The Location Observation and Surveillance Technologies Act of 2018

Text of Model Federal Legislation

Charles Bell, GULC • Nathaniel Fruchter, MIT • Sabrina McCubbin, GULC • Olamide Oladeji, MIT

Location Observation and Surveillance Technologies Act of 2018

A Bill

To amend title 18, United States Code, to specify the conditions in which geolocation information may be acquired, 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 "Location Observation and Surveillance Technologies Act" or the "LOST Act".

SECTION 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

§ 2601. Definitions.

In this chapter:

(1) CONSENT.—The term "consent" means any freely given, specific, informed and unambiguous indication after receiving clear, prominent, and accurate notice that—

(A) informs the individual that his or her geolocation information will be collected by the provider of geolocation information service;

(B) identifies the specific categories of persons to which the geolocation information may be disclosed by the provider of geolocation information services and purposes for which it may be disclosed; and

(C) identifies how an individual may revoke their consent for the collection and disclosure of their geolocation information.

(2) COURT OF COMPETENT JURISDICTION.—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.

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

(4) END-TO-END ENCRYPTION.—"End-to-end encryption" has the meaning given to it in NIST publication SP 800-12.

(5) GEOLOCATION INFORMATION.—The term "geolocation information" includes, with respect to a person,

(A) any information concerning the location of a wireless communication device or tracking device (as that term is defined in 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; or

(B) any information that, in whole or in part, is generated or derived from the aggregation of data from the operation of passive monitoring devices, and could be used to determine or infer information regarding the location of the person over a period of time longer than 12 hours.

(6) GEOLOCATION INFORMATION SERVICE.—The term "geolocation information service" includes

(A) 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; or

(B) the provision of any information that, in whole or in part, is generated or derived from the aggregation of data from the operation of passive monitoring devices, and could be used to determine or infer information regarding the location of the person over time.

(7) GOVERNMENTAL ENTITY.—The term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

(8) ACQUIRE.—The term "acquire" means to obtain or receive geolocation information through the use of any electronic, mechanical, or other device.

(9) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—"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.

(10) NIST ENCRYPTION STANDARDS.—The term "NIST encryption standards" refers to the guidance set forth in the National Institute of Standards and Technology (NIST) publications SP 800-175A and 800-175B, or any documents that directly supersede publications SP 800-175A and 800-175B.

(11) PERSON.—"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.

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

(13) STATE.—"State" means any State of the United States, the District of Columbia, the the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(14) 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.

§ 2602. Acquisition and disclosure of geolocation information prohibited.

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally acquires, endeavors to acquire, or procures any other person to acquire or endeavor to acquire geolocation information pertaining to another person;

(b) intentionally discloses, or endeavors to disclose, to any other person geolocation information pertaining to another person, knowing or having reason to know that the information was acquired in violation of this subsection;

(c) intentionally uses, or endeavors to use, any geolocation information, knowing or having reason to know that the information was acquired in violation of this subsection; or

(d) intentionally discloses, or endeavors to disclose, to any other person the geolocation information pertaining to another person acquired by means authorized by sections 2602(2)(a), 2602(2)(b)(ii), 2602(2)(c), and 2602(2)(e)-(g) of this chapter,

(i) knowing or having reason to know that the information was acquired in connection with a criminal investigation,

(ii) having obtained or received the information in connection with a criminal investigation, and

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

shall be punished as provided in subsection (5) of this section or shall be subject to suit as provided in section 2606.

(2) **Exceptions**.—

(a) **Warrant.**—A governmental entity may acquire geolocation information or require the disclosure by a provider of geolocation information service 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.).

(b) **Course of Business**.—

(i) It shall not be unlawful under this chapter for an officer, employee, or agent of a provider of geolocation information service, electronic communication service, or remote computing service, whose facilities are used in the transmission of a person's geolocation information, to acquire, disclose, or use such person's geolocation information in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service requested by such person or to the protection of the rights or property of the provider of that service.

(ii) Notwithstanding any other law, providers of geolocation information service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to acquire geolocation information or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2602(4) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of geolocation information service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any acquisition or surveillance or the device used to accomplish the acquisition or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2606. No cause of action shall lie in any court against any provider of geolocation information service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(c) **Consent.**—

(1) It shall not be unlawful under this chapter for a person to acquire geolocation information pertaining to another person, where such other person has given prior consent to such acquisition unless such geolocation information is acquired 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) The exception in paragraph (1) permits a parent or legal guardian of a minor child to acquire geolocation information pertaining to that minor child or to give consent for another person to acquire such information.

(d) **Public Information**.—It shall not be unlawful under this chapter for any person—

(1) to acquire 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.

(2) to acquire geolocation information which is transmitted by radio communication—

(i) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(ii) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; or

(iii) by any marine or aeronautical navigation or traffic control system.

(e) **Theft or Fraud**.—It shall not be unlawful under this chapter for a provider of geolocation information service or person acting under color of law to acquire, disclose, or use 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 acquisition, disclosure, or use 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.

(f) **Certain Governmental Entities**.—It shall not be unlawful under this chapter for an officer, employee, or agent of:

(1) the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code; or

(2) the Department of Defense, in the normal course of his employment and in discharge of the responsibilities exercised by the Department in the sustainment and operation of the Global Positioning System network or other space-based positioning, navigation, and timing infrastructure pursuant to section 2281 of title 10 of the United States Code;

to acquire geolocation information, or to disclose or use the information thereby obtained.

(g) **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 his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(3) **Disclosure by provider of geolocation information service.—**

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing a geolocation information service shall not intentionally disclose geolocation information pertaining to another person.

(b) A person or entity providing geolocation information service may disclose such geolocation information—

(1) as otherwise authorized in section 2602(2)(b) or 2604 of this title;

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

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

(4) which were acquired by the service provider and which appear to pertain to the commission of a crime, if such disclosure is made to a law enforcement agency.

(4) **Emergency situation exception.—**

(a) It shall not be unlawful under this chapter for any investigative or law enforcement officer or other emergency responder to acquire 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.

(b) 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, who reasonably determines that—

(1) an emergency situation exists that 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,

that requires geolocation information to be acquired before a warrant or order authorizing such acquisition can, with due diligence, be obtained, and

(2) there are grounds upon which a warrant or order could be entered under this chapter to authorize such acquisition,

may acquire such geolocation information if an application for a warrant or order approving the acquisition is made in accordance with this section within forty-eight hours after the acquisition has occurred, or begins to occur.

(c) In the absence of a warrant or order, such acquisition shall immediately terminate when the geolocation information sought is obtained or when the application for the warrant is denied, whichever is earlier.

(d) In the event such application for approval is denied, or in any other case where the acquisition is terminated without a warrant or order having been issued, any geolocation information acquired 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.

(5) **Penalty.**—Whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

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

(1) Whenever any geolocation information has been acquired, no part of such geolocation 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.

(2) Notwithstanding any other provision of this chapter, whenever any geolocation information has been acquired, no part of such geolocation 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 method or technique by which such geolocation information was acquired would be subject to any privilege or agreement that would prohibit the disclosure of such method or technique in such trial, hearing, or proceeding.

§ 2604. Authorization for disclosure and use of acquired geolocation information.

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of geolocation information, or evidence derived therefrom, may disclose such geolocation information to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of geolocation information or evidence derived therefrom may use such geolocation information to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any geolocation information, or evidence derived from such geolocation information, acquired in accordance with the provisions of this chapter may disclose such geolocation information or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged geolocation information acquired in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in acquiring geolocation information in the manner authorized herein, acquires geolocation information relating to offenses other than those specified in the warrant, the geolocation information, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such geolocation information and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the geolocation

information was otherwise acquired in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of geolocation information, or evidence derived therefrom, may disclose such geolocation information to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of geolocation information, or evidence derived therefrom, may disclose such geolocation information or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such geolocation information or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of geolocation information, or evidence derived therefrom, may disclose such geolocation information or derivative evidence to any appropriate Federal, State, local, or foreign government official to

the extent that such geolocation information or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

§ 2605. Procedure for acquisition of geolocation information.

(a) **Minimization procedures.**

(1) **Requirement to adopt.**—The Attorney General shall adopt minimization procedures for the acquisition of geolocation information authorized under sections 2602(2)(a), 2602(2)(b)(ii), 2602(2)(c), and 2602(2)(e)-(g) of this chapter. Such minimization procedures must:

(i) be reasonably designed in light of the purpose and technique of the particular acquisition, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting persons consistent with the need of the United States to acquire geolocation information;

(ii) require that nonpublicly available geolocation information, which is not foreign intelligence information, as defined in 50 U.S.C. § 1801(e)(1), shall not be disseminated in a manner that identifies any person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

(iii) notwithstanding paragraphs (i) and (ii), allow for the retention and dissemination of geolocation information that is evidence of

a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(2) **Judicial review.**—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review to assess whether such procedures satisfy the requirements of paragraph (1).

(3) **Publication.—**The Attorney General shall make such minimization procedures publicly available to the greatest extent practicable.

(b) **Standards for transmission and storage of geolocation information.**—

(1) Transmission of geolocation information over a public or private network by an investigative or law enforcement officer must use end-to-end encryption as specified in the NIST encryption standards.

(2) Any geolocation information held by an investigative or law enforcement agency must be stored in an encrypted format in adherence with the NIST encryption standards.

§ 2606. Civil action.

(a) **In General**.—Except as provided in section 2602(2)(b)(ii), any person whose geolocation information is acquired, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, 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.**—

(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.**—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 2602(4) of this title; or

(3) a good faith determination that section 2602(3) or 2602(2)(e) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(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, he or she 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 section 2604 is a violation of this chapter for purposes of section 2602(1)(a).

(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".

SECTION 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.".

SECTION 4. 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 et. seq.).

(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.

* * *