The Geolocation Privacy and Surveillance Act One-Page Summary

· Provides clarity for government agencies, commercial service providers, and the public regarding the legal procedures and protections that apply to electronic devices that can be used to track the movements of individual Americans. The Congressional Research Service identified a lack of cohesion throughout criminal court jurisdictions over what standards and procedures must be met in order for location information gathered though electronic devices to be used in court. This lack of clarity has led to confusion among law enforcement and prosecutors, who waste valuable time and resources litigating and appealing what should be clear cut rules.

· Requires the government to show probable cause and get a warrant before acquiring the geolocational information of a U.S. person, while setting out clear exceptions such as emergency or national security situations or cases of theft or fraud.

· Applies to all law enforcement acquisitions of the geolocational information of individual Americans without their knowledge, including acquisition from commercial service providers as well as direct acquisitions using "Stingrays" and similar devices or tracking devices covertly installed by the government.

· Applies to real-time tracking of a person's movements, as well as the acquisition of records of past movements. (Real-time tracking = "Where is John Smith right now?" Acquisition of records of past movements ="Where did John Smith go on St. Patrick's Day?")

· Closely tracks existing wiretapping laws with regard to court procedures for getting a warrant, penalties for acting without a warrant, exclusivity of the authority, authorization without a court order, etc.

· Creates criminal penalties for surreptitiously using an electronic device to track a person's movements that parallel those for wiretapping. (Currently, if a woman's ex-husband taps her phone, he is breaking the law. This legislation would treat hacking her GPS to track her movements as a similar offense).

· Prohibits commercial service providers from sharing customers' geolocation information with outside entities without customer consent.