S 1223

Location Privacy Protection Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Crime and Law Enforcement
Introduced: Jun 16, 2011
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 567.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 567. (Dec 17, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/1223

Sponsor

Name: Sen. Franken, Al [D-MN]
Party: Democratic • **State:** MN • **Chamber:** Senate

Cosponsors (6 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Blumenthal, Richard [D-CT]	D · CT		Jun 16, 2011
Sen. Coons, Christopher A. [D-DE]	D · DE		Jul 11, 2011
Sen. Durbin, Richard J. [D-IL]	D · IL		Sep 19, 2011
Sen. Sanders, Bernard [I-VT]	I · VT		Sep 19, 2011
Sen. Menendez, Robert [D-NJ]	D · NJ		Sep 21, 2011
Sen. Feinstein, Dianne [D-CA]	D · CA		Jan 26, 2012

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	Senate	Reported By	Dec 17, 2012

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

No related bills are listed.

Summary (as of Dec 17, 2012)

Location Privacy Protection Act of 2012 - (Sec. 3) Amends the federal criminal code to prohibit a covered entity from knowingly collecting, receiving, recording, obtaining, or disclosing to a nongovernmental individual or entity geolocation information from an electronic communications device without the express authorization of the individual using the device. Defines a "covered entity" as a nongovernmental individual or entity engaged in the business of offering or providing a service, including an electronic communication service, remote computing service, or geolocation information service, to electronic communications devices.

Makes exceptions if the covered entity has a good faith belief that the collection, receipt, recording, obtaining, or disclosure is: (1) to allow a parent or legal guardian to locate a minor child; (2) for the provision of fire, medical, public safety, or other emergency services; (3) for the sole purpose of transmitting the geolocation information to the individual or another authorized recipient; (4) necessary to protect the rights or property of the covered entity or to protect customers of such entity or other covered entities from fraudulent, abusive, or unlawful use of, or subscription to, such services; (5) pursuant to a court order in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if the individual is given reasonable notice by the person seeking the disclosure of the court proceeding relevant to the issuance of the court order and the individual is afforded the opportunity to appear and contest the claim of the person seeking the disclosure; (6) requested by a law enforcement or intelligence agency, a state, or a political subdivision pursuant to any lawful authority or activity, if the covered entity uses the geolocation information solely for law enforcement or intelligence purposes; or (7) a collection of geolocation information that is necessary for network operation by an entity that is subject to provisions of the Communications Act of 1934 relating to confidentiality of customer information and protection of subscriber privacy, if the entity uses the information solely for purposes of network operation. Requires the court to impose appropriate safeguards against unauthorized disclosure if such a court order is granted.

Prohibits a covered entity from being required to obtain an additional express authorization where: (1) an initial express authorization was previously obtained, (2) the nature of the information sought has not changed, and (3) the geolocation information is being disclosed to a nongovernmental individual or entity specified at the time of the initial authorization.

States that a covered entity: (1) that obtains geolocation information from the covered entity that initially obtained the information shall not be required to obtain an express authorization for obtaining or disclosing such information; (2) that has a reasonable belief that it is impossible to communicate express authorization by means of a display on an electronic communications device may communicate the express affirmative consent orally or in writing; and (3) shall not be required to obtain an express authorization for obtaining or disclosing geolocation information if that entity does not have actual knowledge that the electronic device from which the covered entity is obtaining the information is being used by an individual different from the one from whom that entity obtained express authorization and if such entity is not obtaining such information in a manner that the entity knows and intends to be imperceptible to the individual.

Requires, except where geolocation information is being collected at the request of a law enforcement or intelligence agency, a state, or a political subdivision, a covered entity that obtains the information in a manner that such entity knows and intends to be imperceptible to the individual to provide notice, not earlier than 24 hours and not later than 7 days after the initial collection, that informs the individual: (1) what geolocation information is being obtained; (2) the nongovernmental individuals or entities to which such information is disclosed; and (3) how the individual may electronically revoke consent to the collection and disclosure of such information.

Authorizes civil actions by the Attorney General, state attorneys general, and aggrieved individuals for violations of this

Act, subject to specified limitations.

(Sec. 4) Prohibits a covered entity from knowingly and intentionally disclosing geolocation information about an individual to another individual in aid of interstate domestic violence or stalking.

(Sec. 5) Directs the National Institute of Justice to conduct a national study to examine the role of geolocation information in violence against women.

(Sec. 6) Requires the Attorney General to direct the Internet Crime Complaint Center to: (1) provide education and awareness information to the public and law enforcement, and (2) register complaints regarding the abuse of geolocation information to commit domestic violence, dating violence, sexual assault, stalking, or other related crimes.

(Sec. 7) Authorizes the Director of the Office on Violence Against Women to make grants to entities to develop and provide training to law enforcement officers, prosecutors, judges, and victim service personnel regarding relevant federal, state, territorial, or local law and promising practices, procedures, and policies relating to investigating and prosecuting the misuse of geolocation information in the commission of stalking, domestic violence, dating violence, sexual assault, and other crimes.

Actions Timeline

- **Dec 17, 2012:** Committee on the Judiciary. Reported by Senator Leahy with an amendment in the nature of a substitute. Without written report.
- **Dec 17, 2012:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 567.
- **Dec 13, 2012:** Committee on the Judiciary. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Jun 16, 2011:** Introduced in Senate
- **Jun 16, 2011:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S3894-3896)

LegiList

CONGRESS, MADE CLEAR.

Search Every Federal Bill, Law, and Vote

LegiList is the fastest way to research Congress. Track any bill from introduction to enactment, see how every legislator voted, follow committee activity, and read the full text of every bill — all in one place, always up to date.

legilist.com

Free Course: Learn How Congress Actually Works

LegiList Learn is a free, self-paced course that walks through the entire legislative process — from drafting a bill to a presidential signature. Seven modules, plain language, no politics. Earn a certificate when you finish.

legilist.com/learn

Developer API: Build Apps on Legislative Data

The LegiList API gives developers direct access to bills, votes, legislators, committees, and more. Start free with 1,000 requests per day — no credit card required. Upgrade to Pro when you need to scale.

legilist.com/api

Public data belongs to the public. — legilist.com