

HR 656

Online Communications and Geolocation Protection Act

Congress: 114 (2015–2017, Ended)

Chamber: House

Policy Area: Crime and Law Enforcement

Introduced: Feb 2, 2015

Current Status: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

Latest Action: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. (Mar 17, 2015)

Official Text: <https://www.congress.gov/bill/114th-congress/house-bill/656>

Sponsor

Name: Rep. Lofgren, Zoe [D-CA-19]

Party: Democratic • **State:** CA • **Chamber:** House

Cosponsors (11 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Conyers, John, Jr. [D-MI-13]	D · MI		Feb 2, 2015
Rep. DelBene, Suzan K. [D-WA-1]	D · WA		Feb 2, 2015
Rep. Farenthold, Blake [R-TX-27]	R · TX		Feb 2, 2015
Rep. Massie, Thomas [R-KY-4]	R · KY		Feb 2, 2015
Rep. O'Rourke, Beto [D-TX-16]	D · TX		Feb 2, 2015
Rep. Poe, Ted [R-TX-2]	R · TX		Feb 2, 2015
Rep. Polis, Jared [D-CO-2]	D · CO		Feb 2, 2015
Rep. Sensenbrenner, F. James, Jr. [R-WI-5]	R · WI		Feb 2, 2015
Rep. Swalwell, Eric [D-CA-15]	D · CA		Feb 2, 2015
Rep. Huffman, Jared [D-CA-2]	D · CA		Mar 26, 2015
Rep. Sanford, Mark [R-SC-1]	R · SC		Apr 27, 2016

Committee Activity

Committee	Chamber	Activity	Date
Intelligence (Permanent Select) Committee	House	Referred To	Feb 2, 2015
Judiciary Committee	House	Referred to	Mar 17, 2015

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
114 HR 491	Related bill	Feb 19, 2015: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
114 S 237	Related bill	Jan 22, 2015: Read twice and referred to the Committee on the Judiciary.

Summary (as of Feb 2, 2015)

Online Communications and Geolocation Protection Act

Amends the federal criminal code to authorize a governmental entity to require the disclosure of the contents of any wire or electronic communication that is stored, held, or maintained by an electronic communication service or a remote computing service only pursuant to a warrant. Requires such entity, within three days after it receives such contents from a provider of such service, to serve upon or deliver to the service subscriber, customer, or user a copy of the warrant and required notice. Includes the contents of such a communication among the information that any such service provider shall not knowingly divulge to any governmental entity except as provided under current law.

Prohibits a governmental entity from intentionally intercepting geolocation information pertaining to an individual, or from intentionally disclosing or using such information knowing that it was obtained in violation of existing prohibitions, except: (1) for purposes of electronic surveillance authorized by the Foreign Intelligence Surveillance Act of 1978 (FISA); (2) with the consent of the individual to whom the information pertains or the parent or guardian of a child to whom the information pertains; (3) through any system that is configured so that such information is readily accessible to the general public; (4) by an emergency responder to respond to a request by such individual for assistance or in circumstances in which it is reasonable to believe that individual's life or safety is in jeopardy; (5) pursuant to a warrant issued by a court in accordance with the Federal Rules of Criminal Procedure or as otherwise provided in FISA; or (6) by an investigative or law enforcement officer specially designated to intercept or use geolocation information if such officer reasonably determines that an emergency situation (involving immediate danger of death or serious physical injury to any individual or conspiratorial activities that threaten the national security interest or that are characteristic of organized crime) exists and requires interception or use before an authorizing order can be obtained, there are grounds upon which such an order could be entered, and an application for such order is made within 48 hours after the interception or use occurs.

Prohibits a service provider from intentionally disclosing geolocation information pertaining to an individual to any governmental entity, except: (1) pursuant to the above exceptions, or (2) to disclose to a law enforcement agency information which was inadvertently obtained and which appears to pertain to the commission of a crime.

Prohibits the use of any geolocation information intercepted, used, or disclosed in violation of this Act as evidence in any trial, hearing, or other government proceeding, except in a civil action to obtain relief for a violation of this Act.

Authorizes civil actions to recover damages from persons, other than the United States, where an individual's geolocation information is intentionally disclosed or used in violation of this Act. Requires a federal agency to initiate proceedings to determine whether disciplinary action is warranted against any federal employee when a court or agency has determined that the United States has violated this Act.

Amends the Federal Rules of Criminal Procedure to require a search warrant to obtain geolocation information.

Prohibits obtaining the geolocation information of a person for protective activities or law enforcement or intelligence purposes except pursuant to a warrant issued pursuant to the Federal Rules of Criminal Procedure, this Act, or FISA.

Actions Timeline

- **Mar 17, 2015:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Feb 2, 2015:** Introduced in House
- **Feb 2, 2015:** Referred to the Committee on the Judiciary, and in addition to the Committee on Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

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