HR 135

Cyber Privacy Fortification Act of 2017

Congress: 115 (2017–2019, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: Jan 3, 2017
Current Status: Referred to the Subcommittee on Regulatory Reform, Commercial And Antitrust Law.
Latest Action: Referred to the Subcommittee on Regulatory Reform, Commercial And Antitrust Law. (Jan 12, 2017)
Official Text: https://www.congress.gov/bill/115th-congress/house-bill/135

Sponsor

Name: Rep. Conyers, John, Jr. [D-MI-13]
Party: Democratic • **State:** MI • **Chamber:** House

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Johnson, Henry C. "Hank," Jr. [D-GA-4]	D · GA		Jan 3, 2017

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	House	Referred to	Jan 12, 2017
Judiciary Committee	House	Referred to	Jan 12, 2017

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Jan 3, 2017)

Cyber Privacy Fortification Act of 2017

This bill amends the federal criminal code to provide criminal penalties for intentional failures to provide required notices regarding security breaches of computerized data that there is reason to believe resulted in improper access to specified sensitive personally identifiable information that is electronic or digital.

A person who owns or possesses data in electronic form containing a means of identification, and who has knowledge of a major security breach of the system containing such data, must notify the U.S. Secret Service or the Federal Bureau of Investigation.

A "major security breach" involves: (1) a means of identification pertaining to at least 10,000 individuals that is reasonably believed to have been acquired, (2) databases owned by the federal government, or (3) a means of identification of federal employees or contractors involved in national security matters or law enforcement.

The Department of Justice and state attorneys general may bring civil actions and obtain injunctive relief for violations of federal laws relating to data security.

Federal agencies must prepare and make available to the public privacy impact assessments that describe the impact of certain proposed and final agency rules on the privacy of individuals. Agencies may waive or delay certain privacy impact assessment requirements for emergencies and national security reasons.

Federal agencies must: (1) periodically review promulgated rules that have a significant privacy impact on individuals or a privacy impact on a substantial number of individuals, and (2) consider whether each such rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes.

The bill provides access to judicial review to individuals adversely affected or aggrieved by final agency action on any such rule.

Actions Timeline

- **Jan 12, 2017:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Jan 12, 2017:** Referred to the Subcommittee on Regulatory Reform, Commercial And Antitrust Law.
- **Jan 3, 2017:** Introduced in House
- **Jan 3, 2017:** Referred to the House Committee on the Judiciary.