S 1151

Personal Data Privacy and Security Act of 2011

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Crime and Law Enforcement
Introduced: Jun 7, 2011
Current Status: By Senator Leahy from Committee on the Judiciary filed written report. Report No. 112-91. Additional
Latest Action: By Senator Leahy from Committee on the Judiciary filed written report. Report No. 112-91. Additional and Minority views filed. (Nov 7, 2011)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/1151

Sponsor

Name: Sen. Leahy, Patrick J. [D-VT]
Party: Democratic • **State:** VT • **Chamber:** Senate

Cosponsors (4 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Cardin, Benjamin L. [D-MD]	D · MD		Jun 7, 2011
Sen. Franken, Al [D-MN]	D · MN		Jun 7, 2011
Sen. Schumer, Charles E. [D-NY]	D · NY		Jun 7, 2011
Sen. Blumenthal, Richard [D-CT]	D · CT		Sep 15, 2011

Committee Activity

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

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
112 S 2111	Related bill	**Feb 16, 2012:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 324.
112 S 1408	Related bill	**Feb 6, 2012:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 310.
112 S 1535	Related bill	**Sep 22, 2011:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 182.

Summary (as of Sep 22, 2011)

Personal Data Privacy and Security Act of 2011 - (Sec. 3) Defines "sensitive personally identifiable information" for purposes of this Act to include: (1) specified combinations of data elements in electronic or digital form, such as an individual's first and last name or first initial and last name in combination with home address or telephone number, mother's maiden name, and date of birth; (2) a non-truncated social security number, driver's license number, passport number, or government-issued unique identification number; (3) unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation; (4) a unique account identifier; and (5) any security code, access code, password, or secure code that could be used to generate such codes or passwords.

Title I: Enhancing Punishment for Identity Theft and Other Violations of Data Privacy and Security - (Sec. 101) Amends the federal criminal code to make fraud in connection with the unauthorized access of personally identifiable information (in electronic or digital form) a predicate for instituting a prosecution for racketeering.

(Sec. 102) Imposes a prison term of up to five years and/or a fine on any individual who has knowledge of and intentionally and willfully conceals a security breach and such breach results in economic harm of $1,000 or more to any individual. Grants the U.S. Secret Service and the Federal Bureau of Investigation (FBI) authority to investigate criminal concealments of security breaches.

(Sec. 103) Increases penalties for fraud and related activity in connection with computers.

(Sec. 104) Expands the prohibition against trafficking in passwords to include trafficking through any means by which a protected computer may be accessed without authorization.

(Sec. 105) Imposes criminal penalties for attempts and conspiracies to commit fraud and related activity in connection with computers.

(Sec. 106) Modifies criminal and civil forfeiture provisions, including requiring certain civil forfeiture seizures and forfeitures to be performed by persons designated for that purpose by the Secretary of Homeland Security (DHS) or the Attorney General (DOJ).

(Sec. 107) Prohibits civil actions involving unauthorized use of a protected computer if a violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, constitutes the sole basis for determining that access to the computer is unauthorized or in excess of authorization.

(Sec. 108) Directs the Attorney General to report the number of criminal cases that involve conduct in which: (1) the defendant exceeded authorized access to a nongovernmental computer or accessed a nongovernmental computer without authorization; and (2) the sole basis for such a determination was that the defendant violated a contractual obligation or agreement with a service provider or employer, such as an acceptable use policy or terms of service agreement.

(Sec. 109) Prohibits, during and in relation to a felony violation of provisions regarding fraud and related activity in connection with computers, intentionally causing or attempting to cause damage to a critical infrastructure computer if such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment of the operation of that computer or of the critical infrastructure associated with the computer. Imposes a prison term of between 3 and 20 years, a fine, or both. Prohibits probation for any person convicted of such a violation. Provides for concurrent sentences under specified circumstances.

(Sec. 110) Excludes from the definition of "exceeds authorized access" for purposes of the prohibition against fraudulent use of computers, access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or nongovernment employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.

Title II: Privacy and Security of Personally Identifiable Information - Subtitle A: A Data Privacy and Security Program - (Sec. 201) States that the purpose of this subtitle is to ensure the establishment of standards for developing and implementing safeguards to protect the security of sensitive personally identifiable information.

Subjects a business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive information in electronic or digital form on 10,000 or more U.S. persons to the requirements for the data privacy and security program established by this subtitle.

Makes this subtitle inapplicable to: (1) financial institutions subject to the data security requirements and standards under the Gramm-Leach-Bliley Act; (2) specified entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA); (3) service providers for any electronic communication by a third-party to the extent that such provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication; and (4) public records not otherwise subject to a confidentiality or nondisclosure requirement.

Deems a business entity to be in compliance with the privacy and security program requirements of this subtitle if the entity complies with or provides protection equal to industry standards or standards widely accepted as an effective industry practice, as identified by the Federal Trade Commission (FTC), that are applicable to the type of sensitive information involved in the ordinary course of business of such entity.

(Sec. 202) Requires a business entity subject to this subtitle to comply with specified safeguards identified by the FTC in a rulemaking process for the protection of sensitive personally identifiable information.

Requires such entity to implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the entity and the nature and scope of its activities. Requires the program to be designed to: (1) ensure the privacy, security, and confidentiality of sensitive information; (2) protect against any anticipated vulnerabilities to the privacy, security, or integrity of such information; and (3) protect against unauthorized access to use of such information that could create a significant risk of harm or fraud to any individual.

Requires a business entity subject to the requirements of this subtitle to: (1) identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access, disclosure, use, or alteration of sensitive information or systems containing such information; (2) assess the likelihood of and potential damage from unauthorized access to, or disclosure, use, or alteration of, sensitive information; (3) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of sensitive information; (4) assess the vulnerability of sensitive information during destruction and disposal of such information, including through the disposal or retirement of hardware; (5) design its personal data privacy and security program to control risks; (6) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, and scope of activities of the business entity that control access to systems and facilities containing sensitive information; (7) establish a plan and procedures for minimizing the amount of sensitive information maintained by a business entity; and (8) take steps to ensure appropriate employee training and regular testing of key controls, systems, and procedures of the entity's personal data privacy and security program.

(Sec. 203) Imposes civil penalties upon business entities for violations of the requirements of this subtitle, up to $5,000 per violation per day, with a maximum of $500,000 per violation. Provides additional penalties for intentional or willful violations. Allows an injunction against a business entity to stop continuing violations of the requirements of this subtitle.

Grants authority to the FTC to enforce the requirements of this subtitle.

Authorizes state attorneys general and law enforcement agencies to bring civil actions to protect state residents against business entities that are violating the requirements of this subtitle. Requires states to give advance notice to the FTC of the filing of any civil action.

(Sec. 204) Preempts state laws relating to administrative, technical, and physical safeguards for the protection of personal information.

Subtitle B: Security Breach Notification - (Sec. 211) Requires any agency or business entity engaged in interstate commerce that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information to notify without unreasonable delay, after the discovery of a security breach, any U.S. resident whose information has been, or is reasonably believed to have been, accessed or acquired.

Allows the Secret Service or the FBI to delay notification of a security breach if such notification would impede a criminal investigation or harm national security.

Makes this subtitle inapplicable to: (1) financial institutions subject to the data security requirements and standards under the Gramm-Leach-Bliley Act, and (2) specified entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

(Sec. 212) Allows exemptions from security breach notification requirements if: (1) the Secret Service or the FBI determines that notification of the security breach could be expected to reveal sensitive sources and methods or similarly impede the government's ability to conduct law enforcement investigations, or (2) the FBI determines that notification of the breach could be expected to damage national security.

States that no non-constitutional cause of action shall lie in any court against a federal agency for acts relating to the exemption from notification for law enforcement or national security purposes under this title.

Provides that an agency or business entity shall be exempt from notice requirements if: (1) a risk assessment concludes that there is no significant risk that a security breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to the individuals whose sensitive information was subject to the security breach; (2) without unreasonable delay, but not later than 45 days after the discovery of the breach (unless extended by the FTC), the agency or entity notifies the FTC in writing of the results of the risk assessment and its decision to invoke the risk assessment exemption; and (3) the FTC does not indicate, within 10 business days from receipt of the decision, that notice should be given.

Provides that a business entity will be exempt from notice requirements if it utilizes or participates in a security program that: (1) effectively blocks the use of the sensitive information to initiate unauthorized financial transactions before they are charged to the individual's account, and (2) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(Sec. 213) Provides for individual notice by mail, telephone, and e-mail of a security breach and for notice to major media outlets serving a state or jurisdiction if a security breach involves more than 5,000 individuals.

(Sec. 214) Specifies the required content of a notification of a security breach under this subtitle, including the toll-free telephone numbers of the agencies or business entities involved, addresses for the major credit reporting agencies, and information about availability of victim protection assistance.

(Sec. 215) Requires an agency or business entity that is required to provide notification of a data security breach involving more than 5,000 individuals to also provide notification to credit reporting agencies.

(Sec. 216) Directs the DHS Secretary to designate a federal entity to receive the notices required under this subtitle. Requires business entities and federal agencies to report data security breaches to the designated entity if the breach involves: (1) more than 5,000 individuals, (2) a database that contains information about more than 500,000 individuals, (3) a federal government database, or (4) individuals known to be federal employees or contractors involved in national security or law enforcement. Requires the designated agency to report information it receives about security breaches to the Secret Service, FBI, and FTC for civil law enforcement purposes as promptly as possible, but either 72 hours before notice of a breach is required to be provided to an individual or not later than 10 days after the breach is discovered, whichever occurs first.

(Sec. 217) Authorizes the Attorney General and the FTC to bring civil and administrative actions against business entities for violations of this subtitle and to seek injunctive relief or civil penalties, including increased penalties for willful or intentional violations. Imposes limitations on such penalties.

(Sec. 218) Authorizes state attorneys general or state or local law enforcement agencies to bring a civil action on behalf of state residents who have been threatened or adversely affected by a business entity violating provisions of this subtitle and obtain injunctive relief or civil penalties. Requires a state attorney general bringing a civil action to provide written notice to the Attorney General who may then move to stay the action, move to consolidate all pending actions, intervene, and file petitions for appeal.

(Sec. 219) Provides that the security breach notification provisions of this subtitle supersede other provisions of federal law, with specified exceptions, and state laws relating to notification of a security breach.

(Sec. 220) Directs the FTC, not later than 18 months after the enactment of this Act, to report on the number and nature of the security breaches described in notices filed by business entities invoking the risk assessment exemption under this subtitle and their response to such notices.

Directs the Secret Service and FBI, not later than 18 months after the enactment of this Act, to report on the number and nature of security breaches subject to the national security and law enforcement exemptions under this subtitle. Excludes from such report the contents of any risk assessment provided to the Secret Service and the FBI under this subtitle.

Title III: Compliance with Statutory Pay-As-You-Go Act - Provides that the budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO Legislation" for this Act, provided that such statement has been submitted prior to the vote on passage.

Actions Timeline

- **Nov 7, 2011:** By Senator Leahy from Committee on the Judiciary filed written report. Report No. 112-91. Additional and Minority views filed.
- **Sep 22, 2011:** Committee on the Judiciary. Ordered to be reported with amendments 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. 181.
- **Sep 7, 2011:** Committee on the Judiciary. Hearings held. Hearings printed: S.Hrg. 112-126.
- **Jun 7, 2011:** Introduced in Senate
- **Jun 7, 2011:** Sponsor introductory remarks on measure. (CR S3544-3545)
- **Jun 7, 2011:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S3545-3552)