The Geolocation Information Privacy Protection Act (GIPPA)
Section-by-Section Summary

Section 1. Title

The bill is entitled the "Geolocation Information Privacy Protection Act" or "GIPPA."

Section 2. Definitions

This section provides the definitions of key terms in the bill. It also defines the scope of the act by detailing what is regulated, who is regulated, the security requirements for storing and transferring data, and the information needed to understand exceptions to the regulation.

This bill broadly regulates "geolocation information," which is any information that is used to determine the location of a person or device within one-mile accuracy. However, it limits the information regulated only to data that is created or collected from a device or by service providers of location information. The broad definition allows technology-neutral regulation that naturally adapts to technological development and whose applicability need not be restricted by the scope of currently existing technologies. In addition, it is designed to protect data held by both providers of geolocation information services and entities that administer and/or store the data. Notably, this broad regulation provides protection to individuals who would otherwise have been held to have voluntarily given away their location information to third parties and thus have no constitutional right to privacy of that data from law enforcement (this line of reasoning is formally known as the Third-Party Doctrine).

This bill explicitly regulates "investigative or law enforcement" agents' acquisition, use, disclosure, and storage of geolocation information. The term is found in the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §2510, and thus limits the application of the bill to the same individuals covered by ECPA. "Agent" refers to both individual officers and legal entities, expanding the scope of the act to regulate all law enforcement.

This bill incorporates several definitions from other acts. For example, the terms "court of competent jurisdiction," "electronic communication service," and "remote computing service" are from the ECPA. These definitions are widely used and understood in current jurisprudence. Similarly, the definition of "State" is the same provision as in the GPS Act, H.R. 1062, 115th Cong. (2017) (hereinafter "GPS Act") and the Espionage Act, 18 U.S.C. §3077. This definition was necessary to ensure jurisdiction over both federal and state governments. Finally, the definition of "publicly available" is similar to the term as defined in The Attorney General's Guidelines for Domestic FBI Operations of 2008, but modified to specify that members of the public must have had reasonable opportunity to know the information was available.

Section 3(a). Acquisition and Use of Geolocation Information

This section generally prevents investigative or law enforcement agents from acquiring or using geolocation information. This overarching limitation is predicated on the idea that unless law enforcement has a warrant, or one of the exceptions for a warrantless search applies, they should not be allowed unrestricted access to individuals' geolocation information. This broad rule is subject to a valid warrant under 3(b) and to various exceptions under 3(c).

Section 3(b). Warrant and Notice Requirements

This section differentiates the requirements for the acquisition of geolocation information with and without a warrant. First, law enforcement can acquire or disclose geolocation information by obtaining a valid warrant in accordance with Federal Rule of Criminal Procedure 41. A valid warrant requires law enforcement to describe with particularity the data to be collected or disclosed and to have probable cause for believing that evidence of the crime is present in the place to be searched. A failure to obtain a warrant under the act requires that law enforcement terminate collection immediately and a complete bar on using the location information as evidence. This section also requires law enforcement to notify a person that geolocation information has been obtained within three days. However, law enforcement may delay this notice for up to 90 days if it meets defined exceptions.

Section 3(c). Exceptions

This section provides eight exceptions to the prohibition on acquiring geolocation information. The first exception is for a valid Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801–1885(c), order, when the information is necessary to ensure national security interests. It is the same provision as is found in the GPS Act and is modeled after the exception found in ECPA, 18 U.S.C. §2511(2)(a)(ii) The second exception allows acquisition if the person to whom the data pertains, or their parent or legal guardian in the case of a child, consents. It is the same provision as is found in the GPS Act with slight changes to clarify that the definition of a "child" is the same as that in the Children's Online Privacy Protection Act, 15 U.S.C. §6501, the main privacy statute relating to children. The third exception provides for the disclosure of geolocation information in the event of an emergency, allowing for the operation of 911 and other emergency services, and is modeled after the GPS Act and the Stored Communications Act, 18 U.S.C. §2702(b)(8). The fourth exception allows acquisition in the event of theft or fraud, and it is the same provision as is found in the GPS Act. The fifth exception allows acquisition of publicly available geolocation information. It is based on Fourth Amendment jurisprudence that limits one's expectation of a right to privacy for anything done or said in public. To address instances of unlawful data breaches or hacking, law enforcement is also prohibited from acquiring

geolocation information that was unlawfully made public. The sixth exception allows for compliance with other existing laws and/or the normal business and/or safety of police officers, such as when states require that officers wear body cameras. Finally, the seventh exception allows acquisition with a valid warrant as described in Section 6 below.

The eighth exception allows law enforcement to acquire geolocation information without a warrant as long as (1) the person's information has not been acquired by law enforcement within the past 90 days and (2) the time from first acquisition to last acquisition is not more than twenty-four hours. The 24-hour period is based on the idea put forth by the shadow majority in *US v. Jones* that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." (565 U.S. 400, 430 (2014)). Twenty-four hours provides enough time for law enforcement to monitor a suspect's habits and behavior over the course of a day. After the 24-hour mark, however, law enforcement may be able to paint an incredibly accurate portrait of an individual's life by identifying patterns and inferences across daily movements, which infringes on an individual's expectation of privacy. The 90-day limit is meant to discourage consistent warrantless searches in abrogation of the principle of the bill.

Fundamentally, the 24-hour and 90-day limitations are meant to ensure that law enforcement cannot ascertain substantively more information about an individual than his or her short-term geographical location, while still providing them with a reasonable amount of data-gathering capability for investigations. These restrictions also prevent warrantless use of "blanket" geolocation collection methods that engage in incidental collection beyond specific targeted individuals, such as IMSI-catchers. Due to the inability to determine who is in the vicinity of an IMSI-catcher prior to its use, law enforcement will seek a warrant to comply with the act so as to not violate the 24-hour, 90-day limitation.

Section 4. Data Disclosure

This section limits intentional disclosure of geolocation information by law enforcement and disallows compulsion of geolocation data from service providers without a valid warrant. This section also creates standards for disclosure of geolocation information by requiring that law enforcement and the recipients of geolocation information disclosures use cryptographic standards from the National Institute of Standards and Technology (NIST) to transmit and store geolocation information, and that disclosures may only be made to recipients who have affirmatively acknowledged these requirements. To allow enough time for careful implementation and transition, the act allows an initial three years after the act is passed, for law enforcement to implement the standards.

Section 5. Data Retention and Storage

This section creates specific technological requirements for the storage and deletion of data, procedures for the copying and printing of data, and limits on the length of storage of geolocation data based on NIST guidelines. The requirements stipulate that law enforcement delete any data collected pursuant to an investigation within 90 days of the close of the investigation, and that it delete any data that was not collected pursuant to an investigation within two years of collection. This section has an effective date of two years after the passage of the act.

Section 6. Prohibition of Use as Evidence of Acquired Geolocation Information

This section prevents the use of any geolocation information that has been acquired in violation of this act as evidence in any proceeding. This adopts the exclusionary rule and its extension, the fruit of the poisonous tree doctrine, which excludes any additional evidence gained as a result of the violation.

Section 7. Sanctions for Violations of this Chapter

This section addresses the penalties for violation of the bill by providing two key enforcement mechanisms. First, a court, department, or agency may seek administrative discipline against a law enforcement agent for any violation of the act. Second, an individual may seek injunctive relief, damages, and litigation costs for unlawful acquisition of his or her geolocation data by law enforcement, but would not be able to sue for technical notice violations under the act under Section 4(b), Section 5(b), and Section 5(c). Such technical notice violations are excepted from civil action as they would be better addressed by administrative discipline. This relief is consistent with the relief provided in ECPA, 18 U.S.C. §2520.

Section 8. Conflict of Law

This section provides that this act shall apply notwithstanding any other law.