S 495

Personal Data Privacy and Security Act of 2007

Congress: 110 (2007–2009, Ended)
Chamber: Senate
Policy Area: Crime and Law Enforcement
Introduced: Feb 6, 2007
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 168.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 168. (May 23, 2007)
Official Text: https://www.congress.gov/bill/110th-congress/senate-bill/495

Sponsor

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

Cosponsors (7 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Feingold, Russell D. [D-WI]	D · WI		Feb 6, 2007
Sen. Sanders, Bernard [I-VT]	I · VT		Feb 6, 2007
Sen. Schumer, Charles E. [D-NY]	D · NY		Feb 6, 2007
Sen. Specter, Arlen [R-PA]	R · PA		Feb 6, 2007
Sen. Brown, Sherrod [D-OH]	D · OH		Feb 26, 2007
Sen. Cardin, Benjamin L. [D-MD]	D · MD		May 3, 2007
Sen. Obama, Barack [D-IL]	D · IL		Apr 1, 2008

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	Senate	Reported By	May 23, 2007

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

No related bills are listed.

Summary (as of May 23, 2007)

Personal Data Privacy and Security Act of 2007 **- Title I: Enhancing Punishment For Identity Theft And Other Violations Of Data Privacy and Security -** (Sec. 101) Amends the federal criminal code to add intentionally accessing a computer without authorization to the definition of racketeering activity.

(Sec. 102) Imposes a fine and/or prison term of up to five years for intentionally and willfully concealing a security breach involving sensitive personally identifiable information that causes economic damage to one or more persons. Defines "sensitive personally identifiable information" to include an individual's name in combination with his or her social security number, home address, date of birth, biometrics data, or financial account information.

(Sec. 103) Directs the U.S. Sentencing Commission to review and amend, if appropriate, federal sentencing guidelines for persons convicted of using fraud to access, or to misuse, digitized or electronic personally identifiable information, including sentencing guidelines for identity theft.

(Sec. 104) Amends the federal bankruptcy code to prohibit the dismissal or conversion of a bankruptcy case based upon a debtor's failure to meet means testing eligibility requirements if such debtor is a victim of identity theft.

Title II: Data Brokers - (Sec. 201) Requires interstate data brokers (defined as business entities which, for monetary fees or dues, regularly engage in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals to nonaffiliated third parties on an interstate basis) to: (1) disclose to a requesting individual all personal electronic records pertaining to such individual in their databases or systems at the time of such request; (2) provide guidance to such individuals for correcting inaccuracies in their records; (3) provide written or electronic notice of any adverse action taken against an individual by a third party based upon information in their databases; and (4) correct any inaccurate information in their databases.

(Sec. 202) Imposes civil penalties on data brokers who violate the requirements of this title. Grants the Federal Trade Commission (FTC) enforcement authority over data brokers. Allows state attorneys general to pursue civil remedies against data brokers who are deemed to pose a threat to state residents.

(Sec. 203) Preempts state regulation of data brokers.

(Sec. 204) Makes the provisions of this title effective 180 days after enactment of this Act.

Title III: Privacy And Security Of Personally Identifiable Information - Subtitle A: A Data Privacy and Security Program - (Sec. 301) Imposes requirements for a personal data privacy and security program on business entities that maintain sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons. Exempts certain financial institutions, covered entities under the Health Insurance Portability and Accountability Act (HIPAA), and public records from such requirements.

(Sec. 302) Requires a business entity that is subject to data privacy and security requirements to: (1) implement a comprehensive personal data privacy and security program to ensure the privacy, security, and confidentiality of sensitive personally identifying information and to protect against breaches of and unauthorized access to such information; (2) conduct risk assessments of potential security breaches; (3) adopt risk management and control policies and procedures; (4) ensure employee training and supervision for implementation of data security programs; and (5) undertake vulnerability testing and monitoring of personal data privacy and security programs.

(Sec. 303) Imposes civil penalties on business entities that violate the data privacy and security requirements of this subtitle. Grants enforcement authority for such requirements to the FTC.

(Sec. 304) Preempts state laws relating to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information.

Subtitle B: Security Breach Notification - (Sec. 311) Requires any agency or business entity with sensitive personally identifiable information to notify without unreasonable delay any U.S. resident of a security breach in which such resident's information has been, or is reasonably believed to have been, accessed or acquired.

(Sec. 312) Exempts agencies or business entities from security breach notification requirements if they provide written certification to the Secret Service that providing such notification would impede a criminal investigation or damage national security. Requires the Secret Service to evaluate the merits of such certifications.

(Sec. 313) Requires an agency or business entity to give notice of a security breach to any affected individuals: (1) by written notice to their last known home mailing address, by telephone, or by email (if email notification was consented to); and (2) to major media outlets if the number of residents in a state affected by a security breach exceeds 5,000.

(Sec. 314) Requires the notification to individuals whose sensitive personally identifiable information has been accessed to include: (1) a description of the categories of information an unauthorized individual has acquired; and (2) toll-free numbers for contacting the agency or business entity whose databases have been breached and major credit reporting agencies.

(Sec. 315) Requires any business entity or agency that is required to provide notification to more than 5,000 individuals of a security breach to notify all consumer reporting agencies.

(Sec. 316) Requires any business entity or agency to notify the Secret Service of security breaches of sensitive personally identifying information within 14 days of any data security breach that involves: (1) more than 10,000 individuals; (2) a database that contains information about more than one million individuals nationwide; (3) a federal government database; or (4) individuals known to be government employees or contractors involved in national security or law enforcement. Requires the Secret Service to notify the Federal Bureau of Investigation (FBI), the U.S. Postal Service, and the attorney general of each affected state of a security breach within 14 days of receiving notice of any breach.

(Sec. 317) Authorizes the Attorney General to bring a civil action, including an injunction, in a U.S. district court for violations of security breach notification requirements.

(Sec. 318) Allows state attorneys general to bring a civil action in a U.S. district court to enforce security breach notification requirements. Authorizes the Attorney General to stay, or intervene in, any state action.

(Sec. 319) Declares that the provisions of this subtitle shall supersede any other provision of federal or state law relating to notification by an interstate business entity or agency of a security breach.

(Sec. 320) Authorizes appropriations to the Secret Service to carry out investigations and risk assessments of security breaches.

(Sec. 321) Requires the Secret Service to report to Congress on security breaches resulting from risk assessment exemptions.

(Sec. 322) Makes the provisions of this subtitle effective 90 days after enactment of this Act.

Subtitle C: Office of Federal Identity Protection - Establishes in the FTC an Office of Federal Identity Protection to assist victims of identity theft. Authorizes appropriations for such Office for FY2008-FY2012.

Title IV: Government Access To And Use Of Commercial Data - (Sec. 401) Requires the Administrator of the General Services Administration (GSA), in awarding contracts totaling more than $500,000 to data brokers, to evaluate their data privacy and security programs, their compliance, the extent to which their databases and systems have been compromised by security breaches, and their responses to such breaches. Provides a compliance safe harbor for data brokers and penalties against data brokers for noncompliance with security breach notification requirements.

(Sec. 402) Requires federal agencies to audit and evaluate the information security practices of government contractors and third parties that support the information technology systems of such agencies.

(Sec. 403) Amends the E-Government Act of 2002 to require federal agencies that purchase or subscribe to personally identifiable information from a commercial entity to conduct privacy impact assessments on the use of those services.

Requires the Comptroller General to conduct a study and audit and prepare a report for submission to Congress on federal agency adherence to privacy principles in using data brokers or commercial databases containing personally identifiable information.

(Sec. 404) Requires the Department of Justice to designate a department-wide Chief Privacy Officer. Sets forth the duties and responsibilities of such Officer.

Actions Timeline

- **May 23, 2007:** Committee on the Judiciary. Reported by Senator Leahy with amendments. With written report No. 110-70. Additional views filed.
- **May 23, 2007:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 168.
- **May 3, 2007:** Committee on the Judiciary. Ordered to be reported with amendments favorably.
- **Feb 6, 2007:** Introduced in Senate
- **Feb 6, 2007:** Sponsor introductory remarks on measure. (CR S1628-1629)
- **Feb 6, 2007:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S1629-1635)