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

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

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”.

115TH CONGRESS
1ST Session

S.
SEC. 2. WARRANT FOR STORED CONTENT AND GEOLOCATION INFORMATION.

(a) VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS.—Section 2702 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

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

(ii) by striking “while in electronic storage by that service” and inserting “that is in electronic storage with or otherwise stored, held, or maintained by that service”;

(B) in paragraph (2), in the matter preceding subparagraph (A)—

(i) by striking “to the public”; 

(ii) by striking “divulge” and inserting “disclose”; and 

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

(C) in paragraph (3)—

(i) by striking “a provider of” and inserting “a person or entity providing”;
(ii) by inserting “, or a geolocation service,” after “public”;

(iii) by striking “divulge” and inserting “disclose the contents of any communication described in section 2703(a)”;

(iv) by striking “a record” and inserting “, any records, geolocation information,”; and

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

(2) in subsection (b)—

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

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

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

(B) by striking paragraph (1) and inserting the following:

“(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds,
or maintains such communication, or to an agent of
such addressee, intended recipient, subscriber, or
customer;”; and

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

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

(3) in subsection (c)—

(A) in the matter preceding paragraph

(1)—

   (i) by striking “divulge” and inserting

   “disclose”;

   (ii) by inserting “, geolocation infor-

   mation,” after “record”; and

   (iii) by inserting “wire or electronic”

   before “communications”;

   (B) in paragraph (2)—

   (i) by striking “customer” and insert-

   ing “subscriber”; and

   (ii) by striking “or subscriber” and

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

(D) in paragraph (6), by striking the period at the end and inserting “; or”; and

(E) by adding at the end the following:

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

(b) REQUIRED DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS.—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in the first sentence—

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

(ii) by striking “in an electronic communications system for one hundred and eighty days or less, only pursuant to” and inserting “with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains”;

(iii) by inserting “directing disclosure” before the period at the end; and
(B) by striking the second sentence;

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

“(b) Notice.—Except as provided in section 2705, not later than 10 business days after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service or remote computing service, the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as may be specified by the court issuing the warrant, the subscriber or customer—

“(1) a copy of the warrant or emergency request; and

“(2) a notice that includes the information referred to in clauses (i) and (ii) of section 2705(a)(4)(B).”;
(II) by inserting “, geolocation information service,” after “communication service”; 

(III) by striking “to or” and inserting “or”; 

(IV) by striking “of such service” and inserting “of the provider or service”; 

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

(VI) by striking “when” and inserting “if”; 

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

(iii) in subparagraph (B)— 

(I) by striking “for such” and inserting “directing”; and 

(II) by striking “of this section”; 

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

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

(B) in paragraph (2)—

(i) by striking “A provider” and inserting “INFORMATION TO BE DISCLOSED.—A governmental entity may require a provider”;

(ii) by inserting “, geolocation information service,” after “communication service”; 

(iii) by striking “shall disclose to a governmental entity” and inserting “to disclose, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means authorized under paragraph (1)”; and

(iv) in the matter following subparagraph (F)—

(I) by striking “such” and inserting “the provider or”; and

(II) by striking “when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any
means available under paragraph (1)”; and

(C) in paragraph (3)—

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

(ii) by striking “receiving” and inserting “that receives”;

(4) in subsection (f)(1)—

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

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

(C) by inserting “, geolocation information,” after “records”;

(5) in subsection (g)—

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

(B) by inserting “, geolocation information,” after “of communications”; and

(6) by adding at the end the following:

“(h) GEOLOCATION INFORMATION.—

“(1) IN GENERAL.—A governmental entity may require a provider of electronic communication serv-

ice, geolocation information service, or remote com-
puting service, to disclose stored geolocation information only pursuant to a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures), issued by a court of competent jurisdiction.

“(2) NOTICE.—Except as provided in section 2705, not later than 10 business days after a governmental entity acquires stored geolocation information, the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as may be specified by the court issuing the warrant, the subscriber or customer—

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

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

“(i) RULE OF CONSTRUCTION RELATED TO LEGAL PROCESS.—Nothing in this section or in section 2702 shall limit an otherwise lawful authority of a governmental entity to use an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or a warrant issued using the procedures
described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction to—

“(1) require an originator, addressee, or intended recipient of a wire or electronic communication to disclose a wire or electronic communication (including the contents of that communication) to the governmental entity;

“(2) require a person or entity that provides an electronic communication service to the officers, directors, employees, or agents of the person or entity (for the purpose of carrying out their duties) to disclose wire or electronic communication (including the contents of that communication) to or from the person or entity itself or to or from an officer, director, employee, or agent of the entity to a governmental entity, if the wire or electronic communication is stored, held, or maintained on an electronic communications system owned, operated, or controlled by the person or entity; or

“(3) require a person or entity that provides a remote computing service or electronic communication service to disclose a wire or electronic communication (including the contents of that communication) that advertises or promotes a product or serv-
ice and that has been made readily accessible to the
general public.”.

(c) Cost Reimbursement.—Section 2706(a) of title
18, United States Code, is amended by inserting “
geolocation information,” after “records,”.

SEC. 3. PARTICULARITY REQUIREMENT FOR STORED ELECTRONIC RECORDS.

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

(1) by redesignating—

(A) the first and second sentences as paragraph (1) and adjusting the margins accordingly; and

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

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

(A) in the first sentence—

(i) by striking “(b) or”; and

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

(B) by inserting “The court order shall de-
scribe with particularity the records or other in-
formation to be seized by specifying, as appro-
 priate and reasonable in light of the specific cir-
cumstances of the investigation, the time peri-
ods covered, the target individuals or accounts, the applications or services covered, and the types of information sought.” after “investigation.”;

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

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

”

(B) “the information” and inserting “(A) the information”;

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

(D) by striking “or compliance” and inserting “(B) compliance”.

SEC. 4. NOTICE OF LAWFULLY OBTAINED INFORMATION.

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

(1) in subsection (a)—

(A) by striking paragraph (1) and inserting the following:

“(1) IN GENERAL.—A governmental entity that is seeking a warrant under subsection (a) or (h) of section 2703 may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 90 days.”;
(B) in paragraph (2), in the matter preceding subparagraph (A), by striking “An adverse result for the purposes of paragraph (1) of this subsection is” and inserting “DETERMINATION.—A court shall grant a request for delayed notification made under paragraph (1) if the court determines that there is reason to believe, based on specific and articulable facts, that notification of the existence of the warrant will result in”;

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

“(3) EXTENSION.—Upon request by a governmental entity, a court may grant 1 or more extensions of the delay of notification granted under paragraph (2) of not more than 90 days.”;

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

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

(i) in the matter preceding subparagraph (A)—

(I) by striking “Upon” and inserting “EXPIRATION OF THE DELAY OF NOTIFICATION.—Upon”;


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

(III) by inserting “to” after “deliver”; and

(IV) by striking “to,” and inserting “, electronic mail, or other means reasonably calculated to be effective as specified by the court approving the search warrant,”;

(ii) by striking subparagraph (A);

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

“(A) a copy of the warrant; and”; and

(iv) in subparagraph (B)—

(I) in the matter preceding clause (i)—

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

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

(II) by redesignating—
(aa) clauses (ii) through (iv)
as clauses (iv) through (vi), re-
spectively; and

(bb) clause (i) as clause (ii);

(III) by adding before clause (ii),
as redesignated, the following:

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

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

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

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

(VI) in clause (v), as redesign-
nated, by striking “what governmental
entity or court made the certification
or determination pursuant to which
that delay was made” and inserting
“the identity of the court authorizing
the delay”; and

(VII) in clause (vi), as redesig-
nated, by striking “which provision of
this chapter allowed such delay” and
inserting “of the provision of this
chapter under which the delay was au-
thorized”; and

(F) by striking paragraph (6); and

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

“(b) PrECUSION OF NOTICE TO SUBJECT OF Gov-
ernmental Access.—

“(1) In general.—A governmental entity that
is obtaining the contents of a communication or in-
formation or records under section 2703 may apply
to a court for an order directing a provider of elec-
tronic communication service, geolocation service, or
remote computing service to which a warrant, order,
subpoena, or other directive under section 2703 is
directed not to notify any other person of the exist-
ence of the warrant, order, subpoena, or other direc-
tive for a period of not more than 90 days.
“(2) Determination.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe, based on specific and articulable facts, that notification of the existence of the warrant, order, subpoena, or other directive will result in—

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

“(B) flight from prosecution;

“(C) destruction of or tampering with evidence;

“(D) intimidation of potential witnesses; or

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

“(3) Extension.—Upon request by a governmental entity, a court may grant 1 or more extensions of an order granted under paragraph (2) of not more than 90 days.

“(4) Notification of changed circumstances.—Upon conclusion of the investigation for which a warrant, order, subpoena, or other directive under section 2703 was sought, or if the need for the nondisclosure order under subparagraph (2) ceases to exist, the governmental entity that requested the nondisclosure order shall, within a rea-
sonable period of time, notify the court of the changed circumstances so that the nondisclosure order can be reassessed or vacated.

“(5) Exception.—A provider of electronic communication service or remote computing service to which an order under subsection (b)(2) applies, or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

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

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

“(C) upon an application by a provider, any person the court determines can be notified of the request without causing the adverse result in subparagraph (2) that serves as the basis for the issuance of the nondisclosure order.

“(6) Scope of Nondisclosure Order.—Any person to whom disclosure is made under paragraph (5) shall be subject to the nondisclosure requirements applicable to the person to whom the order is issued under subparagraph (2) in the same manner as the person to whom the request is issued. Any re-
recipient that discloses to a person information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.”.

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

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

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

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

(3) by adding at the end the following:

“(5) the term ‘electronic communications device’ means any device that enables access to or use of an electronic communications system, electronic communication service, remote computing service, or geolocation information service;

“(6) the term ‘geolocation information’—

“(A) means any information concerning the past or current location of an electronic communications device that is in whole or in part generated by or derived from the operation
or use of the electronic communications device; and

“(B) does not include—

“(i) information described in section 2703(e)(2); or

“(ii) the contents of a communication;

and

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

(b) Location Tracking of Electronic Communications Device.—

(1) In general.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

“SEC. 2713. LOCATION TRACKING OF ELECTRONIC COMMUNICATIONS DEVICE.

“(a) Prohibition.—Except as provided in subsection (b), (c), or (d), or section 2702 or 2703, no governmental entity may access or use an electronic communications device to acquire geolocation information.

“(b) Acquisition Pursuant to a Warrant or Court Order.—A governmental entity may access or use an electronic communications device to acquire geolocation information if the governmental entity obtains—
“(1) a warrant issued and executed in accordance with provisions relating to tracking devices in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures), issued by a court of competent jurisdiction authorizing the access or use of an electronic communications device to acquire geolocation information; or

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

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

“(1) as permitted under section 222(d)(4) of the Communications Act of 1934 (47 U.S.C. 222(d)(4)) in order to respond to a call for emergency services by a user of an electronic communications device;
“(2) with the lawful consent of the owner or authorized user of the electronic communications device concerned; or

“(3) if the owner or user of the electronic communications device concerned has knowingly communicated geolocation information in a manner that is readily accessible to the general public.

“(d) Emergency Acquisition of Geolocation Information.—

“(1) In general.—Subject to paragraph (2), an investigative or law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, any United States attorney, any acting United States attorney, or the principal prosecuting attorney of any State or political subdivision thereof acting pursuant to a statute of that State may access or use an electronic communications device to acquire geolocation information if the investigative or law enforcement officer reasonably determines that—

“(A) an emergency situation exists that—

“(i) involves—
“(I) immediate danger of death
or serious bodily injury to any person;
or
“(II) an immediate threat to na-
tional security; and
“(ii) requires the access or use of an
electronic communications device to ac-
quire geolocation information before an
order authorizing the acquisition may, with
due diligence, be obtained; and
“(B) in circumstances in which geolocation
information may be used as evidence of a crime
or in furtherance of a criminal investigation,
there are grounds upon which an order could be
entered under this section to authorize the ac-
cessing or use of an electronic communications
device to acquire geolocation information.
“(2) NOTICE, ORDER AND TERMINATION.—If
an investigative or law enforcement officer accesses
or uses an electronic communications device to ac-
quire geolocation information under paragraph (1)—
“(A) the officer shall, not later than 10
business days after acquiring geolocation infor-
mation, serve upon, or deliver to by registered
or first-class mail, electronic mail, or other
means reasonably calculated to be effective, no-
tice to the owner or authorized user of the elec-
tronic communications device whose geolocation
information was acquired that such information
was obtained or accessed pursuant to the emer-
gency provisions under this subsection and de-
scribing the factual bases that led to the offi-
cer’s determination that an emergency situation
existed;

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

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

“(i) the information sought is ob-
tained;
“(ii) the application for the warrant or order is denied; or

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

“(3) VIOLATION AND SUPPRESSION OF EVIDENCE.—

“(A) IN GENERAL.—In a circumstance described in subparagraph (B)—

“(i) no information obtained, or evidence derived, from geolocation information acquired as part of the access or use of an electronic communications device to acquire geolocation information may be received into evidence or otherwise disclosed 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;

“(ii) no information concerning any person acquired from the geolocation information may be used, disseminated, or dis-
closed in any other manner, without the
consent of the person; and

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

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

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

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

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

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

“(e) ASSISTANCE AND COMPENSATION.—

“(1) IN GENERAL.—A warrant described in
subsection (b)(1) authorizing the accessing or use of
an electronic communications device to acquire
geolocation information shall, upon request of the applicant, direct that a provider of electronic communication service, remote computing service, or geolocation information service shall provide to the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with the services that the provider is providing to or through the electronic communications device in question.

“(2) Compensation.—Any provider of electronic communication service, remote computing service, or geolocation information service providing information, facilities, or technical assistance under a directive under paragraph (1) shall be compensated by the applicant for reasonable expenses incurred in providing the information, facilities, or assistance.

“(f) No Cause of Action Against a Provider.—No cause of action shall lie in any court against any provider of electronic communication service, remote computing service, or geolocation information service, or an officer, employee, or agent of the provider or other specified person for providing information, facilities, or assist-
ance necessary to accomplish an acquisition of geolocation
information authorized under this section.”.

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

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

SEC. 6. SUPPRESSION OF UNLAWFULLY OBTAINED WIRE OR
ELECTRONIC COMMUNICATION OR
GEOLOCATION INFORMATION.

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

“§ 2714. Suppression remedy

“(a) IN GENERAL.—If a governmental entity requires
the disclosure of a wire or electronic communication or
geolocation information in violation of this chapter, or ac-
cesses or uses an electronic communications device to ac-
quire geolocation information in violation of this chapter,
no part of the contents of the communication, no
geolocation information, and no evidence derived there-
from may be received in evidence in any trial, hearing,
or other proceeding in or before any court, grand jury,
department, officer, agency, regulatory body, legislative
committee, or other authority of the United States, a
State, or a political subdivision thereof.
“(b) GROUNDS.—An aggrieved person in a trial, hearing, or proceeding in or before a court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof may move to suppress the contents of any wire or electronic communication or geolocation information disclosed or acquired under this chapter, or evidence derived therefrom, on the grounds that—

“(1) the communication or information was unlawfully disclosed;

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

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

“(c) PROCEDURE.—

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

“(2) INSPECTION.—The judge or other official, upon the filing of a motion under subsection (b), may make available to the aggrieved person or the attorney for the aggrieved person for inspection such portions of the disclosed communication, geolocation
information, or evidence derived therefrom as the judge or other official determines to be in the interests of justice.

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

“(d) APPEAL.—In addition to any other right to appeal, the United States shall have the right to appeal an order granting a motion to suppress made under subsection (b) if the United States attorney certifies to the judge or other official granting such motion that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered and shall be diligently prosecuted.

“(e) DEFINITION.—In this section, the term ‘aggrieved person’ means—

“(1) a person whose wire or electronic communication or geolocation information was disclosed pursuant to this chapter; or

“(2) the owner or authorized user of the electronic communications device whose geolocation information was acquired pursuant to this chapter.”.
(b) Technical and Conforming Amendment.—The table of sections for chapter 121 of title 18, United States Code, as amended by section 5(b), is amended by adding at the end the following:

“2714. Suppression remedy.”.

SEC. 7. Pen Register and Trap and Trace Reforms.

(a) Application for an Order for a Pen Register or a Trap and Trace Device.—Section 3122(b)(2) of title 18, United States Code, is amended—

(1) by striking “a certification by the applicant” and inserting “specific and articulable facts showing that there are reasonable grounds to believe”; and

(2) by inserting “and material” after “relevant”.

(b) Issuance of an Order for a Pen Register or a Trap and Trace Device.—Section 3123 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

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

(ii) by inserting “and material” after “relevant”; and
(B) in paragraph (2)—

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

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

(2) in subsection (d)—

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

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

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

(a) FCC Report.—Not later than 1 year after the date of enactment, the Federal Communications Commission shall submit to the Committee on the Judiciary of the Senate and Committee on the Judiciary of the House of Representatives a report regarding the domestic use of cell-site simulators (or “IMSI catchers”) by Federal, State, and local law enforcement agencies, which shall include—

(1) an evaluation of the security vulnerabilities in cellular phones and cellular networks exploited by
cell-site simulators, and the extent to which those
vulnerabilities could be or have been exploited by
criminals or foreign governments; and

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

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

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

(2) the extent to which the Federal Government
is providing or funding the purchase of cell-site sim-
ulators for State and local law enforcement agencies,
including which Federal grants are used for such purpose;

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

(4) whether any Federal, State, or local law enforcement agencies are using cell-site simulators to obtain the contents of communications, deliver malware to phones, or for purposes other than locating a particular cellular device;

(5) whether and the extent to which any Federal, State, or local law enforcement agencies are using cell-site simulators for enforcement of civil immigration law;

(6) an explanation of the methods used by Federal, State, or local law enforcement agencies to deploy cell-site simulators, including whether such devices are attached to planes or other aerial devices;

(7) an explanation of the approval process that Federal, State, and local law enforcement agencies require prior to use of cell-site simulators, whether these agencies obtain judicial approval prior to de-
ployment of cell-site simulators, and if so, what type
and with what frequency;

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

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

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

SEC. 9. RULE OF CONSTRUCTION.

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

(1) the contents of a wire or electronic commu-
nication pursuant to other lawful authorities, includ-
ing the authorities under chapter 119 of title 18,
United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act; or

(2) geolocation information, records or other information relating to a subscriber or customer of any electronic communication service or remote computing service (not including the content of such communications) pursuant to chapter 119 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act.