HR 3990

Personal Data Privacy and Security Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Crime and Law Enforcement
Introduced: Feb 4, 2014
Current Status: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
Latest Action: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. (Mar 20, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/3990

Sponsor

Name: Rep. Shea-Porter, Carol [D-NH-1]
Party: Democratic • **State:** NH • **Chamber:** House

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Budget Committee	House	Referred To	Feb 4, 2014
Energy and Commerce Committee	House	Referred to	Feb 7, 2014
Financial Services Committee	House	Referred To	Feb 4, 2014
Judiciary Committee	House	Referred to	Mar 20, 2014
Oversight and Government Reform Committee	House	Referred To	Feb 4, 2014

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
113 S 1897	Identical bill	**Jan 8, 2014:** Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S134-142)

Summary (as of Feb 4, 2014)

Personal Data Privacy and Security Act of 2014 - Defines "sensitive personally identifiable information" to include: (1) specified combinations of data elements in electronic or digital form, such as an individual's name, 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; (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 - 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.

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 Secret Service and the Federal Bureau of Investigation (FBI) authority to investigate criminal concealments of security breaches.

Increases penalties for fraud and related activity, and imposes criminal penalties for attempts and conspiracies to commit fraud and related activity, in connection with computers.

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

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).

Prohibits civil actions involving unauthorized use of a protected computer if a violation of a contractual obligation or agreement constitutes the sole basis for determining that access to the computer is unauthorized.

Directs the Attorney General to report the number of criminal cases that involve: (1) unauthorized access to a nongovernmental computer, and (2) conduct in which the sole basis for such a determination was that the defendant violated a contractual obligation or agreement with a service provider or employer.

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 or would have resulted in the substantial impairment of the operation of that computer or associated critical infrastructure.

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 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 - 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 title. Excepts: (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 such requirements if the entity complies with or provides protection equal to industry standards or standards widely accepted as an effective industry practice that are applicable to the type of sensitive information involved in the ordinary course of business.

Requires a business entity subject to this title to: (1) comply with specified safeguards identified by the FTC in a rulemaking process for the protection of sensitive personally identifiable information; and (2) 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 such program to be designed to: (1) ensure the privacy, security, and confidentiality of sensitive information; (2) protect against any anticipated vulnerabilities; 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 such a business entity to: (1) identify reasonably foreseeable 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 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; (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 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; 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.

Prescribes penalties for violations of such requirements. Allows an injunction against a business entity to stop continuing violations of the requirements of this subtitle.

Grants authority to the FTC to enforce such requirements. Authorizes state attorneys general and law enforcement agencies to bring civil actions to protect state residents against business entities that are violating such requirements. Preempts state laws relating to administrative, technical, and physical safeguards for the protection of personal information.

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 any U.S. resident whose information has been accessed or acquired without unreasonable delay after the discovery of a security breach.

Excepts: (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). Allows exemptions 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.

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 breach; (2) without unreasonable delay but not later than 45 days after the discovery of the breach, the agency or entity notifies the FTC of the results of the risk assessment and its decision to invoke the 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.

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. Specifies the required content of a security breach notification. Requires an agency or business entity that is required to provide notification of a breach involving more than 5,000 individuals to also provide notification to credit reporting agencies.

Directs the DHS Secretary to designate a federal entity to receive the notices. 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.

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.

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 title and to 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.

Directs the FTC to report on the number and nature of the security breaches described in notices filed by business entities invoking the risk assessment exemption and their response to such notices.

Directs the Secret Service and FBI to report on the number and nature of security breaches subject to the national security and law enforcement exemptions.

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

- **Mar 20, 2014:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Feb 7, 2014:** Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
- **Feb 4, 2014:** Introduced in House
- **Feb 4, 2014:** Referred to the Committee on the Judiciary, and in addition to the Committees on Energy and Commerce, Financial Services, Oversight and Government Reform, and the Budget, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.