

A BILL TO BE ENTITLED
AN ACT

To enact "The Interception and Disclosure of Geolocation Information Protection Act of 2011"; to amend Article 3 of Chapter 11 of Title 16 of the Official Code of Georgia Annotated, relating to invasions of privacy, so as to specify the circumstances in which a person may acquire geolocation information; to provide for definitions; to provide for the exclusion of evidence obtained in violation of limitations on the acquisition of geolocation information; to provide for civil and criminal penalties; to provide for related matters; to provide for an effective date and applicability; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

This Act shall be known and may be cited as "The Interception and Disclosure of Geolocation Information Protection Act of 2011."

SECTION 2.

Article 3 of Chapter 11 of Title 16 of the Official Code of Georgia Annotated, relating to invasions of privacy, is amended by adding a new part to read as follows:

"Part 3

16-11-90.

As used in this part, the term:

(1) 'Covered services' means electronic communication service, remote computing service, or a geolocation information service.

(2) 'Electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce, but does not include:

25 (A) Any wire or oral communication;

26 (B) Any communication made through a tone-only paging device;

27 (C) Any communication from a tracking device; or

28 (D) Electronic funds transfer information stored by a financial institution in a
29 communications system used for the electronic storage and transfer of funds.

30 (3) 'Electronic communication service' means any service which provides to users of
31 such service the ability to send or receive wire or electronic communications.

32 (4) 'Electronic surveillance' means:

33 (A) The acquisition by any electronic, mechanical, or other surveillance device of the
34 contents of any wire or radio communication sent by or intended to be received by a
35 particular, known person who is in this state, if the contents are acquired by
36 intentionally targeting that person, under circumstances in which a person has a
37 reasonable expectation of privacy and a warrant would be required for law enforcement
38 purposes;

39 (B) The acquisition by any electronic, mechanical, or other surveillance device of the
40 contents of any wire communication to or from a person in this state, without the
41 consent of any party thereto, if such acquisition occurs in this state, but does not include
42 the acquisition of those communications of computer trespassers that are otherwise
43 authorized by law;

44 (C) The intentional acquisition by any electronic, mechanical, or other surveillance
45 device of the contents of any radio communication, under circumstances in which a
46 person has a reasonable expectation of privacy and a warrant would be required for law
47 enforcement purposes, and if both the sender and all intended recipients are located
48 within this state; or

49 (D) The installation or use of any electronic, mechanical, or other surveillance device
50 in this state for monitoring to acquire information, other than from a wire or radio
51 communication, under circumstances in which a person has a reasonable expectation
52 of privacy and a warrant would be required for law enforcement purposes.

53 (5) 'Geolocation information' means, with respect to a person, any information that is not
54 the content of a communication, concerning the location of a wireless communication
55 device or tracking device that, in whole or in part, is generated by or derived from the
56 operation of that device and that could be used to determine or infer information
57 regarding the location of the person.

58 (6) 'Geolocation information service' means the provision of a global positioning service
59 or other mapping, locational, or directional information service to the public, or to such
60 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.

(7) 'Intercept' means the acquisition of geolocation information through the use of any electronic, mechanical, or other device.

(8) 'Investigative or law enforcement officer' means any officer of the United States or of this state or a political subdivision thereof who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in this part, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

(9) 'Person' means any employee or agent of the United States, or of this state or a political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

(10) 'Remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.

(11) 'Tracking device' means any electronic or mechanical device which permits the tracking of the movement of a person or object.

(12) 'Wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

(13) 'Wireless communication device' means any device that enables access to, or use of, any electronic communication system or service, remote computing service, or geolocation information service, if that device utilizes a radio or other wireless connection to access such system or service.

16-11-91.

(a) **Unlawful acts.** Except as otherwise provided in this part, it shall be unlawful for any person to:

(1) Intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, geolocation information pertaining to another person;

(2) 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;

(3) 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

(4) Intentionally disclose, or endeavor to disclose, to any other person the geolocation information pertaining to another person intercepted by means authorized by this Code section as provided in this Code section, while knowing or having reason to know that the information was obtained through the interception of such information in connection with a criminal investigation and with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

(b) Punishment. Any person who violates subsection (a) of this Code section shall be guilty of a felony and, upon conviction thereof, shall be punished by imprisonment for not less than one nor more than five years or a fine not to exceed \$10,000.00, or both.

(c) Exception for information acquired in the normal course of business. It shall not be unlawful under this Code section for an officer, employee, or agent of a provider of covered services, 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.

(d) Exception for conducting foreign intelligence surveillance. Notwithstanding any other provision of this Part, 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. Section 1801, et seq., as amended or replaced.

(e) Exception for consent.

(1) It shall not be unlawful under this Code section 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 this state.

(2) It shall not be unlawful for a parent or legal guardian of a child, under age 18, to intercept geolocation information pertaining to that child or to give consent for another person to intercept such information.

(f) Exception for public information. It shall not be unlawful under this Code section 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.

(g) **Exception for emergency information.** It shall not be unlawful under this Code section 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 a person is threatened, to assist such threatened person.

(h) **Exception for the investigation of theft or fraud.** It shall not be unlawful under this Code section for a person to intercept geolocation information pertaining to the location of another person who has unlawfully taken the device sending the geolocation information if the owner or operator of such device authorizes the interception of the person's geolocation information and such person is lawfully engaged in an investigation.

(i) **Exception for obtaining information pursuant to a warrant.** This Code section shall not apply to any person obtaining information pursuant to a warrant. A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this Code section.

(j) **Exception for person providing covered services.** A person providing covered services may divulge geolocation information of another person:

(1) With the lawful consent of such other person;

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

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

16-11-92.

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 this state or a political subdivision of this state if the disclosure of that information would be in violation of this part.

16-11-93.

(a) Notwithstanding any other provision of this part, any investigative or law enforcement officer, specially designated by the Attorney General or a prosecuting attorney, may

intercept geolocation information if such officer reasonably determines that an emergency situation exists that involves:

- (1) Immediate danger of death or serious physical injury to any person;
- (2) Conspiratorial activities threatening national or state security interest; or
- (3) Conspiratorial activities characteristic of organized crime; and

requires geolocation information be intercepted before an order authorizing such interception can, with due diligence, be obtained.

(b) An application for an order approving such interception shall be made within 48 hours after the interception has occurred or begins to occur. In the absence of an order, an interception of geolocation information carried out under subsection (a) of this Code section shall immediately terminate when the information sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, the geolocation information shall not be admissible in any civil or criminal proceeding.

16-11-94.

(a) Any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this part is authorized to, in a civil action, recover from the person who engaged in that violation such relief as may be appropriate.

(b) In an action under this Code section, appropriate relief includes:

- (1) Such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) Damages under subsection (c) of this Code section and punitive damages in appropriate cases; and
- (3) Reasonable attorney's fees and other litigation costs reasonably incurred.

(c) The court may assess as damages under this Code 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 \$100.00 a day for each day of violation or \$10,000.00.

(d) It is a complete defense against any civil or criminal action brought against any person for conduct in violation of this part if such person 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; or
- (3) A good-faith determination that an exception under Code Section 16-11-91 permitted the conduct complained of.

201 (e) A civil action under this Code section may not be commenced later than one year after
202 the date upon which the claimant first has a reasonable opportunity to discover the
203 violation."

204 **SECTION 3.**

205 This Act shall become effective on July 1, 2012, and shall apply to offenses and violations
206 committed on or after such date.

207 **SECTION 4.**

208 All laws and parts of laws in conflict with this Act are repealed.