AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

114TH CONGRESS
1ST SESSION

H. R. 656

To amend title 18, United States Code, with respect to disclosures to governments by communications-related service providers of certain information consisting of or relating to communications, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 2, 2015

Ms. LOFGREN (for herself, Mr. POE of Texas, Ms. DELBENE, Mr. SENSENBRENNER, Mr. CONYERS, Mr. FARENTHOLD, Mr. POLIS, Mr. MASSIE, Mr. SWALWELL of California, and Mr. O'ROURKE) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Select Committee on Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend title 18, United States Code, with respect to disclosures to governments by communications-related service providers of certain information consisting of or relating to communications, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Online Communications and Geolocation Protection Act".

SEC. 2. WARRANT REQUIRED FOR CONTENTS OF COMMUNICATIONS.

(a) COMPELLED DISCLOSURE OF COMMUNICATION CONTENTS.—

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

(A) in subsection (a)—

(i) by striking ''IN ELECTRONIC STORAGE'' in the subsection header;

(ii) by inserting ''or remote computing service'' in the first sentence after ''electronic communication service'';

(iii) by striking ''that is in electronic storage in an electronic communications system for one hundred and eighty days or less,'' and inserting ''that is stored, held, or maintained by that service,''; and

(iv) by striking the final sentence and inserting ''Within three days after a governmental entity receives such contents from a service provider pursuant to this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant to the sub-

scriber, customer, or user a copy of the warrant and a notice that includes the information referenced in section 2705(a)(4)(A) and (B)(i), except that delayed notice may be provided pursuant to section 2705 of this title.''; and

(B) by striking subsection (b).

(2) CONFORMING AMENDMENT.—Section 2703(d) of title 18, United States Code, is amended by striking ''(b) or''.

(b) VOLUNTARY DISCLOSURE OF COMMUNICATION CONTENTS.—

(1) IN GENERAL.—Section 2702(a)(3) of title 18, United States Code, is amended—

(A) by inserting ''to any governmental entity the contents of communication covered by subsection (a) of section 2703 or any'' after ''divulge'';

(B) by inserting ''or user'' after ''customer''; and

(C) by striking ''(not including the contents of communications covered by paragraph (1) or (2))''.

(2) CONFORMING AMENDMENTS.—Section 2705 of title 18, United States Code, is amended—

(A) in subsection (a)(1)—

(i) in the subsection heading, by striking ''2703(b)'' and inserting ''2703(a)'';

(ii) in subparagraph (A), by striking ''court order'' each place it appears and inserting ''warrant'';

(iii) in subparagraph (A), by striking ''2703(b)'' and inserting ''2703(a)''; and

(iv) by striking subparagraph (B);

(B) by striking subsection (a)(3);

(C) in subsection (a)(4), by striking ''or by certification by a governmental entity, but only in accordance with subsection (b) of this section.'';

(D) in subsection (a)(5)—

(i) by inserting after ''first-class mail,'' the following: ''or other means reasonably calculated to be effective as specified by the court issuing the warrant'';

(ii) by striking ''the process or request'' and replacing it with ''warrant''; and

(iii) in subsection (5)(A)(iii), by striking ''governmental entity or'' and ''certification or'';

(E) by striking subsection (a)(6); and

(F) in subsection (b)—

(i) by striking ''when it is not required to notify the subscriber or customer under section 2703(b)(1), or''; and

(ii) by striking ''subpoena or court order'' each place it appears.

SEC. 3. GEOLOCATION INFORMATION PROTECTION.

(a) IN GENERAL.—

(1) 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 on disclosing geolocation information to governmental entities.
''2604. Prohibition of use of unlawfully obtained geolocation information as evidence.
''2605. Recovery of civil damages and administrative discipline authorized.

''§ 2601. Definitions

''In this chapter:

''(1) ELECTRONIC COMMUNICATION SERVICE.—The term 'electronic communication service' has the meaning given that term in section 2510.

''(2) 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).

"(3) GEOLOCATION INFORMATION.—The term 'geolocation information' means, with respect to an individual, 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 present, prospective, or historical location of the individual.

"(4) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' means a service that generates or uses geolocation information for the provision of a 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.

"(5) GOVERNMENTAL ENTITY.—The term 'governmental entity' means any employee or agent of the United States, or any State or political subdivision thereof.

"(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) REMOTE COMPUTING SERVICE.—The term 'remote computing service' has the meaning given that term in section 2711.

"(9) 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.

"(10) WIRELESS COMMUNICATION DEVICE.—The term 'wireless communication device' means any device that enables access to, or use of, an electronic communication system or service, remote computing service, or geolocation information service, if that device utilizes a radio signal or other wireless connec-

tion to access or use such system or service, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device.

"(11) COVERED SERVICE.—The term 'covered services' means electronic communication service, remote computing service, or geolocation information service.

"§ 2602. Interception and disclosure of geolocation information

"(a) IN GENERAL.—Except as otherwise provided in this chapter, it shall be unlawful for any governmental entity to—

"(1) intentionally intercept, endeavor to intercept, or direct any person to intercept or endeavor to intercept, geolocation information pertaining to an individual;

"(2) intentionally disclose, or endeavor to disclose, or direct any person to disclose or endeavor to disclose geolocation information pertaining to an individual, knowing or having reason to know that the information was obtained in violation of this subsection; or

"(3) intentionally use, or endeavor to use, any geolocation information, knowing or having reason

to know that the information was obtained in violation of this subsection.

"(b) 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.).

"(c) EXCEPTION FOR CONSENT.—

"(1) IN GENERAL.—It shall not be unlawful under this chapter for a governmental entity to intercept, use, or disclose geolocation information pertaining to an individual if that individual has given prior consent to that governmental entity for such interception, use or disclosure.

"(2) CHILDREN.—A parent or legal guardian of a child may consent on behalf of a child for the purposes of paragraph (1).

"(d) EXCEPTION FOR PUBLIC INFORMATION.—It shall not be unlawful under this chapter for a governmental entity to intercept or access geolocation information pertaining to an individual through any system that

is configured so that such information is readily accessible to the general public.

"(e) EXCEPTION FOR EMERGENCY ASSISTANCE.—It shall not be unlawful under this chapter for any investigative or law enforcement officer or other emergency responder to intercept, access, use, or disclose geolocation information pertaining to an individual if such information is used—

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

"(2) to assist the individual in circumstances in which it is reasonable to believe that the life or safety of the individual is in jeopardy.

"(f) EXCEPTION FOR WARRANT.—

"(1) IN GENERAL.—A governmental entity may intercept geolocation information or require the disclosure of geolocation information by a provider of covered services only pursuant to a warrant issued by a court of competent jurisdiction using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures), or as otherwise provided in this chapter or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(2) COURT OF COMPETENT JURISDICTION.—For the purposes of this subsection, the term 'court of competent jurisdiction' includes—

"(A) 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 of this title; or

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

"(g) EMERGENCY SITUATION EXCEPTION.—

"(1) IN GENERAL.—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 pros-

ecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, may intercept or use geolocation information if—

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

"(i) involves—

"(I) immediate danger of death or serious physical injury to any individual;

"(II) conspiratorial activities threatening the national security interest; or

"(III) conspiratorial activities characteristic of organized crime; and

"(ii) requires geolocation information be intercepted or used before an order authorizing such interception or use can, with due diligence, be obtained;

"(B) there are grounds upon which an order could be entered to authorize such interception or use; and

"(C) an application for an order approving such interception or use is made within 48 hours after the interception or use has occurred or begins to occur.

"(2) FAILURE TO OBTAIN COURT ORDER.—

"(A) TERMINATION OF ACQUISITION.—In the absence of an order, an interception or use of geolocation information carried out under paragraph (1) shall immediately terminate when the information sought is obtained or when the application for the order is denied, whichever is earlier.

"(B) 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 each individual who is reasonably able to be contacted and to whom any such geolocation information pertains.

"§ 2603. Prohibition on disclosing geolocation information to governmental entities

"(a) IN GENERAL.—Except as provided in subsection (b), a person providing covered services shall not intentionally disclose to any governmental entity geolocation information pertaining to an individual.

"(b) EXCEPTIONS.—A person providing covered services may disclose geolocation information—

"(1) as otherwise authorized in subsections (b) through (g) of section 2602;

"(2) with the lawful consent of—

"(A) the individual to whom the geolocation information pertains; or

"(B) the parent or guardian of a child to whom the geolocation information pertains;

"(3) as permitted under section 222(d)(4) of the Communications Act of 1934 (47 U.S.C. 222(d)(4)); or

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

"§ 2604. Prohibition of use of unlawfully obtained geolocation information as evidence

"If any geolocation information has been intercepted, used, or disclosed in violation of this chapter, 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, except in a civil action to obtain relief for a violation of this chapter.

"§ 2605. Recovery of civil damages and administrative discipline authorized

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

''(b) RELIEF.—In an action under this section, appropriate relief includes—

''(1) such preliminary and other equitable or declaratory relief as the court may deem appropriate;

''(2) damages under subsection (c) and punitive damages as the court may deem appropriate; 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; 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 defense against any civil action to obtain relief for a violation of this chapter that the defendant acted in a good faith reliance on—

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

"(2) a reasonable 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 dis-

ciplinary 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.''.

(2) 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''.

(3) CONFORMING AMENDMENTS.—Section 3512(a) of title 18, United States Code, is amended—

(A) in paragraph (2)—

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

(ii) 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;''.

(b) REQUIREMENT FOR SEARCH WARRANTS TO OBTAIN 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.''.

(c) STATEMENT OF EXCLUSIVE MEANS OF OBTAINING GEOLOCATION INFORMATION.—

(1) IN GENERAL.—No person may obtain 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 subsection (b), or the amendments made by this section, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(2) GEOLOCATION INFORMATION DEFINED.—In this subsection, the term ''geolocation information'' has the meaning given that term in section 2601 of

1 title 18, United States Code, as amended by sub-
2 section (a).

○