

[Congress](#) / [Bills](#) / [S. 1212 \(112th\)](#) / Text

S. 1212 (112th): Geolocational Privacy and Surveillance Act

[Overview](#) [Summary](#) [Details](#) **Text**

The text of the bill below is as of **Jun 15, 2011** (Introduced).

[Download PDF](#)112TH CONGRESS1ST SESSION**S. 1212**

IN THE SENATE OF THE UNITED STATES

June 15, 2011

Mr. Wyden 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 specify the circumstances in which a person may acquire geolocation information and for other purposes.

Section 1. Short titles

This Act may be cited as the “Geolocational Privacy and Surveillance Act” or the “GPS Act”.

Compare this bill to another bill:

(Select Bill)

React with an emoji

...

Save your opinion

 [Add Note](#) [All Positions »](#)

Primary Source

[Government Publishing Office](#)

Widget for your website

[Get a bill status widget »](#)

Follow GovTrack on social media for more updates:

On GovTrack Insider:

[Energy Innovation and Carbon Dividend Act would create carbon tax to fight climate change—and a...](#)

Should America institute a tax on the main pollutant contributing to global warming? Dec 14, 2018

[PreCheck is PreCheck Act would ban TSA from putting people in expedited security lines if they...](#)

Should the TSA be able to shift people into the PreCheck security line as a way of managing traffic flow at the airport? Dec 13, 2018

[Preserving America's Battlefields Act would double funding to protect historic battlefields](#)

How much should we pay to fund the preservation of Civil War and Revolutionary War battlefields Dec 12, 2018

Sec. 2. Protection of geolocation information

(a) In general.—

Part 1 of title 18, United States Code, is amended by inserting after chapter 119 the following:

Chapter 120

Geolocation information

Sec.

2601. Definitions.

2602. Interception and disclosure of geolocation information.

2603. Prohibition of use as evidence of acquired geolocation information.

2604. Emergency situation exception.

2605. Recovery of civil damages authorized.

Sec. 2601. Definitions

In this chapter:

(1) Covered service.—

The term “covered service” means an electronic communication service, a geolocation information service, or a remote computing service.

(2) Electronic communication service.—

The term “electronic communication service” has the meaning given that term in section 2510.

(3) Electronic surveillance.—

The term “electronic surveillance” has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(4) Geolocation information.—

The term “geolocation information” means, with respect to a person, any information, that is not the content of a communication, concerning the location

of a wireless communication device or tracking device (as that term is defined section 3117) that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person.

(5) Geolocation information service.—

The term “geolocation information service” means the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device.

(6) Intercept.—

The term “intercept” means the acquisition of geolocation information through the use of any electronic, mechanical, or other device.

(7) Investigative or law enforcement officer.—

The term “investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

(8) Person.—

The term “person” means any employee or agent of the United States, or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

(9) Remote computing service.—

The term “remote computing service” has the meaning given that term in section 2711.

(10) State.—

The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(11) Wireless communication device.—

The term “wireless communication device” means any device that enables access to, or use of, an electronic communication system or service or a covered service, if that device utilizes a radio or other wireless connection to access such system or service.

Sec. 2602. Interception and disclosure of geolocation information

(a) In general.—

(1) Prohibition on disclosure or use.—

Except as otherwise specifically provided in this chapter, it shall be unlawful for any person to—

- (A) intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, geolocation information pertaining to another person;
- (B) intentionally disclose, or endeavor to disclose, to any other person geolocation information pertaining to another person, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph;
- (C) intentionally use, or endeavor to use, any geolocation information, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph; or
- (D)
 - (i) intentionally disclose, or endeavor to disclose, to any other person the geolocation information pertaining to

another person intercepted by means authorized by subsections (b) through (h), except as provided in such subsections;

(ii) knowing or having reason to know that the information was obtained through the interception of such information in connection with a criminal investigation;

(iii) having obtained or received the information in connection with a criminal investigation; and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

(2) Penalty.—

Any person who violates paragraph (1) shall be fined under this title, imprisoned not more than five years, or both.

(b) Exception for information acquired in the normal course of business.—

It shall not be unlawful under this chapter for an officer, employee, or agent of a provider of a covered service, whose facilities are used in the transmission of geolocation information, to intercept, disclose, or use that information in the normal course of the officer, employee, or agent's employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of a geolocation information service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(c) Exception for conducting foreign intelligence surveillance.—

Notwithstanding any other provision of this chapter, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of the

official duty of the officer, employee, or agent to conduct electronic surveillance, as authorized by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(d) Exception for consent.—

(1) In general.—

It shall not be unlawful under this chapter for a person to intercept geolocation information pertaining to another person if such other person has given prior consent to such interception unless such information is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(2) Children.—

The exception in paragraph (1) permits a parent or legal guardian of a child to intercept geolocation information pertaining to that child or to give consent for another person to intercept such information.

(e) Exception for public information.—

It shall not be unlawful under this chapter for any person to intercept or access geolocation information relating to another person through any system that is configured so that such information is readily accessible to the general public.

(f) Exception for emergency information.—

It shall not be unlawful under this chapter for any investigative or law enforcement officer or other emergency responder to intercept or access geolocation information relating to a person if such information is used—

(1) to respond to a request made by such person for assistance; or

(2) in circumstances in which it is reasonable to believe that the life or safety of the person is threatened, to assist the person.

(g) Exception for theft or fraud.—

It shall not be unlawful under this chapter for a person acting under color of law to intercept geolocation information pertaining to the location of another person who has unlawfully taken the device sending the geolocation information if—

- (1) the owner or operator of such device authorizes the interception of the person's geolocation information;
- (2) the person acting under color of law is lawfully engaged in an investigation; and
- (3) the person acting under color of law has reasonable grounds to believe that the geolocation information of the other person will be relevant to the investigation.

(h) Exception for warrant.—

(1) Definitions.—

In this subsection:

(A) Court of competent jurisdiction.—

The term “court of competent jurisdiction” includes—

- (i) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—
 - (I) has jurisdiction over the offense being investigated;
 - (II) is in or for a district in which the provider of a geolocation information service is located or in which the geolocation information is stored; or
 - (III) is acting on a request for foreign assistance pursuant to section 3512; or

(ii) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.

(B) Governmental entity.—

The term “governmental entity” means a department or agency of the United States or any State or political subdivision thereof.

(2) Warrant.—

A governmental entity may intercept geolocation information or require the disclosure by a provider of a covered service of geolocation information only pursuant to 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, or as otherwise provided in this chapter or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(i) Prohibition on divulging geolocation information.—

(1) In general.—

Except as provided in paragraph (2), a person providing a covered service shall not intentionally divulge geolocation information pertaining to another person.

(2) Exceptions.—

A person providing a covered service may divulge geolocation information—

(A) as otherwise authorized in subsections (b) through (h);

(B) with the lawful consent of such other person;

(C) to another person employed or authorized, or whose facilities are used, to forward such geolocation information to its destination; or

- (D) which was inadvertently obtained by the provider of the covered service and which appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

Sec. 2603. Prohibition of use as evidence of acquired geolocation information

Whenever any geolocation information has been acquired, no part of such information and no evidence derived therefrom 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 if the disclosure of that information would be in violation of this chapter.

Sec. 2604. Emergency situation exception

(a) Emergency situation exception.—

Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, may intercept geolocation information if—

(1) such officer reasonably determines that an emergency situation exists that—

(A) involves—

- (i) immediate danger of death or serious physical injury to any person;
- (ii) conspiratorial activities threatening the national security interest; or
- (iii) conspiratorial activities characteristic of organized crime; and

(B) requires geolocation information be

intercepted before an order authorizing such interception can, with due diligence, be obtained;

- (2) there are grounds upon which an order could be entered to authorize such interception; and
- (3) an application for an order approving such interception is made within 48 hours after the interception has occurred or begins to occur.

(b) Failure To obtain court order.—

(1) Termination of acquisition.—

In the absence of an order, an interception of geolocation information carried out under subsection (a) shall immediately terminate when the information sought is obtained or when the application for the order is denied, whichever is earlier.

(2) Prohibition on use as evidence.—

In the event such application for approval is denied, the geolocation information shall be treated as having been obtained in violation of this chapter and an inventory shall be served on the person named in the application.

Sec. 2605. Recovery of civil damages authorized

(a) In general.—

Any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.—

In an action under this section, appropriate relief includes—

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.—

The court may assess as damages under this section whichever is the greater of—

(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(2) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

(d) Defense.—

It is a complete defense against any civil or criminal action brought against an individual for conduct in violation of this chapter if such individual acted in a good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2604; or

(3) a good-faith determination that an exception under section 2602 permitted the conduct complained of.

(e) Limitation.—

A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative discipline.—

If a court or appropriate department or agency

determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, such head shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper disclosure is violation.—

Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by this chapter is a violation of this chapter for purposes of this section.

(b) Clerical amendment.—

The table of chapters for part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 119 the following:

*120. Geolocation information*²⁶⁰¹

(c) Conforming amendments.—

Section 3512(a) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

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

(B) a warrant or order for geolocation information or records related thereto, as provided under section 2602 of this title;

Sec. 3. Requirement for search warrants to acquire geolocation information

Rule 41(a) of the Federal Rules of Criminal Procedure is amended—

(1) in paragraph (2)(A), by striking the period at the end and inserting a comma and “including geolocation information.”; and

(2) by adding at the end the following:

(F) “Geolocation information” has the meaning given that term in section 2601 of title 18, United States Code.

Sec. 4. Fraud and related activity in connection with obtaining geolocation information

(a) Criminal violation.—

Section 1039(h) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by striking “and” at the end;

(B) in subparagraph (B), by striking the period at the end and inserting a semicolon and “and”; and

(C) by adding at the end the following new subparagraph:

(C) includes any geolocation information service.

;

(2) by redesignating paragraph (4) as paragraph (5); and

(3) by inserting after paragraph (3) the following:

(4) Geolocation information service.—

The term “geolocation information service” has the meaning given that term in section 2601.

(b) Conforming amendments.—

(1) Definition amendments.—

Section 1039(h)(1) of title 18, United States Code, is amended—

(A) in the paragraph heading, by inserting “or GPS” after “phone”; and

(B) in the matter preceding subparagraph (A), by inserting “or GPS” after “phone”.

(2) Conforming amendments.—

Section 1039 of title 18, United States Code, is amended—

(A) in the section heading by inserting “or GPS” after “phone”;

(B) in subsection (a)—

(i) in the matter preceding paragraph (1), by inserting “or GPS” after “phone”; and

(ii) in paragraph (4), by inserting “or GPS” after “phone”;

(C) in subsection (b)—

(i) in the subsection heading, by inserting “or GPS”

after “phone”;

(ii) in paragraph (1), by inserting “or GPS” after “phone” both places that term appears; and

(iii) in paragraph (2), by inserting “or GPS” after “phone”; and

(D) in subsection (c)—

(i) in the subsection heading, by inserting “or GPS” after “phone”;

(ii) in paragraph (1), by inserting “or GPS” after “phone” both places that term appears; and

(iii) in paragraph (2), by inserting “or GPS” after “phone”.

(3) Chapter analysis.—

The table of sections for chapter 47 of title 18, United States Code, is amended by striking the item relating to section 1039 and inserting the following:

1039. Fraud and related activity in connection with obtaining confidential phone or GPS records information of a covered entity.

(c) Sentencing guidelines.—

(1) Review and Amendment.—

Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section 1039 of title 18, United States Code, as amended by this section.

(2) Authorization.—

The United States Sentencing Commission may amend

the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that section had not expired.

Sec. 5. Statement of exclusive means of acquiring geolocation information

(a) In general.—

No person may acquire the geolocation information of a person for protective activities or law enforcement or intelligence purposes except pursuant to a warrant issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, as amended by section 3, or the amendments made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) Geolocation information defined.—

In this section, the term “geolocation information” has the meaning given that term in section 2601 of title 18, United States Code, as amended by section 2.

site MENU

[Home](#)

[Start Tracking](#)

[About GovTrack](#)

[About the Data](#)

[Privacy & Legal](#)

[Log in](#)

follow

GOVTRACK

[Facebook](#)

[Twitter](#)

[Medium](#)

[Patreon](#)

[Blog](#)

[Code](#)

Launched in 2004, GovTrack helps everyone learn about and track the activities of the United States Congress. This is a project of [Civic Impulse, LLC](#). GovTrack.us is not a government website.

[About the Site](#) | [Contact Us](#)

You are encouraged to reuse any material on this site. Hackers/journalists/researchers: See these [open data sources](#).