HR 1913

APPS Act of 2013

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: May 9, 2013
Current Status: Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
Latest Action: Referred to the Subcommittee on Commerce, Manufacturing, and Trade. (May 10, 2013)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/1913

Sponsor

Name: Rep. Johnson, Henry C. "Hank," Jr. [D-GA-4]
Party: Democratic • **State:** GA • **Chamber:** House

Cosponsors (8 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Chabot, Steve [R-OH-1]	R · OH		May 9, 2013
Rep. Conyers, John, Jr. [D-MI-13]	D · MI		May 9, 2013
Rep. Engel, Eliot L. [D-NY-16]	D · NY		May 9, 2013
Rep. Jackson Lee, Sheila [D-TX-18]	D · TX		May 9, 2013
Rep. Barton, Joe [R-TX-6]	R · TX		May 22, 2013
Rep. Cohen, Steve [D-TN-9]	D · TN		Jul 17, 2013
Rep. Duffy, Sean P. [R-WI-7]	R · WI		Mar 13, 2014
Rep. Enyart, William L. [D-IL-12]	D · IL		Jul 31, 2014

Committee Activity

Committee	Chamber	Activity	Date
Energy and Commerce Committee	House	Referred to	May 10, 2013

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of May 9, 2013)

Application Privacy, Protection, and Security Act of 2013 or the APPS Act of 2013 - Directs mobile device application developers, before the application collects personal data about the user, to notify the user and obtain the user's consent regarding the terms and conditions governing the collection, use, storage, and sharing of such personal data.

Excludes from such notice and consent requirements any "de-identified data" that cannot reasonably be used to identify or infer information about, or otherwise be linked to, a particular individual or mobile device, as determined with a reasonable level of justified confidence based on the available methods and technologies, the nature of the data at issue, and the purposes for which the data will be used.

Requires developers to: (1) provide users with a method to withdraw such consent and to request that the developer delete personal data or refrain from further data collection or sharing, and (2) take measures to prevent unauthorized access to personal and de-identified data.

Requires violations to be treated as unfair or deceptive acts or practices under the Federal Trade Commission Act.

Directs the Federal Trade Commission (FTC) to promulgate regulations to implement and enforce this Act.

Authorizes states to bring civil actions in federal court on behalf of affected state residents.

Declares that nothing in this Act prohibits a developer from disclosing or preserving personal data or de-identified data as required by other federal laws or, except when superceded by this Act, the laws of a state or political subdivision, including court orders.

Permits a developer to satisfy the requirements of this Act by adopting and following a code of conduct for consumer data privacy that: (1) was developed in a multistakeholder process convened by the National Telecommunications and Information Administration (NTIA), as described in the document issued by the President on February 23, 2012, entitled Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy; and (2) is approved pursuant to FTC regulations.

Actions Timeline

- **May 10, 2013:** Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
- **May 9, 2013:** Introduced in House
- **May 9, 2013:** Sponsor introductory remarks on measure. (CR H2558)
- **May 9, 2013:** Referred to the House Committee on Energy and Commerce.