# S 1789

Personal Data Privacy and Security Act of 2005

**Congress:** 109 (2005–2007, Ended)
**Chamber:** Senate
**Policy Area:** Civil Rights and Liberties, Minority Issues
**Introduced:** Sep 29, 2005
**Current Status:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 297.
**Latest Action:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 297. (Nov 17, 2005)
**Official Text:** https://www.congress.gov/bill/109th-congress/senate-bill/1789

## Sponsor

**Name:** Sen. Specter, Arlen [R-PA]
**Party:** Republican • **State:** PA • **Chamber:** Senate

## Cosponsors (3 total)

| Cosponsor | Party / State | Role | Date Joined |
|---|---|---|---|
| Sen. Feingold, Russell D. [D-WI] | D · WI | | Sep 29, 2005 |
| Sen. Feinstein, Dianne [D-CA] | D · CA | | Sep 29, 2005 |
| Sen. Leahy, Patrick J. [D-VT] | D · VT | | Sep 29, 2005 |

## Committee Activity

| Committee | Chamber | Activity | Date |
|---|---|---|---|
| Judiciary Committee | Senate | Reported By | Nov 17, 2005 |

## Subjects & Policy Tags

**Policy Area:**

Civil Rights and Liberties, Minority Issues

## Related Bills

| Bill | Relationship | Last Action |
|---|---|---|
| 109 S 1332 | Related bill | **Jul 1, 2005:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 151. |

## Summary (as of Nov 17, 2005)

Personal Data Privacy and Security Act of 2005 - **Title I: Enhancing Punishment for Identity Theft and Other Violations of Data Privacy and Security** - (Sec. 101) Amends the Racketeer Influenced and Corrupt Organizations Act (RICO) to make fraud and related activity in connection with unauthorized access to sensitive personally identifiable information a predicate offense.

(Sec. 102) Amends the federal criminal code to prohibit a person having the obligation to provide notice of a security breach under this Act from concealing a breach that causes economic damage to one or more persons. Grants the U.S. Secret Service exclusive authority to investigate any such offense.

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

**Title II: Data Brokers** - (Sec. 201) Sets forth requirements for data brokers engaged in interstate commerce with respect to products or services offered to third parties that allow access to or use of sensitive personally identifiable information, with specified exceptions.

Requires such a broker, upon request and for a reasonable fee, to disclose to an individual: (1) all personal electronic records maintained specifically for disclosure to third parties that request information on that individual in the ordinary course of business; and (2) guidance on correcting inaccuracies. Requires a broker to correct disputed information in its systems that does not accurately and completely record the information available from a public record source or licensor or that is otherwise found to be incomplete or inaccurate.

(Sec. 202) Sets civil penalties of up to $1,000 per violation per day up to a maximum of $250,000 for violations of this title, with additional penalties for intentional or willful violations. Authorizes equitable relief. Authorizes the Federal Trade Commission (FTC) to enforce this title and provides for state enforcement. Provides that nothing in this title establishes a private cause of action against a data broker for violation of this title.

**Title III: Privacy and Security of Personally Identifiable Information - Subtitle A: A Data Privacy and Security Program** - (Sec. 301) Subjects a business entity engaged in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons (with specified exceptions) to the requirements of this title.

(Sec. 302) Requires such an entity to: (1) implement a comprehensive data privacy and security program that includes safeguards identified by the FTC for the protection of sensitive personally identifiable information; (2) identify vulnerabilities and assess damage that could result in unauthorized access, disclosure, use, or alteration of such information or systems containing such information; (3) assess the sufficiency of its safeguards to control risks from such access; and (4) assess the vulnerability of such information during its destruction and disposal, including through the disposal or retirement of hardware.

Requires each entity to design its personal program to control those risks and adopt measures that: (1) control access to systems and facilities containing sensitive personally identifiable information; (2) detect fraudulent, unlawful, or unauthorized access, disclosure, use or alteration of such information; (3) protect such information by encryption or other reasonable means; and (4) ensure that such information is properly destroyed and disposed of. Requires each entity to ensure regular testing of key controls, systems, and procedures.

Requires each entity to: (1) exercise due diligence in selecting and training service providers for responsibilities related to safeguarding such information; and (2) require those service providers to implement and maintain specified measures.

Requires each entity to monitor, evaluate, and adjust its data privacy and security program regularly in light of any relevant changes in technology, the sensitivity of (or threats to) personally identifiable information, and changes in business arrangements.

(Sec. 303) Sets daily and maximum civil penalties for violations by a business entity. Establishes additional penalties for intentional or willful violations. Provides for equitable relief. Provides for enforcement by the FTC and by states.

**Subtitle B: Security Breach Notification** - (Sec. 321) Requires any agency or any business entity engaged in interstate commerce that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information, upon discovering a security breach of such information, to notify, without unreasonable delay: (1) all U.S. residents whose sensitive personally identifiable information has been accessed or acquired; or (2) the owner or licensee of the information if that agency or entity does not own or license it. Authorizes delay of notification upon written notice from a federal law enforcement agency that the notification would impede a criminal investigation.

(Sec. 322) Makes notification requirements inapplicable (subject to specified limitations) to an agency that certifies that notification of a breach could cause damage to the national security or hinder a law enforcement investigation. Exempts an agency or business entity if: (1) it concludes and notifies the Secret Service that there is no significant risk that the security breach will result in harm to individuals and the Secret Service does not indicate that notice should be given; or (2) it uses a security program that blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the individual's account and that notifies affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(Sec. 323) Provides that an agency or business entity shall be in compliance with such requirements if it provides both individual notice and media notice.

(Sec. 324) Requires notice to include: (1) a description of the categories of sensitive personally identifiable information acquired by an unauthorized person; (2) a toll-free number that the individual may use to contact the agency or business entity to learn what types of personal information the agency or entity maintained; and (3) the toll-free telephone numbers and addresses for the major credit reporting agencies. Authorizes a state to require that a notice shall also include information regarding victim protection assistance provided by that state.

(Sec. 325) Directs an agency or business entity that is required to provide notification to more than 1,000 individuals to also notify all nationwide consumer reporting agencies of the timing and distribution of the notices.

(Sec. 326) Requires an agency or business entity to give notice of a security breach to the Secret Service if: (1) the number of individuals whose sensitive personally identifying information was acquired by an unauthorized person exceeds 10,000; (2) the breach involves a data system containing information on more than 1 million individuals nationwide; (3) the breach involves databases owned by the federal government; or (4) the breach involves primarily sensitive personally identifiable information of employees and contractors of the federal government involved in national security or law enforcement.

Makes the Secret Service responsible for notifying the attorney general of each state affected and the Federal Bureau of Investigation (FBI) or the U.S. Postal Inspection Service (as appropriate) not later than 14 days after discovering a breach.

(Sec. 327) Authorizes civil actions and injunctive actions by the Attorney General for violations. Amends the Fair Credit Reporting Act to authorize an extended fraud alert upon evidence that the consumer has received notice that his or her financial information has or may have been compromised.

(Sec. 328) Authorizes civil actions by state attorneys general.

(Sec. 329) Provides that this subtitle shall not: (1) supersede any other provision of federal law or of state law relating to notification of a security breach (with an exception); and (2) preclude any operation permitted under the Gramm-Leach-Bliley Act.

(Sec. 330) Authorizes appropriations to cover costs incurred by the Secret Service to carry out investigations and risk assessments of security breaches.

(Sec. 331) Directs the Secret Service to report to Congress on the number and nature of security breaches: (1) described in the notices filed by those business entities invoking the risk assessment exemption; and (2) subject to the national security and law enforcement exemptions.

**Title IV: Government Access To and Use of Commercial Data** - (Sec. 401) Directs the Administrator of the General Services Administration (GSA), in considering contract awards totaling more than $500,000 with data brokers, to evaluate the broker's information privacy and security program. Deems a broker's program to be sufficient if the broker complies with or provides protection equal to applicable industry standards identified by the FTC.

Requires the GSA Administrator, in awarding contracts with data brokers for products or services related to access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, to: (1) include specified penalties; and (2) require the broker to exercise due diligence to require its service providers to implement and maintain specified information safeguards.

(Sec. 402) Requires each agency's information security program to include procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the agency's information systems or operations involving personally identifiable information and ensuring remedial action to address any significant deficiencies.

(Sec. 403) Amends the E-Government Act of 2002 to require an agency to take specified actions, including conducting a privacy impact assessment, before purchasing or subscribing for a fee to personally identifiable information from a data broker. Prohibits a federal agency from entering into a contract with a data broker to access any database consisting primarily of personally identifiable information concerning U.S. persons (other than news reporting or telephone directories) unless the head of such agency: (1) completes a privacy impact assessment; (2) adopts regulations specifying the personnel permitted to use such databases; and (3) incorporates into the agreement totaling more than $500,000 specified provisions regarding penalties and responsibilities related to such information.

Directs the Comptroller General to report on federal agency use of data brokers or commercial databases containing personally identifiable information.

(Sec. 404) Requires the Department of Justice (DOJ) to designate a department-wide Chief Privacy Officer. Directs that Officer to: (1) oversee DOJ's implementation of requirements to conduct privacy impact assessments of the use of commercial data containing personally identifiable information; and (2) coordinate with the Privacy and Civil Liberties Oversight Board.

## Actions Timeline

- **Nov 17, 2005:** Committee on the Judiciary. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Nov 17, 2005:** Committee on the Judiciary. Reported by Senator Specter with an amendment in the nature of a substitute. Without written report.
- **Nov 17, 2005:** Committee on the Judiciary. Reported by Senator Specter with an amendment in the nature of a substitute. Without written report.
- **Nov 17, 2005:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 297.
- **Oct 27, 2005:** Committee on the Judiciary. Committee consideration and Mark Up Session held.
- **Oct 20, 2005:** Committee on the Judiciary. Committee consideration and Mark Up Session held.
- **Sep 29, 2005:** Introduced in Senate
- **Sep 29, 2005:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S10725-10734)