LegiList
Congress, Made Clear.

Bill Fact Sheet – December 12, 2025
https://legilist.com
Bill page: https://legilist.com/bill/114/s/1158

S 1158

Consumer Privacy Protection Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: Senate
Policy Area: Crime and Law Enforcement
Introduced: Apr 30, 2015
Current Status: Read twice and referred to the Committee on the Judiciary. (Sponsor introductory remarks on measure:
Latest Action: Read twice and referred to the Committee on the Judiciary. (Sponsor introductory remarks on measure: CR S2577-2578) (Apr 30, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/senate-bill/1158

Sponsor

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

Cosponsors (5 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Blumenthal, Richard [D-CT]	D · CT		Apr 30, 2015
Sen. Franken, Al [D-MN]	D · MN		Apr 30, 2015
Sen. Markey, Edward J. [D-MA]	D · MA		Apr 30, 2015
Sen. Warren, Elizabeth [D-MA]	D · MA		Apr 30, 2015
Sen. Wyden, Ron [D-OR]	D · OR		Apr 30, 2015

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	Senate	Referred To	Apr 30, 2015

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
114 HR 2977	Identical bill	**Jul 29, 2015:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

Summary (as of Apr 30, 2015)

Consumer Privacy Protection Act of 2015

Establishes a criminal offense for concealment of a security breach of computerized data containing sensitive personally identifiable information that results in economic harm of $1,000 or more to any individual.

Authorizes the Department of Justice (DOJ) to commence a civil action to enjoin unauthorized persons or entities from accessing or transmitting computer commands commonly referred to as botnets that would impair the integrity or availability of 100 or more computers used by financial institutions or the federal government or that affect interstate or foreign commerce or communications during any one-year period, including by denying access to the computers, installing unwanted software, or obtaining information without authorization. Allows DOJ to enjoin the alienation or disposal of, or to seek restraining orders prohibiting the disposal of, property obtained as a result of such a violation.

Expands categories of money laundering offenses to include financial transactions involving the proceeds of unlawful manufacturing, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices.

Requires certain business entities that collect, use, access, transmit, store, or dispose of sensitive personally identifiable information in electronic or digital form of 10,000 or more U.S. persons during any 12-month period to implement a consumer privacy and data security program that complies with safeguards identified by the Federal Trade Commission (FTC).

Requires entities, following discovery of a security breach, to notify U.S. residents whose unencrypted personal information is reasonably believed to have been accessed or acquired. Sets forth special notification procedures for: (1) third party entities that maintain or process data in electronic form on behalf of another entity; and (2) certain providers of electronic data transmission, routing, storage, or network connection services.

Directs entities to notify a federal entity designated by the Department of Homeland Security (DHS) if a security breach involves: (1) the personal information of more than 5,000 individuals, (2) databases containing the personal information of more than 500,000 individuals nationwide, (3) federal databases, or (4) federal employees and contractors involved in national security or law enforcement. Requires the DHS-designated entity to provide the information it receives to: (1) the U.S. Secret Service or the Federal Bureau of Investigation for law enforcement purposes; and (2) other federal agencies for law enforcement, national security, or data security purposes. Establishes a process for DOJ to adjust the thresholds for law enforcement and national security notifications.

Requires notice of certain breaches to be provided to consumer reporting agencies and the FTC.

Exempts certain financial institutions, entities that comply with health record privacy laws, and electronic communication service providers from certain requirements of this Act.

Establishes civil penalties for violations of this Act and provides enforcement authority to the FTC, DOJ, and states.

Supersedes federal and state laws that are less stringent than the data security practices and breach notification standards required by this Act, but permits states to continue to enforce other consumer protection laws and to apply state laws regarding trespasses, contracts, torts, or fraud.

Actions Timeline

- **Apr 30, 2015:** Introduced in Senate
- **Apr 30, 2015:** Read twice and referred to the Committee on the Judiciary. (Sponsor introductory remarks on measure: CR S2577-2578)