S 1535

Personal Data Protection and Breach Accountability Act of 2011

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Commerce
Introduced: Sep 8, 2011
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 182.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 182. (Sep 22, 2011)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/1535

Sponsor

Name: Sen. Blumenthal, Richard [D-CT]
Party: Democratic • **State:** CT • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Franken, Al [D-MN]	D · MN		Sep 21, 2011

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	Senate	Reported By	Sep 22, 2011

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

Bill	Relationship	Last Action
112 S 1408	Related bill	**Feb 6, 2012:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 310.
112 S 1151	Related bill	**Nov 7, 2011:** By Senator Leahy from Committee on the Judiciary filed written report. Report No. 112-91. Additional and Minority views filed.

Summary (as of Sep 22, 2011)

Personal Data Protection and Breach Accountability Act of 2011 - **Title I: Enhancing Punishment for Identity Theft and Other Violations of Data Privacy and Security** - (Sec. 101) Amends the federal criminal code to impose a fine and/or prison term of up to five years for intentionally or willfully concealing a security breach involving sensitive personally identifiable information when such breach results in economic harm or substantial emotional distress to one or more persons.

(Sec. 102) Makes it unlawful for a service provider, as defined by this Act, to knowingly or intentionally redirect web searches or otherwise monitor, manipulate, aggregate, and market data from websites without the consent of the Internet user. Imposes a civil fine of up to $500,000 for a violation of this provision and an increased fine of up to $1 million for engaging in a pattern or practice of activity that violates this provision.

Title II: Privacy and Security of Sensitive Personally Identifiable Information - Subtitle A: Data Privacy and Security Program - (Sec. 201) Makes any interstate business entity that collects, accesses, transmits, uses, stores, or disposes of sensitive personally identifiable information on 10,000 or more U.S. persons subject to the requirements for a data privacy and security program under this Act. Exempts public records not otherwise subject to a confidentiality or nondisclosure requirement, certain financial institutions subject to the Gramm-Leach-Bliley Act, business entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and service providers exclusively engaged in the transmission, routing, or storage of data.

(Sec. 202) Requires business entities that are subject to personal data privacy and security requirements of this Act to implement a comprehensive program that: (1) ensures the privacy, security, and confidentiality of sensitive personally identifiable information; (2) protects against any anticipated vulnerabilities to the privacy, security, or integrity of such information; and (3) protects against unauthorized access to such information that could create a significant risk of harm.

Requires such entities to: (1) assess risks of future security breaches and design a personal data privacy and security program to control such risks; (2) ensure employee training for implementing a security program; (3) ensure regular testing of key controls, systems, and procedures of such program; and (4) monitor, evaluate, and adjust the security program to reflect relevant changes in technology and other considerations.

(Sec. 203) Authorizes the Attorney General to bring a civil action or request injunctive relief against any business entity that violates the requirements of this subtitle and obtain fines against such entity for violations, including enhanced penalties for intentional or willful violations.

(Sec. 204) Authorizes a state attorney general to bring a civil action or request injunctive relief against a business entity that adversely threatens or affects the residents of the state by violating the requirements of this subtitle.

(Sec. 205) Allows individuals aggrieved by a violation of the data privacy and security requirements of this subtitle to bring a civil action to recover for personal injuries sustained as a result of such violation. Allows punitive damages against a business entity that intentionally or willfully violates the provisions of this subtitle.

Subtitle B: Security Breach Notification - (Sec. 211) Requires any agency or interstate business entity that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information to notify without unreasonable delay any U.S. resident whose information has been, or is reasonably believed to have been, accessed or acquired. Allows a federal law enforcement agency or member of the intelligence community to delay notification if it determines that such notification would impede a lawful criminal investigation or authorized intelligence activity.

(Sec. 212) Exempts an agency or business entity from the notification requirement if: (1) the U.S. Secret Service or the Federal Bureau of Investigation (FBI) determines that notification of a security breach would reveal sensitive sources, impede law enforcement investigations, or cause damage to national security; or (2) the agency or entity conducts a risk assessment in consultation with the Federal Trade Commission (FTC) and concludes that there is no significant risk of a security breach and the FTC does not act to deny an exemption. Exempts from the requirements of this subtitle certain financial institutions subject to the Gramm-Leach-Bliley Act and business entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

(Sec. 213) Sets forth the method of notice required for informing individuals of a security breach, including written notice to the last known home mailing address or email address of such individuals and public notice by electronic means or by general media if the sensitive personally identifiable information of more than 5,000 individuals is involved.

(Sec. 214) Establishes requirements for the content of a notice to an individual whose sensitive personally identifiable information has been breached, including a description of the categories of such information, contact information, and a notice that such individual is entitled to a free consumer credit report on a quarterly basis for two years.

(Sec. 215) Requires an agency or business entity that is required to provide notice of a security breach to provide at no cost to an individual whose sensitive personally identifiable information was breached a consumer credit report on a quarterly basis for a two-year period, a credit monitoring service, a security freeze on the individual's credit report, and compensation for damages incurred by an individual resulting from the security breach.

(Sec. 216) Requires any agency or business entity that is required to notify more than 5,000 individuals of a security breach to also notify consumer credit reporting agencies without unreasonable delay.

(Sec. 217) Requires the Secretary of Homeland Security (DHS), in consultation with the Attorney General, to designate a federal entity (designated entity) to receive information and reports about information security incidents, threats, and vulnerabilities. Requires the designated entity to provide such information to the Secret Service, to the FBI, to the FTC for civil law enforcement purposes, and to other federal agencies for law enforcement, national security, or data security purposes. Requires business entities and agencies to notify the designated entity of a security breach within 10 days of discovery.

(Sec. 218) Authorizes the Attorney General to bring a civil action or request injunctive relief against any business entity that violates the requirements of this subtitle. Grants the FTC authority for enforcing compliance with the requirements of this subtitle.

(Sec. 219) Authorizes a state attorney general to bring a civil action or request injunctive relief against a business entity that adversely threatens or affects the residents of the state by violating the requirements of this subtitle.

(Sec. 220) Allows individuals aggrieved by a violation of the notice requirements of this subtitle to bring a civil action to recover for personal injuries sustained as a result of such violation or obtain injunctive relief. Allows punitive damages against a business entity that intentionally or willfully violates the provisions of this subtitle.

(Sec. 221) Provides that the provisions of this subtitle supersede other provisions of federal or state law relating to notification, but do not exempt any entity from liability under common law for damages caused by failure to notify an individual following a security breach.

(Sec. 222) Authorizes appropriations to the Secret Service to carry out investigations and risk assessments of security

breaches.

(Sec. 223) Requires the Secret Service and the FBI to report to Congress, not later than 18 months after the enactment of this Act, on the number and nature of the security breaches described in notices filed by entities seeking a risk assessment exemption and the response of the Secret Service and FBI to such notices.

Subtitle C: Post-Breach Technical Information Clearinghouse - (Sec. 230) Requires the entity designated by DHS under this Act to maintain a clearinghouse of technical information concerning system vulnerabilities identified in the wake of security breaches. Allow agencies and business entities that are certified to review information in the clearinghouse to access such information to improve the security and reduce the vulnerability of networks that contain sensitive personally identifiable information.

(Sec. 231) Requires the DHS designated entity to ensure that: (1) technical information disclosed to it is stored in a format designed to protect proprietary business information from inadvertent disclosure; and (2) all information stored in the technical information clearinghouse is presented in a form that minimizes the potential for such information to be traced to a particular network, company, or security breach incident. Exempts information in the technical information clearinghouse from disclosure under the Freedom of Information Act.

Title III: Access to and Use of Commercial Data - (Sec. 301) Requires the Administrator of the General Services Administration (GSA), in considering contract awards totaling more than $500,000, to evaluate: (1) the data privacy and security program of a data broker and the broker's compliance with such program, (2) the extent to which databases and systems have been compromised by security breaches, and (3) data broker responses to such breaches. Defines a "data broker" as a business entity that regularly collects, transmits, or provides access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity for purposes of providing such information to non-affiliated third parties on an interstate basis.

(Sec. 302) Requires federal agencies to: (1) evaluate and audit the information security practices of contractors or third party business entities that support the information systems or operations of such agencies involving sensitive personally identifiable information, and (2) ensure remedial action to address any significant deficiencies.

(Sec. 303) Requires federal agencies to conduct a privacy impact assessment before purchasing or subscribing to personally identifiable information from a data broker. Requires the Comptroller General to study and report on federal agency adherence to key privacy principles in using data brokers of commercial databases containing sensitive personally identifiable information.

(Sec. 304) Requires the FBI, in coordination with the Secret Service, to submit to the Judiciary Committees of Congress within one year after the enactment of this Act a report on any reported security breaches at agencies or business entities during the preceding year.

(Sec. 305) Requires the Attorney General to submit annual reports to Congress on federal, state, and private enforcement of this Act with recommendations for increasing the effectiveness of such enforcement actions.

(Sec. 306) Requires the FBI, in coordination with the Attorney General and the FTC to report to the Judiciary Committees of Congress within one year after the enactment of this Act on the effectiveness of post-breach notification practices by agencies and business entities.

Title IV: Compliance with Statutory Pay-As-You-Go Act - (Sec. 401) Provides for compliance of the budgetary effects

of this Act with the Statutory Pay-As-You-Go Act of 2010.

Actions Timeline

- **Sep 22, 2011:** Committee on the Judiciary. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Sep 22, 2011:** Committee on the Judiciary. Reported by Senator Leahy with an amendment in the nature of a substitute. Without written report.
- **Sep 22, 2011:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 182.
- **Sep 8, 2011:** Introduced in Senate
- **Sep 8, 2011:** Read twice and referred to the Committee on the Judiciary.