

S 2171

Location Privacy Protection Act of 2014

Congress: 113 (2013–2015, Ended)

Chamber: Senate

Policy Area: Crime and Law Enforcement

Introduced: Mar 27, 2014

Current Status: Committee on the Judiciary Subcommittee on Privacy, Technology and the Law. Hearings held.

Latest Action: Committee on the Judiciary Subcommittee on Privacy, Technology and the Law. Hearings held. (Jun 4, 2014)

Official Text: <https://www.congress.gov/bill/113th-congress/senate-bill/2171>

Sponsor

Name: Sen. Franken, Al [D-MN]

Party: Democratic • **State:** MN • **Chamber:** Senate

Cosponsors (5 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Coons, Christopher A. [D-DE]	D · DE		Mar 27, 2014
Sen. Warren, Elizabeth [D-MA]	D · MA		Mar 27, 2014
Sen. Blumenthal, Richard [D-CT]	D · CT		Apr 2, 2014
Sen. Durbin, Richard J. [D-IL]	D · IL		Apr 3, 2014
Sen. Feinstein, Dianne [D-CA]	D · CA		Jun 5, 2014

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	Senate	Hearings By (subcommittee)	Jun 4, 2014

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

No related bills are listed.

Location Privacy Protection Act of 2014 - Amends the federal criminal code to prohibit a covered entity (nongovernmental individual or entity) from knowingly collecting or disclosing to another covered entity geolocation information from an electronic communications device without the consent of the individual using the device. Specifies exceptions, including for collection or disclosure: (1) for the provision of fire, medical, public safety, or other emergency services; or (2) pursuant to a court order or a request by a law enforcement agency.

Defines "geolocation information" as specified information that is not the contents of a communication, is generated by or derived from the operation or use of such a device, is sufficient to identify the street and city or town in which the device is located, and does not include the Internet protocol address or the home, business, or billing address of the individual. Defines "consent" as affirmative express consent after receiving clear, prominent, and accurate notice that: (1) informs the individual that his or her geolocation information will be collected, (2) identifies the categories of covered entities to which the information may be disclosed, and (3) provides the individual easy access to the collecting agency's geolocation information website.

Requires a covered entity that initially collects geolocation information from such a device in a manner that it has reason to believe is imperceptible to the individual using the device, in addition to obtaining consent, to provide clear, prominent, and accurate notice to the individual, not earlier than 24 hours nor later than 7 days after the initial collection, that geolocation information is being collected

Requires a covered entity that collects the geolocation information of more than 1,000 electronic communications devices in a year to maintain a publicly accessible Internet website that includes: (1) the nature of the information collected; (2) the purposes for which the covered entity collects, uses, and discloses the information; (3) the specific covered entities to which the collecting entity discloses geolocation information; and (4) how an individual may electronically revoke consent for the collection and disclosure of such information.

Requires the Attorney General to issue regulations to implement such requirements. Authorizes civil actions by the Attorney General and aggrieved individuals for violations of this Act, subject to specified limitations.

Prohibits: (1) the unauthorized disclosure of geolocation information in aid of interstate domestic violence or stalking; (2) the fraudulent collection of geolocation records information obtained by a geolocation information service; and (3) the manufacture, distribution, possession, and advertising of geolocation information intercepting devices. Provides for the forfeiture of such devices. Establishes in the Treasury an Anti-Stalking Fund: (1) into which shall be deposited an amount equal to the value of any such device and related proceeds forfeited, and (2) which the Attorney General shall use for training on investigating and prosecuting stalking crimes and for support of help line and emergency response efforts for such crimes.

Directs the Attorney General to include as part of each National Crime Victimization Survey, and the Director of the Center for Disease Control and Prevention (CDC) to include as part of each National Intimate Partner and Sexual Violence Survey, questions examining the role that various new technologies that use geolocation information may have in the facilitation of domestic violence, dating violence, sexual assault, or stalking.

Requires the Attorney General to direct the Internet Crime Complaint Center to provide education and awareness information to the public and law enforcement and register complaints regarding the abuse of geolocation information to commit domestic violence, dating violence, sexual assault, stalking, or other related crimes. Authorizes the Director of the Office on Violence Against Women to make grants to develop and provide training relating to investigating and

prosecuting the misuse of geolocation information in the commission of such crimes.

Actions Timeline

- **Jun 4, 2014:** Committee on the Judiciary Subcommittee on Privacy, Technology and the Law. Hearings held.
- **Mar 27, 2014:** Introduced in Senate
- **Mar 27, 2014:** Read twice and referred to the Committee on the Judiciary.

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