A BILL

To amend title 18, United States Code, to specify the circumstances in which law enforcement may acquire, use, and keep geolocation information.

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 "Geolocation Information Privacy Protection Act" (GIPPA).

SECTION 2. DEFINITIONS.

In this chapter:

(1) "Acquisition" means the obtaining of information through any means other than solely human observation.

(2) "Authorized possessor" means, with respect to a device or geolocation information,

(a) the owner of the device and/or geolocation information; or

(b) a person who has been authorized by the owner to possess the device; or

(c) a person to whose geolocation the information pertains.

(3) "Covered service" means an electronic communication service, a remote computing service, or any entity that makes publicly available a global positioning service or other mapping, locational, or directional information service.

(4) "End-to-end encryption" means the transmission of communication between a sender and a receiver such that no parties facilitating the communication, other than the sender and receiver, are able to decrypt the communication contents.

(5) “Geolocation” means the latitude and longitude at which a person is located.

(6) “Geolocation information” means, with respect to a person, any information or data that is created or collected by a service provider or device and is used, expected to be used, or collected for the purpose of determining or recording with reasonable certainty and within a distance of one mile the present, past, or future geolocation of a person, even if the information or data is not by itself sufficient to achieve that purpose.

(7) “Human observation” means observation or recording of observations conducted by a human or humans through their natural senses of sight, hearing, touch, smell, and/or taste, unaided by any observational technology, as defined below.

(8) “Investigative or law enforcement agent” means any officer or entity of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations or to make arrests, and any attorney authorized by law to prosecute or participate in the prosecution related to such investigations or such arrests.

(9) “NIST cryptographic standards” refers to the guidelines described in U.S. National Institute of Standards Technology (“NIST”) Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government, or its most up-to-date successor. In the case that new standards are released by NIST that supersede older standards, the term “NIST cryptographic standards” shall encompass both the new standard and its predecessor standard for the 90 days following the release of the new standard, after which the term shall refer only to the new standard.

(10) “Observational technology” means any technology that substantially adds to a human’s observation, recording, and/or memory capabilities, including but not limited to—

(a) IMSI-catchers;

(b) audio, image, or video recording equipment, such as cameras;

and excluding technology that serves to enhance a human's sensory capabilities to a level that is commonly considered to be within a reasonable range of normal human capabilities, or that records natural language written or dictated by a human to describe his or her observations.

(11) "Publicly available" means information that—

(a) can be lawfully disclosed to the public, and

(b) members of the public have reasonable opportunity to know it is available, and

(c) satisfies any of the following:

(1) has been published or broadcast for public consumption;

(2) is available on request to the public;

(3) is accessible online or otherwise to the public;

(4) is made reasonably available to the public by subscription or purchase;

(5) could be seen or heard by casual observers in a place open to the public;

(6) is made available at a meeting open to the public; or

(7) is obtained by visiting any place or attending any event open to the public.

(12) "Service provider" means a person that provides or facilitates the provision of a covered service, and/or provides or facilitates in the administration of a covered service, such as electronic storage of geolocation data.

(13) "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.

(14) The following terms have the meaning given to them in §2510:

(a) "Court of competent jurisdiction";

(b) "Electronic communication service";

(c) "Remote computing service."

SECTION 3. ACQUISITION AND USE OF GEOLOCATION INFORMATION.

(a) IN GENERAL.—Except as otherwise specifically provided in this act, an investigative or law enforcement agent shall not—

(1) intentionally acquire nor direct any other person to acquire a person's geolocation information; nor

(2) intentionally use, nor endeavor to use, any geolocation information, knowing or having reason to know that the geolocation information was obtained through acquisition in violation of this paragraph.

(b) WARRANT.—An investigative or law enforcement agent may acquire geolocation information or require the disclosure of geolocation information by another entity only pursuant to a valid warrant.

(1) WARRANT REQUIREMENTS.—An investigative or law enforcement agent must obtain a warrant issued using the procedures described in Federal Rule of Criminal Procedure 41 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction in order to acquire geolocation information. Any warrant for the acquisition of geolocation information must both—

(A) describe with particularity the geolocation data to be seized by specifying:

(i) whether this time period is to be contemporaneous with seizure;

(ii) the geographical precision of data to be seized for each time period;

(iii) the frequency of geolocation data collection within each time period;

(iv) the targeted individuals or accounts;

(v) the applications, devices, or services covered; and

(vi) if appropriate, the types of locations sought.

(B) require that information obtained through the execution of the warrant, but outside of the scope of the objective of the warrant, shall be sealed and not subject to further review, use, or disclosure without a court order, which will be granted only on the finding of probable cause that the information is relevant to ongoing or active investigation.

(2) NOTICE OF WARRANT.—No later than 3 days after an investigative or law enforcement agent obtains geolocation information pursuant to a valid warrant, the State or investigative or law enforcement agent shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the relevant authorized possessor(s)—

(A) a copy of the warrant; and

(B) a notice that includes information referred to in paragraph (1)(A)(iv)-(vi).

(3) DELAY OF NOTIFICATION.—

(A) IN GENERAL.—An investigative or law enforcement agent that is seeking a warrant under paragraph (1)(A) may include in the application for the warrant a request for an order delaying the notification for a period of not more than 90 days.

(B) DETERMINATION.—A court shall grant a request for delayed notification if the court determines there is reason to believe that notification of the existence of the warrant may result in—

(i) endangering the life or physical safety of any person;

(ii) flight from prosecution;

(iii) destruction of or tampering with evidence;

(iv) intimidation of potential witnesses;

(v) otherwise seriously jeopardizing an investigation or unduly delaying a trial; or

(vi) endangerment of national security.

(C) EXPIRATION OF THE DELAY OF NOTIFICATION.—Upon expiration of the period of delay of notification, the State or investigative or law enforcement agent shall—

(i) serve notice pursuant to the requirements of paragraph (b)(2) and a notice that informs the relevant authorized possessor(s)—

(I) that information maintained for such relevant authorized possessor(s) by the covered service named in the process or request was supplied to, or requested by, the investigative or law enforcement entity;

(II) of the date on which the request to the provider for information was made by the State or investigative or law enforcement agent and the date on which the information was provided by the provider to the

State or investigative or law enforcement agent;

(III) that notification of such relevant authorized possessor(s) was delayed, and the length of the delay;

(IV) the identity of the court authorizing the delay; and

(V) of the provision of this chapter under which the delay was authorized; and

(ii) send written notification of service and a copy of the notice served to the court that granted the delay request; and

(iii) annually publish a report including the number of delays requested and granted, to be made available to the public free of charge.

(c) GENERAL EXCEPTIONS.—Notwithstanding any other provision of this act, any investigative or law enforcement agent, with authorization from 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 acquire, for reasonably specific purposes, geolocation information concerning a person only in the following circumstances and to the extent necessary for such purposes:

(1) 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.).

(2) CONSENT.—

(A) IN GENERAL.—It shall not be unlawful under this chapter for a person to acquire or use geolocation information pertaining to another person if such other person has given prior consent, while being at least 18 years of age, to such acquisition and use, unless such information was 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.

(B) CHILDREN.—The exception in paragraph (c)(2)(B)(1) permits a parent or legal guardian of a child, as defined under 15 U.S.C. §6501, to acquire geolocation information pertaining to that child or to give consent for another person to acquire such information.

(3) EMERGENCY INFORMATION.—It shall not be unlawful under this chapter for any investigative or law enforcement agent or other emergency responder to acquire or access geolocation information relating to a person if such information is used—

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

(B) in circumstances in which it is reasonable to believe there is immediate danger of death or serious physical injury to any person.

(4) THEFT OR FRAUD.—It shall not be unlawful under this chapter for an investigative or law enforcement agent to acquire geolocation information pertaining to the location of another person who has unlawfully taken the device sending the geolocation information if—

(A) the authorized possessor of such device authorizes such acquisition of the device's geolocation information;

(B) the investigative or law enforcement agent is lawfully engaged in an investigation; and

(C) the investigative or law enforcement agent has reasonable grounds to believe that the geolocation information of the other person will be relevant to the investigation.

(5) PUBLICLY AVAILABLE INFORMATION.—It shall not be unlawful under this chapter for any law enforcement entity to acquire or access geolocation information relating to another person through any system that is intentionally and lawfully configured by an authorized possessor to make that information publicly available, except where such information unlawfully became publicly available.

(6) COMPLIANCE.—An agency or department of the United States or a State may collect geolocation information concerning an investigative or law enforcement agent in order to ensure compliance with existing laws and/or the safety of the officer, in accordance with the data retention requirements in Section 5.

(7) EXIGENT CIRCUMSTANCES.— Such officer reasonably determines that an exigent circumstance, as defined in Section 4(c)(2), exists and, for the purpose of investigating a reasonable articulable suspicion regarding the exigent circumstance:

(A) geolocation information must be acquired before an order authorizing such acquisition can, with due diligence, be obtained; and

(B) there are grounds upon which a court order could be entered to authorize such acquisition, and an application for a court order approving such acquisition is made within 48 hours after the acquisition has occurred or begins to occur and has not been denied.

(8) LIMITED SHORT-TERM SURVEILLANCE.—It shall not be unlawful under this chapter for any law enforcement entity to acquire or access geolocation information if one of the following two conditions are met and no other laws are violated—

(A) an investigative or law enforcement agent has not made an acquisition of geolocation concerning said person within the 90 days prior to the start of acquisition; and

(B) the time from first acquisition to last acquisition, excluding gaps of more than 90 days, is no more than 24 hours.

SECTION 4. DATA DISCLOSURE.

(a) IN GENERAL.—

(1) PROHIBITION ON DISCLOSURE.—Except as reasonably pursuant to a valid investigation, it shall be unlawful for any investigative or law enforcement agent to intentionally disclose, or endeavor to disclose, to another person geolocation information pertaining to another person—

(A) knowing or having reason to know that the information was obtained through the acquisition of such information in violation of Section 3 of the act; or

(B) that was acquired by means authorized by Section 3 of the act.

(2) REQUIRING DISCLOSURE FROM SERVICE PROVIDERS.—An investigative or law

enforcement agent may not require a service provider to disclose geolocation information contemporaneously or prospectively with respect to the provider's collection of such information unless pursuant to Section 3.

(b) STANDARDS FOR DISCLOSURE.—

(1) Any disclosure of geolocation information over the internet or over an intranet by or to an investigative or law enforcement officer, employee, or agent thereof must employ end-to-end encryption in adherence with NIST cryptographic standards.

(2) If security vulnerabilities in the NIST encryption standards are discovered and disclosed to an investigative or law enforcement agent, all relevant security patches must be deployed within a reasonable period of time of endorsement by NIST. During the intervening period, after a vulnerability is found and while it has not been patched, geolocation information may not be transferred by or to an investigative or law enforcement agent over the internet except in case of a reasonable determination that an exigent circumstance exists that both—

(A) involves—

(i) immediate danger of death or serious physical injury to any person, or

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime; and

(B) requires for the purpose of investigating a reasonable articulable suspicion regarding said exigent circumstance that geolocation information be disclosed immediately.

(3) Any entity to whom geolocation information is disclosed must store it in encrypted

form adhering to the data storage requirements in Section 5, and must process unencrypted data only for the minimum time periods necessary for the purpose(s) for which the data was disclosed. The requirements in this paragraph and the purpose(s) for which the disclosed data may be used must be communicated clearly in writing to any person to whom a disclosure is pending, and the person must affirmatively agree to the conditions before the disclosure happens.

(4) EFFECTIVE DATE.—Subsection (b)(1)-(2) shall take effect in three years.

SECTION 5. DATA RETENTION AND STORAGE.

(a) DATA STORAGE REQUIREMENTS.

(1) All copies of geolocation information must be stored encrypted in adherence with NIST cryptographic standards.

(2) Unencrypted data must be processed only for the minimum time periods necessary for the unimpeded operation of an ongoing investigation.

(b) COPYING OR PRINTING DATA.—An investigative or law enforcement agent must—

(1) keep a log of each copy made of geolocation information so that all copies can later be purged subject to deletion requirements;

(2) maintain digital copies of data carried into the field encrypted whenever possible; and

(3) maintain any prints or other hard copies made of data in a secure location. When hard copies of data are created, there must be a written record detailing—

(A) a time period, no longer than 30 days, after which the hard copy must be destroyed; and

(B) a justification that using a digital copy instead was reasonably believed to be

inadequate or harmful for the intended purpose.

(c) LENGTH OF STORAGE.—An investigative or law enforcement agent may store geolocation data for an allowed period defined as follows:

(1) for the length of the investigation pursuant to which the geolocation data was collected; or

(2) in the case of data that was not collected pursuant to any investigation, for up to 2 years.

At the close of the allowed period, an investigative or law enforcement agent shall—

(3) delete any geolocation information, including all backups, after no more than 90 days; and

(4) send notifications within 30 days to any parties to whom the geolocation data was disclosed, to inform them that they must delete all copies of the data and send back a statement confirming the deletion within 60 days of receiving the notification.

(d) DELETION.— An investigative or law enforcement agent shall follow the National Industrial Security Program Operating Manual, DoD 5220.22-M, Clearing and Sanitization Matrix to sanitize data.

(e) EFFECTIVE DATE.—Subsection (a) shall take effect in two years.

SECTION 6. PROHIBITION OF USE AS EVIDENCE OF ACQUIRED GEOLOCATION INFORMATION.

(a) PROHIBITION ON USE AS EVIDENCE.—Whenever any geolocation information has been acquired in violation of this act, 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.

(b) NOTICE.—In the event a warrant application 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.

SECTION 7. SANCTIONS FOR VIOLATIONS OF THIS CHAPTER.

(a) Any investigative or law enforcement officer, employee, or agent thereof that is found to have violated the conditions in Sections 3, 4, 5, or 6 of this act may be subject to penalties under this Section, including civil action from the person whose right under this act were violated and/or appropriate administrative discipline. In the cases of violations of Section 4(b), Section 5(b), and Section 5(c), civil actions are only applicable in the case that the claimant has contacted law enforcement to inform them about the violation and to request administrative discipline be taken, and law enforcement has been unresponsive to the concerns expressed by the claimant for more than 365 days.

(b) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or a State has violated any provision of this chapter, and the court or appropriate department or agency finds that circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States or a State 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.

(c) 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 (d) in appropriate cases; and

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

(d) COMPUTATION OF DAMAGES.—In any action under this section, the court may assess as damages 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 $700 a day for each day of violation or $70,000.

(e) DEFENSE.—A good-faith reliance on any of the following is a complete defense against any criminal action brought under this chapter or under any other law:

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

(2) a request of an investigative or law enforcement agent under Section 3(d)(8) of this act; or

(3) a good-faith determination that Section 3(d) of this act permitted the conduct complained of.

(f) 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.

SECTION 8. This act shall apply notwithstanding any other law.

Introduced for Congressional Debate by _____.