S 2378

Commercial Privacy Bill of Rights Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: Senate
Policy Area: Commerce
Introduced: May 21, 2014
Current Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.
Latest Action: Read twice and referred to the Committee on Commerce, Science, and Transportation. (May 21, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/senate-bill/2378

Sponsor

Name: Sen. Menendez, Robert [D-NJ]
Party: Democratic • **State:** NJ • **Chamber:** Senate

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Referred To	May 21, 2014

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

Bill	Relationship	Last Action
113 HR 4711	Identical bill	**May 23, 2014:** Referred to the Subcommittee on Commerce, Manufacturing, and Trade.
113 S 1976	Related bill	**Jan 30, 2014:** Read twice and referred to the Committee on Commerce, Science, and Transportation.
113 HR 3481	Related bill	**Nov 15, 2013:** Referred to the Subcommittee on Communications and Technology.
113 S 1700	Related bill	**Nov 14, 2013:** Read twice and referred to the Committee on Commerce, Science, and Transportation.

Summary (as of May 21, 2014)

Title I: Commercial Privacy - Commercial Privacy Bill of Rights Act of 2014 - Directs the Federal Trade Commission (FTC) to initiate a rulemaking to require covered entities to carry out security measures to protect personally identifiable information, unique identifier information, and other information that may be used to identify a specific individual.

Defines "covered entity" as a person (a person, partnership, or corporation over which the FTC has authority under the Federal Trade Commission Act, a common carrier subject to the Communications Act of 1934, or a nonprofit organization) who collects, uses, transfers, or stores such information concerning more than 5,000 individuals during any consecutive 12-month period.

Directs the FTC to require covered entities to: (1) notify individuals of their practices regarding the collection, use, transfer, and storage of such information; (2) provide timely notice before implementing a material change in such practices; (3) offer individuals a mechanism to provide opt-in consent for any unauthorized use of such information or a third party's use for behavioral advertising or marketing; and (4) provide access to, and methods to correct, stored information.

Permits covered entities to execute contracts with service providers to collect, use, and store information on behalf of the covered entity.

Restricts covered entities to the collection of only as much information relating to an individual as reasonably necessary to: (1) process or enforce a transaction or deliver a requested service, including inventory management, financial reporting and accounting, planning, product or service improvement, forecasting, and customer support; (2) prevent or detect fraud or provide for a secure environment; (3) investigate a possible crime or comply with a law; (4) market or advertise to such individual if the information used for such marketing or advertising was collected directly by the covered entity; and (5) conduct internal operations and customer research, including the collection of information about Internet website visits and click-through rates to improve website navigation and the customer's experience.

Limits the duration of time that a covered entity is authorized to retain such information to only the period necessary to provide the transaction, deliver the service, or comply with a law. Restricts the use of retained information to the purpose for which it was collected or a reasonably related purpose.

Directs covered entities that contract to transfer information to third parties to prohibit such third parties from combining transferred information that is not personally identifiable with other information in order to identify the individual without the individual's opt-in consent.

Requires covered entities to attempt to establish procedures to ensure the accuracy of personally identifiable information that could be used to deny consumers benefits or cause significant harm.

Sets forth the circumstances under which a covered entity may be required to provide notice of a breach of security to: (1) U.S. citizens or residents whose personally identifiable information is reasonably believed to have been acquired or accessed, (2) the FTC, (3) third parties, (4) service providers, and (5) credit reporting agencies.

Exempts a covered entity from certain notice requirements if:

- the covered entity, following a breach of security, concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct; or

the covered entity participates in a security program that blocks the use of the personally identifiable information to initiate an unauthorized financial transaction before it is charged to the account of the individual and that notifies affected individuals after a security breach that resulted in attempted fraud or an attempted unauthorized transaction.

Requires a covered entity to notify a federal government entity designated by the Secretary of Homeland Security (DHS) if a breach of security involves: (1) the personally identifiable information of more than 10,000 individuals, (2) a database containing the personally identifiable information of more than 1 million individuals, (3) federal government databases, or (4) the personally identifiable information of federal employees or contractors involved in national security or law enforcement.

Directs the designated entity to provide each notice it receives to:

- the U.S. Secret Service;
- the Federal Bureau of Investigation (FBI);
- the FTC;
- the U.S. Postal Inspection Service, if mail fraud is involved;
- attorneys general of affected states; and
- appropriate federal agencies for law enforcement, national security, or data security purposes.

Sets forth enforcement provisions for the FTC, the Attorney General (DOJ), and states. Establishes civil penalties for state actions against covered entities that recklessly or repeatedly violate specified requirements.

Prohibits this title from being construed to provide a private right of action.

Directs the FTC to initiate a rulemaking to establish requirements for a nongovernmental organization to administer safe harbor programs under which participants are exempted from certain requirements of this title if they implement particular mechanisms that protect against unauthorized information uses and provide consumers a means of opting out of the transfer of specified information to third parties.

Title II: Online Privacy of Children - Do Not Track Kids Act of 2014 **-** Amends the Children's Online Privacy Protection Act of 1998 to apply the prohibitions against collecting personal information from children to online applications and mobile applications directed to children. Establishes additional privacy protections against the collection of personal or geolocation information from children and minors.

Revises the definition of:

- "operator" to include online and mobile applications (currently, only Internet websites and online services) and to make such definition apply specifically to operators and providers of such websites, services, or applications who, for commercial purposes, in interstate or foreign commerce, collect or maintain personal information from or about their users, allow another person to collect such personal information, or allow users of such websites, services, or applications to publicly disclose personal information; and
- "disclosure" to mean the release of personal information (currently, the release of personal information collected from a child in identifiable form).

Requires verifiable parental consent, under specified circumstances, for the collection, use, or disclosure of personal information of a child, including certain online contact information collected in response to a specific request from a child

when such information is used to contact a different child.

Prohibits, without verifiable parental consent in the case of a child or without consent of the minor in the case of a minor, an operator of a website, online service, online application, or mobile application directed to children or minors, or an operator having actual knowledge that personal information being collected is from children or minors, from: (1) using, disclosing to third parties, or compiling personal information collected from children or minors for targeted marketing purposes; and (2) collecting geolocation information in a manner that violates the regulations prescribed under this title.

Defines a "minor" as an individual over the age of 12 and under the age of 16.

Prohibits an operator from discontinuing service provided to a child or minor on the basis of a refusal, by the child's parent or the minor, to permit the further use or maintenance in retrievable form, or future collection, of certain personal or geolocation information from such individuals, to the extent that the operator is capable of providing such service without such information.

Requires an operator of a website, online service, online application, or mobile application directed to children or minors to treat all users as children or minors for purposes of this title, except as permitted by regulation.

Prohibits an operator of a website, online service, or such applications directed to minors from collecting personal information from minors unless such operator has adopted, and complies with, a Digital Marketing Bill of Rights for Teens that is consistent with the Fair Information Practices Principles established by this title.

Requires the FTC to promulgate regulations that require operators to implement mechanisms that permit a user to erase content submitted by such user that is publicly available through such websites, services, or applications and that contains or displays personal information of children or minors.

Sets forth enforcement provisions for the FTC, other federal agencies, and states.

Actions Timeline

- **May 21, 2014:** Introduced in Senate
- **May 21, 2014:** Read twice and referred to the Committee on Commerce, Science, and Transportation.