 “(e) REPORTING OF CYBERSECURITY DISCLO-
22 SURES.—On an annual basis, the Attorney General of the
23 United States shall submit to the Committee on the Judi-
24 ciary of the House of Representatives and the Committee
25 on the Judiciary of the Senate a report containing—

1 “(1) the number of accounts from which the
2 Federal Government has received voluntary disclo-
3 sures under subsection (b)(5) that pertain to the
4 protection of cybersecurity; and

5 “(2) a summary of the basis for disclosure in
6 each instance where—

7 “(A) a voluntary disclosure under sub-
8 section (b)(5) that pertains to the protection of
9 cybersecurity was made to the Department of
10 Justice; and

11 “(B) the investigation pertaining to the
12 disclosure was closed without the filing of crimi-
13 nal charges.”.

14 **SEC. 8. ELECTRONIC COMMUNICATION IDENTIFIABLE IN-**
15 **FORMATION.**

16 (a) **IN GENERAL.**—Section 2709(a) of title 18,
17 United States Code, is amended by striking “electronic
18 communication transactional records” and inserting “elec-
19 tronic communication identifiable information”.

20 (b) **REQUIRED CERTIFICATION.**—Section 2709(b) of
21 title 18, United States Code, is amended to read as fol-
22 lows:

23 “(b) **REQUIRED CERTIFICATION.**—The Director of
24 the Federal Bureau of Investigation, or a designee in a
25 position not lower than Deputy Assistant Director at Bu-

1 reau headquarters or a Special Agent in Charge in a Bu-
2 reau field office designated by the Director, may request
3 the toll billing records and electronic communication iden-
4 tifiable information of a person or entity if the Director
5 (or designee) certifies in writing to the wire or electronic
6 communication service provider or geolocation information
7 service provider to which the request is made that the toll
8 billing records and electronic communication identifiable
9 information sought are relevant to an authorized inves-
10 tigation to protect against international terrorism or clan-
11 destine intelligence activities, provided that such an inves-
12 tigation of a United States person is not conducted solely
13 on the basis of activities protected by the First Amend-
14 ment to the Constitution of the United States.”.