



Two Federal Geolocation Tracking Bills Introduced

August 8, 2011 by James Taylor, Ken Florin and Ieuan Jolly

Bills limiting the use of geolocation information collected from mobile and other devices were introduced in both chambers of Congress in June. The Location Privacy Protection Act of 2011 (S. 1223) and The Geolocation Privacy and Surveillance (GPS) Act (H.R. 2168, S. 1212) both would limit the collection and use of data by mobile device manufacturers and others. In addition, The GPS Act would also prevent law enforcement from obtaining this data without a warrant.

Sens. Al Franken (D-Minn.) and Richard Blumenthal (D-Conn.) introduced [The Location Privacy Protection Act](#). According to [statements](#) issued by Sen. Franken, chairman of the Judiciary Subcommittee on Privacy, Technology and the Law, the bill is aimed at closing “loopholes” in current federal law allowing device manufacturers, app developers and telephone companies offering wireless Internet service to freely share their consumer location information with third parties.

The bill would require covered entities to get consumers’ express authorization before both collecting location data and sharing that data with third parties. Express authorization is defined in the Act as “express affirmative consent after receiving clear and prominent notice,” displayed on the device, of what geolocation data will be collected and to what third parties the data will be disclosed. The notice must be separate from terms of use, privacy policies or end user agreement.

The Act defines covered entities as nongovernment entities in interstate commerce that offer or provide “a service to electronic communications devices, including, but not limited to, offering or providing electronic communication service, remote computing service, or geolocation information service[.]” Electronic communications devices specifically include those meant to be carried by or on a person, or travel with the individual, including the person’s vehicle.

The bill contains an “Anti-Cyberstalking Protection” provision that requires companies to provide a verification’ to an individual, displayed on the individual’s device, not earlier than 24 hours and not later than seven days after the individual expressly authorizes the disclosure of geolocation data to another individual, that data is being disclosed, as well as how consent may be revoked.

The bill allows civil actions by the U.S. Attorney General against violators of the Act, as well as actions by states Attorneys General and private cases of action. It also creates criminal penalties for those that aid in or facilitate stalking, including those entities that create so-called “stalking apps” that disclose geolocation information, knowing and intending that domestic violence or stalking will result. The bill also criminalizes knowingly and intentionally aggregating and selling of the location data of children 10 years old and younger.

The bill also calls upon the National Institute of Justice to issue a study on the use of location technology in dating violence, stalking and domestic violence. Other provisions facilitate the reporting of these crimes to the FBI’s Internet Crime Complaint Center and call upon the Attorney General to develop a training curriculum aimed at helping law enforcement, courts, and victim advocates better investigate and prosecute crimes involving the misuse of geolocation data.



Advanced Media
and Technology

LAW BLOG



While The Location Privacy Protection Act of 2011 would apply only to nongovernment entities and does not affect the ability of law enforcement to obtain geolocation data, the [GPS Act](#), introduced by Sen. Ron Wyden (D-Ore.) and Rep. Jason Chaffetz (R-Utah), applies to government agencies – including law enforcement – as well as commercial entities and individuals. Under the GPS Act, companies would be required to obtain consent before sharing the data with third parties. For law enforcement, information gathered from mobile devices would be treated the same as a wiretap, requiring a warrant to obtain the information.

Modeled after federal wiretapping laws, the bill would prohibit the interception or use of geolocation information data by any person, or the disclosure to another person of that information, without prior consent. “Person” is broadly defined under the Act as “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.” Geolocation information includes any information concerning the location of a wireless communication device or tracking device, generated by or derived from the operation of that device, that could be used to determine the location of the person.

While the Act allows service providers to collect geolocation information in the normal course of business, it specifically prohibits the disclosure of information to third persons without consent. Unlike the Location Privacy Protection Act, the GPS Act does not require “affirmative consent after notice” nor does it provide any requirements for consent or how entities covered by the Act must obtain it, other than that the consent must be prior to the interception, use or disclosure of the information.

As it relates to law enforcement, the Act prohibits the interception of geolocation information without a warrant obtained pursuant to the provided procedures, which closely track those in the federal wiretapping laws. The Act provides a limited list of exceptions to the warrant requirement, including exceptions for the investigation of the theft of the device, or in circumstances where the safety of the device’s owner is threatened.

The Act authorizes a private right of action for damages, as well as criminal penalties for violations. It also authorizes an administrative discipline process for officers or employees found to have willfully or intentionally violated the Act.

This publication may constitute "Attorney Advertising" under the New York Rules of Professional Conduct and under the law of other jurisdictions.

© 2011 Loeb & Loeb LLP. All rights reserved.