

115TH CONGRESS
1ST SESSION

S. 1657

To amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers and for geolocation information in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 27, 2017

Mr. LEE (for himself and Mr. LEAHY) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers and for geolocation information in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes.

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 “ECPA Modernization
5 Act of 2017”.

1 **SEC. 2. WARRANT FOR STORED CONTENT AND**
2 **GEOLOCATION INFORMATION.**

3 (a) VOLUNTARY DISCLOSURE OF CUSTOMER COMMU-
4 NICATIONS OR RECORDS.—Section 2702 of title 18,
5 United States Code, is amended—

6 (1) in subsection (a)—

7 (A) in paragraph (1)—

8 (i) by striking “divulge” and inserting
9 “disclose”; and

10 (ii) by striking “while in electronic
11 storage by that service” and inserting
12 “that is in electronic storage with or other-
13 wise stored, held, or maintained by that
14 service”;

15 (B) in paragraph (2), in the matter pre-
16 ceding subparagraph (A)—

17 (i) by striking “to the public”;

18 (ii) by striking “divulge” and insert-
19 ing “disclose”; and

20 (iii) by striking “which is carried or
21 maintained on” and inserting “that is
22 stored, held, or maintained by”; and

23 (C) in paragraph (3)—

24 (i) by striking “a provider of” and in-
25 serting “a person or entity providing”;

1 (ii) by inserting “, or a geolocation
2 service,” after “public”;

3 (iii) by striking “divulge” and insert-
4 ing “disclose the contents of any commu-
5 nication described in section 2703(a)”;

6 (iv) by striking “a record” and insert-
7 ing “, any records, geolocation informa-
8 tion,”; and

9 (v) by striking “(not including the
10 contents of communications covered by
11 paragraph (1) or (2)) to any governmental
12 entity” and inserting “to any governmental
13 entity”;

14 (2) in subsection (b)—

15 (A) in the matter preceding paragraph
16 (1)—

17 (i) by striking “divulge” and inserting
18 “disclose”; and

19 (ii) by inserting “wire or electronic”
20 before “communication”;

21 (B) by striking paragraph (1) and insert-
22 ing the following:

23 “(1) to an originator, addressee, or intended re-
24 cipient of such communication, to the subscriber or
25 customer on whose behalf the provider stores, holds,

1 or maintains such communication, or to an agent of
 2 such addressee, intended recipient, subscriber, or
 3 customer;”; and

4 (C) by striking paragraph (3) and insert-
 5 ing the following:

6 “(3) with the lawful consent of the originator,
 7 addressee, or intended recipient of such communica-
 8 tion, or of the subscriber or customer on whose be-
 9 half the provider stores, holds, or maintains such
 10 communication;”; and

11 (3) in subsection (c)—

12 (A) in the matter preceding paragraph
 13 (1)—

14 (i) by striking “divulge” and inserting
 15 “disclose”;

16 (ii) by inserting “, geolocation infor-
 17 mation,” after “record”; and

18 (iii) by inserting “wire or electronic”
 19 before “communications”;

20 (B) in paragraph (2)—

21 (i) by striking “customer” and insert-
 22 ing “subscriber”; and

23 (ii) by striking “or subscriber” and
 24 inserting “or customer”;

1 (C) in paragraph (5), by striking “or” at
 2 the end;

3 (D) in paragraph (6), by striking the pe-
 4 riod at the end and inserting “; or”; and

5 (E) by adding at the end the following:

6 “(7) to a governmental entity as permitted
 7 under section 222(d)(4) of the Communications Act
 8 of 1934 (47 U.S.C. 222(d)(4)) in order to respond
 9 to a call for emergency services by a user of an elec-
 10 tronic communications device.”.

11 (b) REQUIRED DISCLOSURE OF CUSTOMER COMMU-
 12 NICATIONS OR RECORDS.—Section 2703 of title 18,
 13 United States Code, is amended—

14 (1) in subsection (a)—

15 (A) in the first sentence—

16 (i) by inserting “or remote computing
 17 service” after “service”;

18 (ii) by striking “in an electronic com-
 19 munications system for one hundred and
 20 eighty days or less, only pursuant to” and
 21 inserting “with or otherwise stored, held,
 22 or maintained by the provider only if the
 23 governmental entity obtains”; and

24 (iii) by inserting “directing disclo-
 25 sure” before the period at the end; and

1 (B) by striking the second sentence;

2 (2) by striking subsection (b) and inserting the
3 following:

4 “(b) NOTICE.—Except as provided in section 2705,
5 not later than 10 business days after a governmental enti-
6 ty receives the contents of a wire or electronic communica-
7 tion of a subscriber or customer from a provider of elec-
8 tronic communication service or remote computing service,
9 the governmental entity shall serve upon, or deliver to by
10 registered or first-class mail, electronic mail, or other
11 means reasonably calculated to be effective as may be
12 specified by the court issuing the warrant, the subscriber
13 or customer—

14 “(1) a copy of the warrant or emergency re-
15 quest; and

16 “(2) a notice that includes the information re-
17 ferred to in clauses (i) and (ii) of section
18 2705(a)(4)(B).”;

19 (3) in subsection (c)—

20 (A) in paragraph (1)—

21 (i) in the matter preceding subpara-
22 graph (A)—

23 (I) by striking “A governmental”
24 and inserting “IN GENERAL.—Subject
25 to paragraph (2), a governmental”;

1 (II) by inserting “, geolocation
2 information service,” after “commu-
3 nication service”;

4 (III) by striking “to or” and in-
5 serting “or”;

6 (IV) by striking “of such service”
7 and inserting “of the provider or serv-
8 ice”;

9 (V) by inserting “or geolocation
10 information” after “communications”;
11 and

12 (VI) by striking “when” and in-
13 serting “if”;

14 (ii) in subparagraph (A), by inserting
15 “directing disclosure” before the semicolon
16 at the end;

17 (iii) in subparagraph (B)—

18 (I) by striking “for such” and in-
19 serting “directing”; and

20 (II) by striking “of this section”;

21 (iv) in subparagraph (C), by striking
22 the semicolon at the end and inserting “;
23 or”;

24 (v) in subparagraph (D), by striking
25 “; or” and inserting a period; and

1 (vi) by striking subparagraph (E);

2 (B) in paragraph (2)—

3 (i) by striking “A provider” and in-
4 serting “INFORMATION TO BE DIS-
5 CLOSED.—A governmental entity may re-
6 quire a provider”;

7 (ii) by inserting “, geolocation infor-
8 mation service,” after “communication
9 service”;

10 (iii) by striking “shall disclose to a
11 governmental entity” and inserting “to dis-
12 close, in response to an administrative sub-
13 poena authorized by Federal or State stat-
14 ute, a grand jury, trial, or civil discovery
15 subpoena, or any means authorized under
16 paragraph (1)”;

17 (iv) in the matter following subpara-
18 graph (F)—

19 (I) by striking “such” and insert-
20 ing “the provider or”; and

21 (II) by striking “when the gov-
22 ernmental entity uses an administra-
23 tive subpoena authorized by a Federal
24 or State statute or a Federal or State
25 grand jury or trial subpoena or any

1 means available under paragraph
 2 (1)”; and

3 (C) in paragraph (3)—

4 (i) by striking “A governmental” and
 5 inserting “NOTICE NOT REQUIRED.—A
 6 governmental”; and

7 (ii) by striking “receiving” and insert-
 8 ing “that receives”;

9 (4) in subsection (f)(1)—

10 (A) by inserting “, geolocation information
 11 service,” after “communication services”;

12 (B) by striking “a remote” and inserting
 13 “remote”; and

14 (C) by inserting “, geolocation informa-
 15 tion,” after “records”;

16 (5) in subsection (g)—

17 (A) by inserting “, geolocation information
 18 service,” after “communications service”; and

19 (B) by inserting “, geolocation informa-
 20 tion,” after “of communications”; and

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

22 “(h) GEOLOCATION INFORMATION.—

23 “(1) IN GENERAL.—A governmental entity may
 24 require a provider of electronic communication serv-
 25 ice, geolocation information service, or remote com-

1 puting service, to disclose stored geolocation infor-
2 mation only pursuant to a warrant issued and exe-
3 cuted in accordance with the Federal Rules of
4 Criminal Procedure (or, in the case of a State court,
5 issued using State warrant procedures), issued by a
6 court of competent jurisdiction.

7 “(2) NOTICE.—Except as provided in section
8 2705, not later than 10 business days after a gov-
9 ernmental entity acquires stored geolocation infor-
10 mation, the governmental entity shall serve upon, or
11 deliver to by registered or first-class mail, electronic
12 mail, or other means reasonably calculated to be ef-
13 fective as may be specified by the court issuing the
14 warrant, the subscriber or customer—

15 “(A) a copy of the warrant or emergency
16 request; and

17 “(B) a notice that includes the information
18 referred to in clauses (i) and (ii) of section
19 2705(a)(4)(B).

20 “(i) RULE OF CONSTRUCTION RELATED TO LEGAL
21 PROCESS.—Nothing in this section or in section 2702
22 shall limit an otherwise lawful authority of a governmental
23 entity to use an administrative subpoena authorized by
24 Federal or State statute, a grand jury, trial, or civil dis-
25 covery subpoena, or a warrant issued using the procedures

1 described in the Federal Rules of Criminal Procedure (or,
2 in the case of a State court, issued using State warrant
3 procedures) by a court of competent jurisdiction to—

4 “(1) require an originator, addressee, or in-
5 tended recipient of a wire or electronic communica-
6 tion to disclose a wire or electronic communication
7 (including the contents of that communication) to
8 the governmental entity;

9 “(2) require a person or entity that provides an
10 electronic communication service to the officers, di-
11 rectors, employees, or agents of the person or entity
12 (for the purpose of carrying out their duties) to dis-
13 close wire or electronic communication (including the
14 contents of that communication) to or from the per-
15 son or entity itself or to or from an officer, director,
16 employee, or agent of the entity to a governmental
17 entity, if the wire or electronic communication is
18 stored, held, or maintained on an electronic commu-
19 nications system owned, operated, or controlled by
20 the person or entity; or

21 “(3) require a person or entity that provides a
22 remote computing service or electronic communica-
23 tion service to disclose a wire or electronic commu-
24 nication (including the contents of that communica-
25 tion) that advertises or promotes a product or serv-

1 ice and that has been made readily accessible to the
 2 general public.”.

3 (c) COST REIMBURSEMENT.—Section 2706(a) of title
 4 18, United States Code, is amended by inserting
 5 “geolocation information,” after “records,”.

6 **SEC. 3. PARTICULARITY REQUIREMENT FOR STORED ELEC-**
 7 **TRONIC RECORDS.**

8 Section 2703(d) of title 18, United States Code, is
 9 amended—

10 (1) by redesignating—

11 (A) the first and second sentences as para-
 12 graph (1) and adjusting the margins accord-
 13 ingly; and

14 (B) the third sentence as paragraph (2)
 15 and adjusting the margins accordingly;

16 (2) in paragraph (1), as redesignated—

17 (A) in the first sentence—

18 (i) by striking “(b) or”; and

19 (ii) by striking “the contents of a wire
 20 or electronic communication, or”; and

21 (B) by inserting “The court order shall de-
 22 scribe with particularity the records or other in-
 23 formation to be seized by specifying, as appro-
 24 priate and reasonable in light of the specific cir-
 25 cumstances of the investigation, the time peri-

1 ods covered, the target individuals or accounts,
 2 the applications or services covered, and the
 3 types of information sought.” after “investiga-
 4 tion.”; and

5 (3) in paragraph (2), as redesignated—

6 (A) by striking “, if” and inserting “, if—
 7 ”;

8 (B) by striking “the information” and in-
 9 serting “(A) the information”;

10 (C) by inserting “; or” after “nature”; and

11 (D) by striking “or compliance” and in-
 12 serting “(B) compliance”.

13 **SEC. 4. NOTICE OF LAWFULLY OBTAINED INFORMATION.**

14 Section 2705 of title 18, United States Code, is
 15 amended—

16 (1) in subsection (a)—

17 (A) by striking paragraph (1) and insert-
 18 ing the following:

19 “(1) IN GENERAL.—A governmental entity that
 20 is seeking a warrant under subsection (a) or (h) of
 21 section 2703 may include in the application for the
 22 warrant a request for an order delaying the notifica-
 23 tion required under section 2703(b) for a period of
 24 not more than 90 days.”;

1 (B) in paragraph (2), in the matter pre-
2 ceding subparagraph (A), by striking “An ad-
3 verse result for the purposes of paragraph (1)
4 of this subsection is” and inserting “DETER-
5 MINATION.—A court shall grant a request for
6 delayed notification made under paragraph (1)
7 if the court determines that there is reason to
8 believe, based on specific and articulable facts,
9 that notification of the existence of the warrant
10 will result in”;

11 (C) by striking paragraphs (3) and (4) and
12 inserting the following:

13 “(3) EXTENSION.—Upon request by a govern-
14 mental entity, a court may grant one or more exten-
15 sions of the delay of notification granted under para-
16 graph (2) of not more than 90 days.”;

17 (D) by redesignating paragraph (5) as
18 paragraph (4);

19 (E) in paragraph (4), as redesignated,—

20 (i) in the matter preceding subpara-
21 graph (A)—

22 (I) by striking “Upon” and in-
23 serting “EXPIRATION OF THE DELAY
24 OF NOTIFICATION.—Upon”;

1 (II) by striking “(1) or (4) of
2 this subsection” and inserting “(2) or
3 (3)”;

4 (III) by inserting “to” after “de-
5 liver”; and

6 (IV) by striking “to,” and insert-
7 ing “, electronic mail, or other means
8 reasonably calculated to be effective
9 as specified by the court approving
10 the search warrant,”;

11 (ii) by striking subparagraph (A);

12 (iii) by striking “a copy of the process
13 or request together with notice that” and
14 inserting the following:

15 “(A) a copy of the warrant; and”; and

16 (iv) in subparagraph (B)—

17 (I) in the matter preceding clause

18 (i)—

19 (aa) by inserting “notice
20 that” before “informs”; and

21 (bb) by striking “such” and
22 inserting “the”;

23 (II) by redesignating—

1 (aa) clauses (ii) through (iv)
2 as clauses (iv) through (vi), re-
3 spectively; and

4 (bb) clause (i) as clause (ii);
5 (III) by adding before clause (ii),
6 as redesignated, the following:

7 “(i) of the nature of the law enforce-
8 ment inquiry with reasonable specificity;”;

9 (IV) in clause (ii), as redesign-
10 nated, by striking “to or requested by
11 that governmental authority and the
12 date on which the supplying or re-
13 quest took place” and inserting “to,
14 or requested by, the governmental en-
15 tity”;

16 (V) by inserting after clause (ii),
17 as redesignated, the following:

18 “(iii) of the date on which the warrant
19 was served on the provider and the date on
20 which the information was provided by the
21 provider to the governmental entity;”;

22 (VI) in clause (v), as redesign-
23 nated, by striking “what governmental
24 entity or court made the certification
25 or determination pursuant to which

1 that delay was made” and inserting
 2 “the identity of the court authorizing
 3 the delay”; and

4 (VII) in clause (vi), as redesign-
 5 nated, by striking “which provision of
 6 this chapter allowed such delay” and
 7 inserting “of the provision of this
 8 chapter under which the delay was au-
 9 thorized”; and

10 (F) by striking paragraph (6); and

11 (2) by striking subsection (b) and inserting the
 12 following:

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

15 “(1) IN GENERAL.—A governmental entity that
 16 is obtaining the contents of a communication or in-
 17 formation or records under section 2703 may apply
 18 to a court for an order directing a provider of elec-
 19 tronic communication service, geolocation service, or
 20 remote computing service to which a warrant, order,
 21 subpoena, or other directive under section 2703 is
 22 directed not to notify any other person of the exist-
 23 ence of the warrant, order, subpoena, or other direc-
 24 tive for a period of not more than 90 days.

1 “(2) DETERMINATION.—A court shall grant a
 2 request for an order made under paragraph (1) if
 3 the court determines that there is reason to believe,
 4 based on specific and articulable facts, that notifica-
 5 tion of the existence of the warrant, order, subpoena,
 6 or other directive will result in—

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

9 “(B) flight from prosecution;

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

12 “(D) intimidation of potential witnesses; or

13 “(E) otherwise seriously jeopardizing an
 14 investigation or unduly delaying a trial.

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

19 “(4) NOTIFICATION OF CHANGED CIR-
 20 CUMSTANCES.—Upon conclusion of the investigation
 21 for which a warrant, order, subpoena, or other direc-
 22 tive under section 2703 was sought, or if the need
 23 for the nondisclosure order under subparagraph (2)
 24 ceases to exist, the governmental entity that re-
 25 quested the nondisclosure order shall, within a rea-

1 sonable period of time, notify the court of the
2 changed circumstances so that the nondisclosure
3 order can be reassessed or vacated.

4 “(5) EXCEPTION.—A provider of electronic
5 communication service or remote computing service
6 to which an order under subsection (b)(2) applies, or
7 officer, employee, or agent thereof, may disclose in-
8 formation otherwise subject to any applicable non-
9 disclosure requirement to—

10 “(A) those persons to whom disclosure is
11 necessary in order to comply with the request;

12 “(B) an attorney in order to obtain legal
13 advice or assistance regarding the request; and

14 “(C) upon an application by a provider,
15 any person the court determines can be notified
16 of the request without causing the adverse re-
17 sult in subparagraph (2) that serves as the
18 basis for the issuance of the nondisclosure
19 order.

20 “(6) SCOPE OF NONDISCLOSURE ORDER.—Any
21 person to whom disclosure is made under paragraph
22 (5) shall be subject to the nondisclosure require-
23 ments applicable to the person to whom the order is
24 issued under subparagraph (2) in the same manner
25 as the person to whom the request is issued. Any re-

1 cipient that discloses to a person information other-
 2 wise subject to a nondisclosure requirement shall no-
 3 tify the person of the applicable nondisclosure re-
 4 quirement.”.

5 **SEC. 5. WARRANT REQUIREMENT FOR REAL-TIME**
 6 **GEOLOCATION INFORMATION AND LOCATION**
 7 **TRACKING.**

8 (a) DEFINITIONS.—Section 2711 of title 18, United
 9 States Code, is amended—

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

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

14 (3) 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 past or current location of an electronic
 23 communications device that is in whole or in
 24 part generated by or derived from the operation

1 or use of the electronic communications device;
 2 and

3 “(B) does not include—

4 “(i) information described in section
 5 2703(c)(2); or

6 “(ii) the contents of a communication;
 7 and

8 “(7) the term ‘geolocation information service’
 9 means the provision of a service or functionality that
 10 uses or collects geolocation information.”.

11 (b) LOCATION TRACKING OF ELECTRONIC COMMU-
 12 NICATIONS DEVICE.—

13 (1) IN GENERAL.—Chapter 121 of title 18,
 14 United States Code, is amended by adding at the
 15 end the following:

16 **“SEC. 2713. LOCATION TRACKING OF ELECTRONIC COMMU-
 17 NICATIONS DEVICE.**

18 “(a) PROHIBITION.—Except as provided in sub-
 19 section (b), (c), or (d), or section 2702 or 2703, no govern-
 20 mental entity may access or use an electronic communica-
 21 tions device to acquire geolocation information.

22 “(b) ACQUISITION PURSUANT TO A WARRANT OR
 23 COURT ORDER.—A governmental entity may access or use
 24 an electronic communications device to acquire geolocation
 25 information if the governmental entity obtains—

1 “(1) a warrant issued and executed in accord-
2 ance with provisions relating to tracking devices in
3 the Federal Rules of Criminal Procedure (or, in the
4 case of a State court, issued using State warrant
5 procedures), issued by a court of competent jurisdic-
6 tion authorizing the access or use of an electronic
7 communications device to acquire geolocation infor-
8 mation; or

9 “(2) a court order under title I, title III, or title
10 VII of the Foreign Intelligence Surveillance Act of
11 1978 (50 U.S.C. 1801 et seq., 1821 et seq., and
12 1881 et seq.) authorizing the access or use of an
13 electronic communications device to acquire
14 geolocation information.

15 “(c) PERMITTED ACQUISITIONS WITHOUT COURT
16 ORDER.—A governmental entity may access or use an
17 electronic communications device to acquire geolocation
18 information—

19 “(1) as permitted under section 222(d)(4) of
20 the Communications Act of 1934 (47 U.S.C.
21 222(d)(4)) in order to respond to a call for emer-
22 gency services by a user of an electronic communica-
23 tions device;

1 “(2) with the lawful consent of the owner or au-
2 thorized user of the electronic communications de-
3 vice concerned; or

4 “(3) if the owner or user of the electronic com-
5 munications device concerned has knowingly commu-
6 nicated geolocation information in a manner that is
7 readily accessible to the general public.

8 “(d) EMERGENCY ACQUISITION OF GEOLOCATION
9 INFORMATION.—

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

23 “(A) an emergency situation exists that—

24 “(i) involves—

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

4 “(II) an immediate threat to na-
5 tional security; and

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

11 “(B) in circumstances in which geolocation
12 information may be used as evidence of a crime
13 or in furtherance of a criminal investigation,
14 there are grounds upon which an order could be
15 entered under this section to authorize the ac-
16 cessing or use of an electronic communications
17 device to acquire geolocation information.

18 “(2) NOTICE, ORDER AND TERMINATION.—If
19 an investigative or law enforcement officer accesses
20 or uses an electronic communications device to ac-
21 quire geolocation information under paragraph (1)—

22 “(A) the officer shall, not later than 10
23 business days after acquiring geolocation infor-
24 mation, serve upon, or deliver to by registered
25 or first-class mail, electronic mail, or other

1 means reasonably calculated to be effective, no-
2 tice to the owner or authorized user of the elec-
3 tronic communications device whose geolocation
4 information was acquired that such information
5 was obtained or accessed pursuant to the emer-
6 gency provisions under this subsection and de-
7 scribing the factual bases that led to the offi-
8 cer's determination that an emergency situation
9 existed;

10 “(B) in circumstances in which geolocation
11 information may be used as evidence of a crime
12 or in furtherance of a criminal investigation,
13 not later than 48 hours after the activity to ac-
14 quire or access the geolocation information has
15 occurred, or begins to occur, the investigative or
16 law enforcement officer shall seek a warrant or
17 order described in subsection (b) approving the
18 acquisition; and

19 “(C) unless a warrant or order described
20 in subsection (b) is issued approving the acqui-
21 sition, the activity to acquire the geolocation in-
22 formation shall terminate immediately at the
23 earlier of the time—

24 “(i) the information sought is ob-
25 tained;

1 “(ii) the application for the warrant
2 or order is denied; or

3 “(iii) at which 48 hours have elapsed
4 since the activity to acquire or access the
5 geolocation information began to occur.

6 “(3) VIOLATION AND SUPPRESSION OF EVI-
7 DENCE.—

8 “(A) IN GENERAL.—In a circumstance de-
9 scribed in subparagraph (B)—

10 “(i) no information obtained, or evi-
11 dence derived, from geolocation informa-
12 tion acquired as part of the access or use
13 of an electronic communications device to
14 acquire geolocation information may be re-
15 ceived into evidence or otherwise disclosed
16 in any trial, hearing, or other proceeding
17 in or before any court, grand jury, depart-
18 ment, office, agency, regulatory body, legis-
19 lative committee, or other authority of the
20 United States, a State, or political subdivi-
21 sion thereof;

22 “(ii) no information concerning any
23 person acquired from the geolocation infor-
24 mation may be used, disseminated, or dis-

1 closed in any other manner, without the
2 consent of the person; and

3 “(iii) all information collected shall be
4 promptly destroyed.

5 “(B) CIRCUMSTANCES.—A circumstance
6 described in this subparagraph is any instance
7 in which—

8 “(i) an investigative or law enforce-
9 ment officer does not—

10 “(I) obtain a warrant or order
11 described in subsection (b) within 48
12 hours of commencing the access or
13 use of the electronic communications
14 device; or

15 “(II) terminate the activity to ac-
16 quire geolocation information in ac-
17 cordance with paragraph (2)(B); or

18 “(ii) a court denies the application for
19 a warrant or order approving the accessing
20 or use of an electronic communications de-
21 vice to acquire geolocation information.

22 “(e) ASSISTANCE AND COMPENSATION.—

23 “(1) IN GENERAL.—A warrant described in
24 subsection (b)(1) authorizing the accessing or use of
25 an electronic communications device to acquire

1 geolocation information shall, upon request of the
2 applicant, direct that a provider of electronic com-
3 munication service, remote computing service, or
4 geolocation information service shall provide to the
5 applicant forthwith all information, facilities, and
6 technical assistance necessary to accomplish the ac-
7 quisition unobtrusively and with a minimum of inter-
8 ference with the services that the provider is pro-
9 viding to or through the electronic communications
10 device in question.

11 “(2) COMPENSATION.—Any provider of elec-
12 tronic communication service, remote computing
13 service, or geolocation information service providing
14 information, facilities, or technical assistance under
15 a directive under paragraph (1) shall be com-
16 pensated by the applicant for reasonable expenses
17 incurred in providing the information, facilities, or
18 assistance.

19 “(f) NO CAUSE OF ACTION AGAINST A PROVIDER.—
20 No cause of action shall lie in any court against any pro-
21 vider of electronic communication service, remote com-
22 puting service, or geolocation information service, or an
23 officer, employee, or agent of the provider or other speci-
24 fied person for providing information, facilities, or assist-

1 ance necessary to accomplish an acquisition of geolocation
2 information authorized under this section.”.

3 (2) TECHNICAL AND CONFORMING AMEND-
4 MENT.—The table of sections for chapter 121 of
5 title 18, United States Code, is amended by adding
6 at the end the following:

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

7 **SEC. 6. SUPPRESSION OF UNLAWFULLY OBTAINED WIRE**
8 **OR ELECTRONIC COMMUNICATION OR**
9 **GEOLOCATION INFORMATION.**

10 (a) IN GENERAL.—Chapter 121 of title 18, United
11 States Code, as amended by section 5(b), is amended by
12 adding at the end the following:

13 **“§ 2714. Suppression remedy**

14 “(a) IN GENERAL.—If a governmental entity requires
15 the disclosure of a wire or electronic communication or
16 geolocation information in violation of this chapter, or ac-
17 cesses or uses an electronic communications device to ac-
18 quire geolocation information in violation of this chapter,
19 no part of the contents of the communication, no
20 geolocation information, and no evidence derived there-
21 from may be received in evidence in any trial, hearing,
22 or other proceeding in or before any court, grand jury,
23 department, officer, agency, regulatory body, legislative
24 committee, or other authority of the United States, a
25 State, or a political subdivision thereof.

1 “(b) GROUND.—An aggrieved person in a trial,
2 hearing, or proceeding in or before a court, department,
3 officer, agency, regulatory body, or other authority of the
4 United States, a State, or a political subdivision thereof
5 may move to suppress the contents of any wire or elec-
6 tronic communication or geolocation information disclosed
7 or acquired under this chapter, or evidence derived there-
8 from, on the grounds that—

9 “(1) the communication or information was un-
10 lawfully disclosed;

11 “(2) the warrant under which it was disclosed
12 is insufficient on its face; or

13 “(3) the disclosure was not made in conformity
14 with the warrant.

15 “(c) PROCEDURE.—

16 “(1) TIMING.—A motion under subsection (b)
17 shall be made before the trial, hearing, or proceeding
18 commences, unless there was no opportunity to
19 make such motion or the person was not aware of
20 the grounds of the motion.

21 “(2) INSPECTION.—The judge or other official,
22 upon the filing of a motion under subsection (b),
23 may make available to the aggrieved person or the
24 attorney for the aggrieved person for inspection such
25 portions of the disclosed communication, geolocation

1 information, or evidence derived therefrom as the
2 judge or other official determines to be in the inter-
3 ests of justice.

4 “(3) MOTION GRANTED.—If a motion under
5 subsection (b) is granted, the contents of the dis-
6 closed wire or electronic communication, geolocation
7 information, or evidence derived therefrom, shall be
8 treated as having been obtained in violation of this
9 chapter.

10 “(d) APPEAL.—In addition to any other right to ap-
11 peal, the United States shall have the right to appeal an
12 order granting a motion to suppress made under sub-
13 section (b) if the United States attorney certifies to the
14 judge or other official granting such motion that the ap-
15 peal is not taken for purposes of delay. Such appeal shall
16 be taken within 30 days after the date the order was en-
17 tered and shall be diligently prosecuted.

18 “(e) DEFINITION.—In this section, the term ‘ag-
19 grieved person’ means—

20 “(1) a person whose wire or electronic commu-
21 nication or geolocation information was disclosed
22 pursuant to this chapter; or

23 “(2) the owner or authorized user of the elec-
24 tronic communications device whose geolocation in-
25 formation was acquired pursuant to this chapter.”.

1 (b) TECHNICAL AND CONFORMING AMENDMENT.—
 2 The table of sections for chapter 121 of title 18, United
 3 States Code, as amended by section 5(b), is amended by
 4 adding at the end the following:

“2714. Suppression remedy.”.

5 **SEC. 7. PEN REGISTER AND TRAP AND TRACE REFORMS.**

6 (a) APPLICATION FOR AN ORDER FOR A PEN REG-
 7 ISTER OR A TRAP AND TRACE DEVICE.—Section
 8 3122(b)(2) of title 18, United States Code, is amended—

9 (1) by striking “a certification by the appli-
 10 cant” and inserting “specific and articulable facts
 11 showing that there are reasonable grounds to be-
 12 lieve”; and

13 (2) by inserting “and material” after “rel-
 14 evant”.

15 (b) ISSUANCE OF AN ORDER FOR A PEN REGISTER
 16 OR A TRAP AND TRACE DEVICE.—Section 3123 of title
 17 18, United States Code, is amended—

18 (1) in subsection (a)—

19 (A) in paragraph (1)—

20 (i) by striking “certified to the court”
 21 and inserting “offered specific and
 22 articulable facts showing that there are
 23 reasonable grounds to believe”; and

24 (ii) by inserting “and material” after
 25 “relevant”; and

1 (B) in paragraph (2)—

2 (i) by striking “has certified to the
3 court” and inserting “offered specific and
4 articulable facts showing that there are
5 reasonable grounds to believe”; and

6 (ii) by inserting “and material” after
7 “relevant”; and

8 (2) in subsection (d)—

9 (A) in paragraph (1), by inserting “for a
10 period of 30 days after termination of the
11 order, unless” after “sealed”; and

12 (B) in paragraph (2), by inserting “for a
13 period of 30 days after termination of the
14 order” after “investigation”.

15 **SEC. 8. GAO AND FCC REPORT ON CELL-SITE SIMULATORS.**

16 (a) FCC REPORT.—Not later than 1 year after the
17 date of enactment, the Federal Communications Commis-
18 sion shall submit to the Committee on the Judiciary of
19 the Senate and Committee on the Judiciary of the House
20 of Representatives a report regarding the domestic use of
21 cell-site simulators (or “IMSI catchers”) by Federal,
22 State, and local law enforcement agencies, which shall in-
23 clude—

24 (1) an evaluation of the security vulnerabilities
25 in cellular phones and cellular networks exploited by

1 cell-site simulators, and the extent to which those
2 vulnerabilities could be or have been exploited by
3 criminals or foreign governments; and

4 (2) an analysis of whether the use of cell-site
5 simulators results in disruptions in cellular phone
6 service in affected areas and the extent of such dis-
7 ruptions.

8 (b) GAO REPORT.—Not later than 1 year after the
9 date of enactment, the Comptroller General of the United
10 States shall submit to the Committee on the Judiciary of
11 the Senate and the Committee on the Judiciary of the
12 House of Representatives a report regarding the domestic
13 use of cell-site simulators (or “TMSI catchers”) by Fed-
14 eral, State, and local law enforcement agencies, which to
15 the extent feasible shall include—

16 (1) a list of each Federal, State, and local law
17 enforcement agency that uses cell-site simulators,
18 and for what purposes, including whether the devices
19 are used to monitor protests or other large public
20 gatherings and the types of crimes they are used to
21 investigate;

22 (2) the extent to which the Federal Government
23 is providing or funding the purchase of cell-site sim-
24 ulators for State and local law enforcement agencies,

1 including which Federal grants are used for such
2 purpose;

3 (3) a list of each Federal agency that makes
4 cell-site simulators available for use by State or local
5 law enforcement agencies, information about any
6 agreements or procedures governing that sharing,
7 and information about how frequently such sharing
8 occurs;

9 (4) whether any Federal, State, or local law en-
10 forcement agencies are using cell-site simulators to
11 obtain the contents of communications, deliver
12 malware to phones, or for purposes other than locat-
13 ing a particular cellular device;

14 (5) whether and the extent to which any Fed-
15 eral, State, or local law enforcement agencies are
16 using cell-site simulators for enforcement of civil im-
17 migration law;

18 (6) an explanation of the methods used by Fed-
19 eral, State, or local law enforcement agencies to de-
20 ploy cell-site simulators, including whether such de-
21 vices are attached to planes or other aerial devices;

22 (7) an explanation of the approval process that
23 Federal, State, and local law enforcement agencies
24 require prior to use of cell-site simulators, whether
25 these agencies obtain judicial approval prior to de-

1 ployment of cell-site simulators, and if so, what type
2 and with what frequency;

3 (8) an evaluation of whether Federal, State, or
4 local law enforcement agencies have adequate train-
5 ing and auditing mechanisms in place regarding the
6 use of cell-site simulators, and whether these agen-
7 cies have policies or procedures governing the dele-
8 tion of information collected by cell-site simulators;

9 (9) the number of State and local law enforce-
10 ment agencies that are subject to nondisclosure
11 agreements or other orders limiting disclosure of in-
12 formation regarding the use of cell-site simulators;
13 and

14 (10) the extent to which Federal, State, or local
15 law enforcement use of cell cite simulators has a dis-
16 proportionate impact on particular communities, and
17 disparately impacts particular racial, ethnic, or other
18 disadvantaged communities.

19 **SEC. 9. RULE OF CONSTRUCTION.**

20 Nothing in this Act, or an amendment made by this
21 Act, shall be construed to preclude the acquisition by the
22 United States Government of—

23 (1) the contents of a wire or electronic commu-
24 nication pursuant to other lawful authorities, includ-
25 ing the authorities under chapter 119 of title 18,

1 United States Code, the Foreign Intelligence Sur-
2 veillance Act of 1978 (50 U.S.C. 1801 et seq.), or
3 any other provision of Federal law not specifically
4 amended by this Act; or

5 (2) geolocation information, records or other in-
6 formation relating to a subscriber or customer of
7 any electronic communication service or remote com-
8 puting service (not including the content of such
9 communications) pursuant to chapter 119 of title
10 18, United States Code, the Foreign Intelligence
11 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.),
12 or any other provision of Federal law not specifically
13 amended by this Act.

○