HR 6529

ECPA 2.0 Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: House
Policy Area: Crime and Law Enforcement
Introduced: Sep 21, 2012
Current Status: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
Latest Action: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security. (Oct 3, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/house-bill/6529

Sponsor

Name: Rep. Lofgren, Zoe [D-CA-16]
Party: Democratic • **State:** CA • **Chamber:** House

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Intelligence (Permanent Select) Committee	House	Referred To	Sep 21, 2012
Judiciary Committee	House	Referred to	Oct 3, 2012

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
112 HR 2168	Related bill	**May 17, 2012:** Subcommittee Hearings Held.
112 S 1212	Related bill	**Jun 15, 2011:** Read twice and referred to the Committee on the Judiciary.

Summary (as of Sep 21, 2012)

ECPA 2.0 Act of 2012 - 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 such prohibition or in connection with a criminal investigation, with specified exceptions. Includes among such exceptions: (1) interception by a U.S. employee in conducting electronic surveillance authorized by the Foreign Intelligence Surveillance Act of 1978 (FISA), (2) interception with the individual's consent, (3) interception through any system that is configured so that such information is readily accessible to the general public, (4) interception and use 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 threatened, and (5) interception or required disclosure pursuant to a warrant issued by a court in accordance with the Federal Rules of Criminal Procedure or as otherwise provided in FISA.

Prohibits: (1) a service provider from intentionally divulging geolocation information to any governmental entity, except pursuant to the above exceptions or to divulge to a law enforcement agency information which was inadvertently obtained and which appears to pertain to the commission of a crime; or (2) the use of any geolocation information intercepted, used, or disclosed in violation of this Act as evidence in any trial or other government proceeding.

Permits a specially designated investigative or law enforcement officer to intercept geolocation information if: (1) such officer reasonably determines that an emergency situation exists that involves 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, (2) there are grounds upon which an order could be entered to authorize such interception, and (3) an application for such order is made within 48 hours after the interception.

Authorizes civil actions to recover damages from persons, other than the United States, where an individual's geolocation information is intercepted, disclosed, or intentionally 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 acquire geolocation information.

Prohibits: (1) intentionally obtaining by fraud confidential GPS records from any geolocation information service; or (2) acquiring 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.

Requires an application for an order for a wiretap to include a statement of facts relied upon by the applicant to justify issuance of the order. Authorizes the court to issue such an order if it finds that the application establishes specific and articulable facts showing reasonable grounds to believe that the information likely to be obtained is relevant to an ongoing criminal investigation.

Requires a service provider to disclose subscriber, customer, or user information to a governmental entity pursuant to an

administrative subpoena only when that subpoena specifies the person whose information is sought by name, address, telephone or instrument number, subscriber number, or other uniquely identifying information.

Actions Timeline

- **Oct 3, 2012:** Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
- **Sep 21, 2012:** Introduced in House
- **Sep 21, 2012:** 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.