113TH CONGRESS
2D SESSION

S. 2378

To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 21, 2014

Mr. MENENDEZ introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

TITLE I—COMMERCIAL PRIVACY

SEC. 101. SHORT TITLE.

This title may be cited as the ''Commercial Privacy Bill of Rights Act of 2014''.

SEC. 102. FINDINGS.

The Congress finds the following:

(1) Personal privacy is worthy of protection through appropriate legislation.

(2) Trust in the treatment of personally identifiable information collected on and off the Internet is essential for businesses to succeed.

(3) Persons interacting with others engaged in interstate commerce have a significant interest in their personal information, as well as a right to control how that information is collected, used, stored, or transferred.

(4) Persons engaged in interstate commerce and collecting personally identifiable information on individuals have a responsibility to treat that infor-

mation with respect and in accordance with common standards.

(5) On the day before the date of the enactment of this Act, the laws of the Federal Government and State and local governments provided inadequate privacy protection for individuals engaging in and interacting with persons engaged in interstate commerce.

(6) As of the day before the date of the enactment of this Act, with the exception of Federal Trade Commission enforcement of laws against unfair and deceptive practices, the Federal Government has eschewed general commercial privacy laws in favor of industry self-regulation, which has led to several self-policing schemes, some of which are enforceable, and some of which provide insufficient privacy protection to individuals.

(7) As of the day before the date of the enactment of this Act, many collectors of personally identifiable information have yet to provide baseline fair information practice protections for individuals.

(8) The ease of gathering and compiling personal information on the Internet and off, both overtly and surreptitiously, is becoming increasingly efficient and effortless due to advances in technology

which have provided information gatherers the ability to compile seamlessly highly detailed personal histories of individuals.

(9) Personal information requires greater privacy protection than is available on the day before the date of the enactment of this Act. Vast amounts of personal information, including sensitive information, about individuals are collected on and off the Internet, often combined and sold or otherwise transferred to third parties, for purposes unknown to an individual to whom the personally identifiable information pertains.

(10) Toward the close of the 20th century, as individuals' personal information was increasingly collected, profiled, and shared for commercial purposes, and as technology advanced to facilitate these practices, Congress enacted numerous statutes to protect privacy.

(11) Those statutes apply to the government, telephones, cable television, e-mail, video tape rentals, and the Internet (but only with respect to children and law enforcement requests).

(12) As in those instances, the Federal Government has a substantial interest in creating a level playing field of protection across all collectors of per-

sonally identifiable information, both in the United States and abroad.

(13) Enhancing individual privacy protection in a balanced way that establishes clear, consistent rules, both domestically and internationally, will stimulate commerce by instilling greater consumer confidence at home and greater confidence abroad as more and more entities digitize personally identifiable information, whether collected, stored, or used online or offline.

SEC. 103. DEFINITIONS.

(a) IN GENERAL.—Subject to subsection (b), in this title:

(1) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(2) COVERED ENTITY.—The term ''covered entity'' means any person to whom this title applies under section 151.

(3) COVERED INFORMATION.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''covered information'' means only the following:

(i) Personally identifiable information.

(ii) Unique identifier information.

(iii) Any information that is collected, used, or stored in connection with personally identifiable information or unique identifier information in a manner that may reasonably be used by the party collecting the information to identify a specific individual.

(B) EXCEPTION.—The term ''covered information'' does not include the following:

(i) Personally identifiable information obtained from public records that is not merged with covered information gathered elsewhere.

(ii) Personally identifiable information that is obtained from a forum—

(I) where the individual voluntarily shared the information or authorized the information to be shared; and

(II) that—

(aa) is widely and publicly available and was not made publicly available in bad faith; and

(bb) contains no restrictions on who can access and view such information.

(iii) Personally identifiable information reported in public media.

(iv) Personally identifiable information dedicated to contacting an individual at the individual's place of work.

(4) ESTABLISHED BUSINESS RELATIONSHIP.—The term ''established business relationship'' means, with respect to a covered entity and a person, a relationship formed with or without the exchange of consideration, involving the establishment of an account by the person with the covered entity for the receipt of products or services offered by the covered entity.

(5) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means only the following:

(A) Any of the following information about an individual:

(i) The first name (or initial) and last name of an individual, whether given at birth or time of adoption, or resulting from a lawful change of name.

(ii) The postal address of a physical place of residence of such individual.

(iii) An e-mail address.

(iv) A telephone number or mobile device number.

(v) A social security number or other government issued identification number issued to such individual.

(vi) The account number of a credit card issued to such individual.

(vii) Unique identifier information that alone can be used to identify a specific individual.

(viii) Biometric data about such individual, including fingerprints and retina scans.

(B) If used, transferred, or stored in connection with 1 or more of the items of information described in subparagraph (A), any of the following:

(i) A date of birth.

(ii) The number of a certificate of birth or adoption.

(iii) A place of birth.

(iv) Unique identifier information that alone cannot be used to identify a specific individual.

(v) Precise geographic location, at the same degree of specificity as a global positioning system or equivalent system, and not including any general geographic information that may be derived from an Internet Protocol address.

(vi) Information about an individual's quantity, technical configuration, type, destination, location, and amount of uses of voice services, regardless of technology used.

(vii) Any other information concerning an individual that may reasonably be used by the party using, collecting, or storing that information to identify that individual.

(6) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means—

(A) personally identifiable information which, if lost, compromised, or disclosed without authorization either alone or with other in-

formation, carries a significant risk of economic or physical harm; or

(B) information related to—

(i) a particular medical condition or a health record; or

(ii) the religious affiliation of an individual.

(7) THIRD PARTY.—

(A) IN GENERAL.—The term ''third party'' means, with respect to a covered entity, a person that—

(i) is—

(I) not related to the covered entity by common ownership or corporate control; or

(II) related to the covered entity by common ownership or corporate control and an ordinary consumer would not understand that the covered entity and the person were related by common ownership or corporate control;

(ii) is not a service provider used by the covered entity to receive personally identifiable information or sensitive person-

ally identifiable information in performing services or functions on behalf of and under the instruction of the covered entity; and

(iii) with respect to the collection of covered information of an individual, does not have an established business relationship with the individual and does not identify itself to the individual at the time of such collection in a clear and conspicuous manner that is visible to the individual.

(B) COMMON BRANDS.—The term ''third party'' may include, with respect to a covered entity, a person who operates under a common brand with the covered entity.

(8) UNAUTHORIZED USE.—

(A) IN GENERAL.—The term ''unauthorized use'' means the use of covered information by a covered entity or its service provider for any purpose not authorized by the individual to whom such information relates.

(B) EXCEPTIONS.—Except as provided in subparagraph (C), the term ''unauthorized use'' does not include use of covered information re-

lating to an individual by a covered entity or its service provider as follows:

(i) To process and enforce a transaction or deliver a service requested by that individual.

(ii) To operate the covered entity that is providing a transaction or delivering a service requested by that individual, such as inventory management, financial reporting and accounting, planning, and product or service improvement or forecasting.

(iii) To prevent or detect fraud or to provide for a physically or virtually secure environment.

(iv) To investigate a possible crime.

(v) That is required by a provision of law or legal process.

(vi) To market or advertise to an individual from a covered entity within the context of a covered entity's own Internet website, services, or products if the covered information used for such marketing or advertising was—

(I) collected directly by the covered entity; or

(II) shared with the covered entity—

(aa) at the affirmative request of the individual; or

(bb) by an entity with which the individual has an established business relationship.

(vii) Use that is necessary for the improvement of transaction or service delivery through research, testing, analysis, and development.

(viii) Use that is necessary for internal operations, including the following:

(I) Collecting customer satisfaction surveys and conducting customer research to improve customer service information.

(II) Information collected by an Internet website about the visits to such website and the click-through rates at such website—

(aa) to improve website navigation and performance; or

(bb) to understand and improve the interaction of an indi-

vidual with the advertising of a covered entity.

(ix) Use—

(I) by a covered entity with which an individual has an established business relationship;

(II) which the individual could have reasonably expected, at the time such relationship was established, was related to a service provided pursuant to such relationship; and

(III) which does not constitute a material change in use or practice from what could have reasonably been expected.

(C) SAVINGS.—A use of covered information regarding an individual by a covered entity or its service provider may only be excluded under subparagraph (B) from the definition of ''unauthorized use'' under subparagraph (A) if the use is reasonable and consistent with the practices and purposes described in the notice given the individual in accordance with section 121(a)(1).

(9) UNIQUE IDENTIFIER INFORMATION.—The term ''unique identifier information'' means a unique persistent identifier associated with an individual or a networked device, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number.

(b) MODIFIED DEFINITION BY RULEMAKING.—If the Commission determines that a term defined in any of paragraphs (3) through (8) is not reasonably sufficient to protect an individual from unfair or deceptive acts or practices, the Commission may by rule modify such definition as the Commission considers appropriate to protect such individual from an unfair or deceptive act or practice to the extent that the Commission determines will not unreasonably impede interstate commerce.

Subtitle A—Right to Security and Accountability

SEC. 111. SECURITY.

(a) RULEMAKING REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to require each covered entity to carry out security measures to protect the covered information it collects and maintains.

(b) PROPORTION.—The requirements prescribed under subsection (a) shall provide for security measures

that are proportional to the size, type, nature, and sensitivity of the covered information a covered entity collects.

(c) CONSISTENCY.—The requirements prescribed under subsection (a) shall be consistent with guidance provided by the Commission and recognized industry practices for safety and security on the day before the date of the enactment of this Act.

(d) TECHNOLOGICAL MEANS.—In a rule prescribed under subsection (a), the Commission may not require a specific technological means of meeting a requirement.

SEC. 112. ACCOUNTABILITY.

Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information it collects—

(1) have managerial accountability, proportional to the size and structure of the covered entity, for the adoption and implementation of policies consistent with this title;

(2) have a process to respond to non-frivolous inquiries from individuals regarding the collection, use, transfer, or storage of covered information relating to such individuals; and

(3) describe the means of compliance of the covered entity with the requirements of this Act upon request from—

(A) the Commission; or

(B) an appropriate safe harbor program established under section 151.

SEC. 113. PRIVACY BY DESIGN.

Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information privacy program by—

(1) incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on—

(A) the reasonable expectations of such individuals regarding privacy; and

(B) the relevant threats that need to be guarded against in meeting those expectations; and

(2) maintaining appropriate management processes and practices throughout the data life cycle that are designed to ensure that information systems comply with—

(A) the provisions of this title;

(B) the privacy policies of a covered entity; and

(C) the privacy preferences of individuals that are consistent with the consent choices and related mechanisms of individual participation as described in section 122.

Subtitle B—Right to Notice and Individual Participation

SEC. 121. TRANSPARENT NOTICE OF PRACTICES AND PURPOSES.

(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to require each covered entity—

(1) to provide accurate, clear, concise, and timely notice to individuals of—

(A) the practices of the covered entity regarding the collection, use, transfer, and storage of covered information; and

(B) the specific purposes of those practices;

(2) to provide accurate, clear, concise, and timely notice to individuals before implementing a material change in such practices; and

(3) to maintain the notice required by paragraph (1) in a form that individuals can readily access.

(b) COMPLIANCE AND OTHER CONSIDERATIONS.—In the rulemaking required by subsection (a), the Commission—

(1) shall consider the types of devices and methods individuals will use to access the required notice;

(2) may provide that a covered entity unable to provide the required notice when information is collected may comply with the requirement of subsection (a)(1) by providing an alternative time and means for an individual to receive the required notice promptly;

(3) may draft guidance for covered entities to use in designing their own notice and may include a draft model template for covered entities to use in designing their own notice; and

(4) may provide guidance on how to construct computer-readable notices or how to use other technology to deliver the required notice.

SEC. 122. INDIVIDUAL PARTICIPATION.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to require each covered entity—

(1) to offer individuals a clear and conspicuous mechanism for opt-in consent for any use of their covered information that would otherwise be unauthorized use;

(2) to offer individuals a robust, clear, and conspicuous mechanism for opt-in consent for the use by third parties of the individuals' covered information for behavioral advertising or marketing;

(3) to provide any individual to whom the personally identifiable information that is covered information pertains, and which the covered entity or its service provider stores, appropriate and reasonable—

(A) access to such information; and

(B) mechanisms to correct such information to improve the accuracy of such information; and

(4) in the case that a covered entity enters bankruptcy or an individual requests the termination of a service provided by the covered entity to the individual or termination of some other relationship with the covered entity, to permit the individual to easily request that—

(A) all of the personally identifiable information that is covered information that the covered entity maintains relating to the individual,

except for information the individual authorized the sharing of or which the individual shared with the covered entity in a forum that is widely and publicly available, be rendered not personally identifiable; or

(B) if rendering such information not personally identifiable is not possible, to cease the unauthorized use or transfer to a third party for an unauthorized use of such information or to cease use of such information for marketing, unless such unauthorized use or transfer is otherwise required by a provision of law.

(b) UNAUTHORIZED USE TRANSFERS.—In the rulemaking required by subsection (a), the Commission shall provide that with respect to transfers of covered information to a third party for which an individual provides opt-in consent, the third party to which the information is transferred may not use such information for any unauthorized use other than a use—

(1) specified pursuant to the purposes stated in the required notice under section 121(a); and

(2) authorized by the individual when the individual granted consent for the transfer of the information to the third party.

(c) ALTERNATIVE MEANS TO TERMINATE USE OF COVERED INFORMATION.—In the rulemaking required by subsection (a), the Commission shall allow a covered entity to provide individuals an alternative means, in lieu of the access, consent, and correction requirements, of prohibiting a covered entity from use or transfer of that individual's covered information.

(d) SERVICE PROVIDERS.—

(1) IN GENERAL.—The use of a service provider by a covered entity to receive covered information in performing services or functions on behalf of and under the instruction of the covered entity does not constitute an unauthorized use of such information by the covered entity if the covered entity and the service provider execute a contract that requires the service provider to collect, use, and store the information on behalf of the covered entity in a manner consistent with—

(A) the requirements of this title; and

(B) the policies and practices related to such information of the covered entity.

(2) TRANSFERS BETWEEN SERVICE PROVIDERS FOR A COVERED ENTITY.—The disclosure by a service provider of covered information pursuant to a contract with a covered entity to another service pro-

vider in order to perform the same service or functions for that covered entity does not constitute an unauthorized use.

(3) LIABILITY REMAINS WITH COVERED ENTITY.—A covered entity remains responsible and liable for the protection of covered information that has been transferred to a service provider for processing, notwithstanding any agreement to the contrary between a covered entity and the service provider.

Subtitle C—Rights Relating to Data Minimization, Constraints on Distribution, and Data Integrity

SEC. 131. DATA MINIMIZATION.

Each covered entity shall—

(1) collect only as much covered information relating to an individual as is reasonably necessary—

(A) to process or enforce a transaction or deliver a service requested by such individual;

(B) for the covered entity to provide a transaction or delivering a service requested by such individual, such as inventory management, financial reporting and accounting, planning, product or service improvement or forecasting, and customer support and service;

(C) to prevent or detect fraud or to provide for a secure environment;

(D) to investigate a possible crime;

(E) to comply with a provision of law;

(F) for the covered entity to market or advertise to such individual if the covered information used for such marketing or advertising was collected directly by the covered entity; or

(G) for internal operations, including—

(i) collecting customer satisfaction surveys and conducting customer research to improve customer service; and

(ii) collection from an Internet website of information about visits and click-through rates relating to such website to improve—

(I) website navigation and performance; and

(II) the customer's experience;

(2) retain covered information for only such duration as—

(A) with respect to the provision of a transaction or delivery of a service to an individual—

(i) is necessary to provide such transaction or deliver such service to such individual; or

(ii) if such service is ongoing, is reasonable for the ongoing nature of the service; or

(B) is required by a provision of law;

(3) retain covered information only for the purpose it was collected, or reasonably related purposes; and

(4) exercise reasonable data retention procedures with respect to both the initial collection and subsequent retention.

SEC. 132. CONSTRAINTS ON DISTRIBUTION OF INFORMATION.

(a) IN GENERAL.—Each covered entity shall—

(1) require by contract that any third party to which it transfers covered information use the information only for purposes that are consistent with—

(A) the provisions of this title; and

(B) as specified in the contract;

(2) require by contract that such third party may not combine information that the covered entity has transferred to it, that relates to an individual, and that is not personally identifiable information

with other information in order to identify such individual, unless the covered entity has obtained the opt-in consent of such individual for such combination and identification; and

(3) before executing a contract with a third party—

(A) assure through due diligence that the third party is a legitimate organization; and

(B) in the case of a material violation of the contract, at a minimum notify the Commission of such violation.

(b) TRANSFERS TO UNRELIABLE THIRD PARTIES PROHIBITED.—A covered entity may not transfer covered information to a third party that the covered entity knows—

(1) has intentionally or willfully violated a contract required by subsection (a); and

(2) is reasonably likely to violate such contract.

(c) APPLICATION OF RULES TO THIRD PARTIES.—

(1) IN GENERAL.—Except as provided in paragraph (2), a third party that receives covered information from a covered entity shall be subject to the provisions of this Act as if it were a covered entity.

(2) EXEMPTION.—The Commission may, as it determines appropriate, exempt classes of third par-

ties from liability under any provision of subtitle B if the Commission finds that—

(A) such class of third parties cannot reasonably comply with such provision; or

(B) with respect to covered information relating to individuals that is transferred to such class, compliance by such class with such provision would not sufficiently benefit such individuals.

SEC. 133. DATA INTEGRITY.

(a) IN GENERAL.—Each covered entity shall attempt to establish and maintain reasonable procedures to ensure that personally identifiable information that is covered information and maintained by the covered entity is accurate in those instances where the covered information could be used to deny consumers benefits or cause significant harm.

(b) EXCEPTION.—Subsection (a) shall not apply to covered information of an individual maintained by a covered entity that is provided—

(1) directly to the covered entity by the individual;

(2) to the covered entity by another entity at the request of the individual;

(3) to prevent or detect fraud; or

(4) to provide for a secure environment.

Subtitle D—Right to Notice of Breaches of Security

SEC. 141. DEFINITIONS.

In this subtitle:

(1) BREACH OF SECURITY.—

(A) IN GENERAL.—The term ''breach of security'' means compromise of the security, confidentiality, or integrity of, or loss of, data in electronic form that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to or acquisition of personally identifiable information from a covered entity.

(B) EXCLUSIONS.—The term ''breach of security'' does not include—

(i) a good faith acquisition of personally identifiable information by a covered entity, or an employee or agent of a covered entity, if the personally identifiable information is not subject to further use or unauthorized disclosure;

(ii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or an intelligence agency

of the United States, a State, or a political subdivision of a State; or

(iii) the release of a public record not otherwise subject to confidentiality or non-disclosure requirements.

(2) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or other database, including recordable tapes and other mass storage devices.

(3) DESIGNATED ENTITY.—The term ''designated entity'' means the Federal Government entity designated by the Secretary of Homeland Security under section 143(a).

(4) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized use of another person's personally identifiable information for the purpose of engaging in commercial transactions under the identity of such other person, including any contact that violates section 1028A of title 18, United States Code.

(5) MAJOR CREDIT REPORTING AGENCY.—The term ''major credit reporting agency'' means a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis within the

meaning of section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(6) SERVICE PROVIDER.—The term ''service provider'' means a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personally identifiable information from other information that such person transmits, routes, or stores, or for which such person provides connections. Any such person shall be treated as a service provider under this subtitle only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

SEC. 142. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—A covered entity that owns or possesses data in electronic form containing personally identifiable information, following the discovery of a breach of security of the system maintained by the covered entity that contains such information, shall notify—

(1) each individual who is a citizen or resident of the United States and whose personally identifi-

able information has been, or is reasonably believed to have been, acquired or accessed from the covered entity as a result of the breach of security; and

(2) the Commission, unless the covered entity has notified the designated entity under section 143.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD PARTIES.—In the event of a breach of security of a system maintained by a third party that has been contracted to maintain or process data in electronic form containing personally identifiable information on behalf of a covered entity who owns or possesses such data, the third party shall notify the covered entity of the breach of security.

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personally identifiable information that is owned or possessed by another covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider shall notify of the breach of security only the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified.

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—

(A) IN GENERAL.—If a covered entity is required to provide notification to more than 5,000 individuals under subsection (a)(1), the covered entity also shall notify each major credit reporting agency of the timing and distribution of the notices, except when the only personally identifiable information that is the subject of the breach of security is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(B) NOTICE TO CREDIT REPORTING AGENCIES BEFORE INDIVIDUALS.—Such notice shall be given to each credit reporting agency without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the covered entity of a security breach.

(2) REASONABLE DELAY.—

(A) IN GENERAL.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, prevent further disclosures, restore the reasonable integrity of the data system, and provide notice to law enforcement when required.

(B) EXTENSION.—

(i) IN GENERAL.—Except as provided in subsection (d), delay of notification shall not exceed 60 days following the discovery of the security breach, unless the covered entity requests an extension of time and the Commission determines in writing that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, restore the reasonable integrity of the data system, or to provide notice to the designated entity.

(ii) APPROVAL OF REQUEST.—If the Commission approves the request for delay, the covered entity may delay the period for notification for additional periods of up to 30 days.

(3) BURDEN OF PRODUCTION.—The covered entity, third party, or service provider required to provide notice under this title shall, upon the request of the Commission provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF DIRECT NOTIFICATION.—Except as provided in paragraph (2), a covered entity shall be in compliance with the notification requirement under subsection (a)(1) if—

(i) the covered entity provides conspicuous and clearly identified notification—

(I) in writing; or

(II) by e-mail or other electronic means if—

(aa) the covered entity's primary method of communication with the individual is by e-mail or such other electronic means; or

(bb) the individual has consented to receive notification by

e-mail or such other electronic means and such notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001); and

(ii) the method of notification selected under clause (i) can reasonably be expected to reach the intended individual.

(B) CONTENT OF DIRECT NOTIFICATION.—Each method of notification under subparagraph (A) shall include the following:

(i) The date, estimated date, or estimated date range of the breach of security.

(ii) A description of the personally identifiable information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security.

(iii) A telephone number that an individual can use at no cost to the individual to contact the covered entity to inquire

about the breach of security or the information the covered entity maintained about that individual.

(iv) Notice that the individual may be entitled to consumer credit reports under subsection (e)(1).

(v) Instructions how an individual can request consumer credit reports under subsection (e)(1).

(vi) A telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency.

(vii) A telephone number, that an individual can use at no cost to the individual, and an Internet website address to obtain information regarding identity theft from the Commission.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to individuals under subsection (a)(1) may provide notification under this paragraph instead of paragraph (1) of this subsection if—

(i) notification under paragraph (1) is not feasible due to lack of sufficient contact information for the individual required to be notified; or

(ii) the covered entity owns or possesses data in electronic form containing personally identifiable information of fewer than 10,000 individuals and direct notification is not feasible due to excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A).

(B) METHOD OF SUBSTITUTE NOTIFICATION.—Notification under this paragraph shall include the following:

(i) Conspicuous and clearly identified notification by e-mail to the extent the covered entity has an e-mail address for an individual who is entitled to notification under subsection (a)(1).

(ii) Conspicuous and clearly identified notification on the Internet website of the

covered entity if the covered entity maintains an Internet website.

(iii) Notification to print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personally identifiable information was acquired or accessed reside.

(C) CONTENT OF SUBSTITUTE NOTIFICATION.—Each method of notification under this paragraph shall include the following:

(i) The date, estimated date, or estimated date range of the breach of security.

(ii) A description of the types of personally identifiable information that were or are reasonably believed to have been acquired or accessed as a result of the breach of security.

(iii) Notice that an individual may be entitled to consumer credit reports under subsection (e)(1).

(iv) Instructions how an individual can request consumer credit reports under subsection (e)(1).

(v) A telephone number that an individual can use at no cost to the individual

to learn whether the individual's personally identifiable information is included in the breach of security.

(vi) A telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency.

(vii) A telephone number, that an individual can use at no cost to the individual, and an Internet website address to obtain information from the Commission regarding identity theft.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS CONCERNING SUBSTITUTE NOTIFICATION.—

(i) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall prescribe criteria for determining circumstances under which notification may be provided under paragraph (2), including criteria for determining whether providing notification under paragraph (1) is not feasible due to excessive costs to the covered entity re-

quired to provide such notification relative to the resources of such covered entity.

(ii) OTHER CIRCUMSTANCES.—The regulations required by clause (i) may also identify other circumstances in which notification under paragraph (2) would be appropriate, including circumstances under which the cost of providing direct notification exceeds the benefits to individuals.

(B) GUIDANCE.—

(i) IN GENERAL.—The Commission, in consultation with the Administrator of the Small Business Administration, shall publish and otherwise make available general guidance with respect to compliance with this subsection.

(ii) CONTENTS.—The guidance required by clause (i) shall include the following:

(I) A description of written or e-mail notification that complies with paragraph (1).

(II) Guidance on the content of notification under paragraph (2), including the extent of notification to

print and broadcast media that complies with subparagraph (B)(iii) of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—Subject to the provisions of this subsection, not later than 60 days after the date of a request by an individual who received notification under subsection (a)(1) and quarterly thereafter for 2 years, a covered entity required to provide notification under such subsection to such individual shall provide, or arrange for the provision of, to such individual at no cost to such individual, consumer credit reports from at least 1 major credit reporting agency.

(2) LIMITATION.—Paragraph (1) shall not apply if the only personally identifiable information that is the subject of the breach of security is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—Not later than 1 year after the date of the enactment of this Act, the Commission shall prescribe the following:

(A) Criteria for determining the circumstances under which a covered entity required to provide notification under subsection (a)(1) must provide or arrange for the provision of free consumer credit reports under this subsection.

(B) A simple process under which a covered entity that is a small business concern or small nonprofit organization may request a full or a partial waiver or a modified or an alternative means of complying with this subsection if providing free consumer credit reports is not feasible due to excessive costs relative to the resources of such covered entity and relative to the level of harm, to affected individuals, caused by the breach of security.

(4) DEFINITIONS.—In this subsection:

(A) SMALL BUSINESS CONCERN.—The term ''small business concern'' has the meaning given such term under section 3 of the Small Business Act (15 U.S.C. 632).

(B) SMALL NONPROFIT ORGANIZATION.—The term ''small nonprofit organization'' has the meaning the Commission shall give such term for purposes of this subsection.

(f) DELAY OF NOTIFICATION AUTHORIZED FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If the United States Secret Service or the Federal Bureau of Investigation determines that notification under this section would impede a criminal investigation or a national security activity, such notification shall be delayed upon written notice from the United States Secret Service or the Federal Bureau of Investigation to the covered entity that experienced the breach of security. The notification from the United States Secret Service or the Federal Bureau of Investigation shall specify the period of delay requested for national security or law enforcement purposes.

(2) SUBSEQUENT DELAY OF NOTIFICATION.—

(A) IN GENERAL.—If the notification required under subsection (a)(1) is delayed pursuant to paragraph (1), a covered entity shall give notice not more than 30 days after the day such law enforcement or national security delay was invoked unless a Federal law enforcement or intelligence agency provides written notification that further delay is necessary.

(B) WRITTEN JUSTIFICATION REQUIREMENTS.—

(i) UNITED STATES SECRET SERVICE.—If the United States Secret Service instructs a covered entity to delay notification under this section beyond the 30-day period set forth in subparagraph (A) (referred to in this clause as ''subsequent delay''), the United States Secret Service shall submit written justification for the subsequent delay to the Secretary of Homeland Security before the subsequent delay begins.

(ii) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation instructs a covered entity to delay notification under this section beyond the 30-day period set forth in subparagraph (A) (referred to in this clause as ''subsequent delay''), the Federal Bureau of Investigation shall submit written justification for the subsequent delay to the Attorney General before the subsequent delay begins.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any Federal

agency for acts relating to the delay of notification for national security or law enforcement purposes under this subtitle.

(g) GENERAL EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if, following a breach of security, the covered entity reasonably concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) FTC GUIDANCE.—Not later than 1 year after the date of the enactment of this Act, the Commission, after consultation with the Director of the National Institute of Standards and Technology, shall issue guidance regarding the application of the exemption under paragraph (1).

(h) EXEMPTIONS FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—A covered entity shall be exempt from the notice requirements under this section if—

(A) a determination is made—

(i) by the United States Secret Service or the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to reveal sen-

sitive sources and methods or similarly impede the ability of the Government to conduct law enforcement or intelligence investigations; or

(ii) by the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to cause damage to the national security; and

(B) the United States Secret Service or the Federal Bureau of Investigation, as the case may be, provides written notice of its determination under subparagraph (A) to the covered entity.

(2) UNITED STATES SECRET SERVICE.—If the United States Secret Service invokes an exemption under paragraph (1), the United States Secret Service shall submit written justification for invoking the exemption to the Secretary of Homeland Security before the exemption is invoked.

(3) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation invokes an exemption under paragraph (1), the Federal Bureau of Investigation shall submit written justification for invoking the exemption to the Attorney General before the exemption is invoked.

(4) IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for national security or law enforcement purposes under this subtitle.

(5) REPORTS.—Not later than 540 days after the date of the enactment of this Act, and upon request by Congress thereafter, the United States Secret Service and the Federal Bureau of Investigation shall submit to Congress a report on the number and nature of breaches of security subject to the exemptions for national security and law enforcement purposes under this subsection.

(i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the notice requirements under this section if the covered entity utilizes or participates in a security program that—

(A) effectively 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

(B) provides notice to each affected individual after a breach of security that resulted in

attempted fraud or an attempted unauthorized transaction.

(2) LIMITATIONS.—An exemption under paragraph (1) shall not apply if—

(A) the breach of security includes personally identifiable information, other than a credit card number or credit card security code, of any type; or

(B) the breach of security includes both the individual's credit card number and the individual's first and last name.

(j) FINANCIAL INSTITUTIONS REGULATED BY FEDERAL FUNCTIONAL REGULATORS.—

(1) IN GENERAL.—A covered financial institution shall be deemed in compliance with this section if—

(A) the Federal functional regulator with jurisdiction over the covered financial institution has issued a standard by regulation or guideline under title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) that—

(i) requires financial institutions within its jurisdiction to provide notification to individuals following a breach of security; and

(ii) provides protections substantially similar to, or greater than, those required under this Act; and

(B) the covered financial institution is in compliance with the standard under subparagraph (A).

(2) DEFINITIONS.—In this subsection:

(A) COVERED FINANCIAL INSTITUTION.—The term ''covered financial institution'' means a financial institution that is subject to—

(i) the data security requirements of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(ii) any implementing standard issued by regulation or guideline issued under that Act; and

(iii) the jurisdiction of a Federal functional regulator under that Act.

(B) FEDERAL FUNCTIONAL REGULATOR.—The term ''Federal functional regulator'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(C) FINANCIAL INSTITUTION.—The term ''financial institution'' has the meaning given

the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(k) EXEMPTION; HEALTH PRIVACY.—

(1) COVERED ENTITY OR BUSINESS ASSOCIATE UNDER HITECH ACT.—To the extent that a covered entity under this section acts as a covered entity or a business associate under section 13402 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17932), has the obligation to provide notification to individuals following a breach of security under that Act or its implementing regulations, and is in compliance with that obligation, the covered entity shall be deemed in compliance with this section.

(2) ENTITY SUBJECT TO HITECH ACT.—To the extent that a covered entity under this section acts as a vendor of personal health records, a third party service provider, or other entity subject to section 13407 of the Health Information Technology for Economical and Clinical Health Act (42 U.S.C. 17937), has the obligation to provide notification to individuals following a breach of security under that Act or its implementing regulations, and is in compliance with that obligation, the covered entity shall be deemed in compliance with this section.

(3) LIMITATION OF STATUTORY CONSTRUCTION.—Nothing in this subtitle may be construed in any way to give effect to the sunset provision under section 13407(g)(2) of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937(g)(2)) or to otherwise limit or affect the applicability, under section 13407 of that Act, of the requirement to provide notification to individuals following a breach of security for vendors of personal health records and each entity described in clause (ii), (iii), or (iv) of section 13424(b)(1)(A) of that Act (42 U.S.C. 17953(b)(1)(A)).

(l) INTERNET WEBSITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission, finds that notification of the breach of security via the Commission's Internet website would be in the public interest or for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet website.

(m) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of the enactment of this Act, the Commission shall conduct a study on the feasibility and advisability of requiring notification provided pursuant to subsection

(d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

SEC. 143. NOTICE TO LAW ENFORCEMENT.

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall designate a Federal Government entity to receive notice under this section.

(b) NOTICE TO DESIGNATED ENTITY.—A covered entity shall notify the designated entity of a breach of security if—

(1) the number of individuals whose personally identifiable information was, or is reasonably believed to have been, acquired or accessed as a result of the breach of security exceeds 10,000;

(2) the breach of security involves a database, networked or integrated databases, or other data system containing the personally identifiable information of more than 1,000,000 individuals;

(3) the breach of security involves databases owned by the Federal Government; or

(4) the breach of security involves primarily personally identifiable information of individuals known to the covered entity to be employees or con-

tractors of the Federal Government involved in national security or law enforcement.

(c) CONTENT OF NOTICES.—

(1) IN GENERAL.—Each notice under subsection (b) shall contain the following:

(A) The date, estimated date, or estimated date range of the breach of security.

(B) A description of the nature of the breach of security.

(C) A description of each type of personally identifiable information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security.

(D) A statement of each paragraph under subsection (b) that applies to the breach of security.

(2) CONSTRUCTION.—Nothing in this section shall be construed to require a covered entity to reveal specific or identifying information about an individual as part of the notice under paragraph (1).

(d) NOTICE BY DESIGNATED ENTITY.—The designated entity shall promptly provide each notice it receives under subsection (b) to the following:

(1) The United States Secret Service.

(2) The Federal Bureau of Investigation.

(3) The Commission.

(4) The United States Postal Inspection Service, if the breach of security involves mail fraud.

(5) The attorney general of each State affected by the breach of security.

(6) Such other Federal agencies as the designated entity considers appropriate for law enforcement, national security, or data security purposes.

(e) TIMING OF NOTICES.—Notice under this section shall be delivered as follows:

(1) Notice under subsection (b) shall be delivered as promptly as possible, but—

(A) not less than 3 business days before notification to an individual under section 142(a)(1); and

(B) not later than 10 days after the date of discovery of the events requiring notice.

(2) Notice under subsection (d) shall be delivered as promptly as possible, but not later than 1 business day after the date that the designated entity receives notice of a breach of security from a covered entity.

Subtitle E—Enforcement

SEC. 151. GENERAL APPLICATION.

The requirements of this title shall apply to any person who—

(1) collects, uses, transfers, or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period; and

(2) is—

(A) a person over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

(B) a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.), notwithstanding the definition of the term ''Acts to regulate commerce'' in section 4 of the Federal Trade Commission Act (15 U.S.C. 44) and the exception provided by section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)) for such carriers; or

(C) a nonprofit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of such Code, notwithstanding the definition of the

term ''Acts to regulate commerce'' in section 4 of the Federal Trade Commission Act (15 U.S.C. 44) and the exception provided by section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)) for such organizations.

SEC. 152. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A reckless or repetitive violation of a provision of this title, except section 143, shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(b) POWERS OF COMMISSION.—

(1) IN GENERAL.—Except as provided in paragraph (3), the Commission shall enforce this title, except section 143, in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title.

(2) PRIVILEGES AND IMMUNITIES.—Except as provided in paragraph (3), any person who violates a provision of this title, except section 143, shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(3) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—The Commission shall enforce this title, except section 143, with respect to common carriers and nonprofit organizations described in section 151 to the extent necessary to effectuate the purposes of this title as if such carriers and nonprofit organizations were persons over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)).

(c) RULEMAKING AUTHORITY.—

(1) LIMITATION.—In promulgating rules under this title, the Commission may not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(2) ADMINISTRATIVE PROCEDURE.—The Commission shall promulgate regulations under this title

in accordance with section 553 of title 5, United States Code.

(d) RULE OF CONSTRUCTION.—Nothing in this title shall be construed to limit the authority of the Commission under any other provision of law.

SEC. 153. ENFORCEMENT BY ATTORNEY GENERAL.

(a) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of section 143.

(b) PENALTIES.—

(1) IN GENERAL.—Upon proof of such conduct by a preponderance of the evidence, a covered entity shall be subject to a civil penalty of not more than $1,000 per individual whose personally identifiable information was or is reasonably believed to have been accessed or acquired as a result of the breach of security that is the basis of the violation, up to a maximum of $100,000 per day while such violation persists.

(2) LIMITATIONS.—The total amount of the civil penalty assessed under this subsection against a covered entity for acts or omissions relating to a single breach of security shall not exceed $3,000,000, unless the conduct constituting a viola-

tion of subtitle D was reckless or repeated, in which case an additional civil penalty of up to $3,000,000 may be imposed.

(3) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of the enactment of this Act, and each year thereafter, the amounts specified in paragraphs (1) and (2) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(c) INJUNCTIVE ACTIONS.—If it appears that a covered entity has engaged, or is engaged, in any act or practice that constitutes a violation of subtitle D, the Attorney General may petition an appropriate United States district court for an order enjoining such practice or enforcing compliance with such subtitle.

(d) ISSUANCE OF ORDER.—A court may issue such an order under paragraph (c) if it finds that the conduct in question constitutes a violation of subtitle D.

SEC. 154. ENFORCEMENT BY STATES.

(a) CIVIL ACTION.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely

affected by a covered entity who violates any part of this title in a manner that results in economic or physical harm to an individual or engages in a pattern or practice that violates any part of this title other than section 143, the attorney general may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States—

(1) to enjoin further violation of this title or a regulation promulgated under this title by the defendant;

(2) to compel compliance with this title or a regulation promulgated under this title; or

(3) for violations of this title or a regulation promulgated under this title to obtain civil penalties in the amount determined under section title.

(b) RIGHTS OF FEDERAL TRADE COMMISSION.—

(1) NOTICE TO FEDERAL TRADE COMMISSION.—

(A) IN GENERAL.—Except as provided in subparagraph (C), the attorney general of a State shall notify the Commission in writing of any civil action under subsection (b), prior to initiating such civil action.

(B) CONTENTS.—The notice required by subparagraph (A) shall include a copy of the

complaint to be filed to initiate such civil action.

(C) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notice required by subparagraph (A), the State shall provide notice immediately upon instituting a civil action under subsection (b).

(2) INTERVENTION BY FEDERAL TRADE COMMISSION.—Upon receiving notice required by paragraph (1) with respect to a civil action, the Commission may—

(A) intervene in such action; and

(B) upon intervening—

(i) be heard on all matters arising in such civil action; and

(ii) file petitions for appeal of a decision in such action.

(c) PREEMPTIVE ACTION BY FEDERAL TRADE COMMISSION.—If the Commission institutes a civil action for violation of this title or a regulation promulgated under this title, no attorney general of a State may bring a civil action under subsection (a) against any defendant named in the complaint of the Commission for violation of this title or a regulation promulgated under this title that is alleged in such complaint.

(d) INVESTIGATORY POWERS.—Nothing in this section may be construed to prevent the attorney general of a State from exercising the powers conferred on such attorney general by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) ACTIONS BY OTHER STATE OFFICIALS.—

(1) IN GENERAL.—In addition to civil actions brought by attorneys general under subsection (a), any other officer of a State who is authorized by the

State to do so may bring a civil action under subsection (a), subject to the same requirements and limitations that apply under this section to civil actions brought by attorneys general.

(2) SAVINGS PROVISION.—Nothing in this section may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

SEC. 155. CIVIL PENALTIES.

(a) IN GENERAL.—In an action brought under section 154, in addition to any other penalty otherwise applicable to a violation of this title or any regulation promulgated under this title, the following civil penalties shall apply:

(1) SUBTITLE A VIOLATIONS.—A covered entity that recklessly or repeatedly violates subtitle A is liable for a civil penalty equal to the amount calculated by multiplying the number of days that the entity is not in compliance with such subtitle by an amount not to exceed $33,000.

(2) SUBTITLE B VIOLATIONS.—A covered entity that recklessly or repeatedly violates subtitle B is liable for a civil penalty equal to the amount calculated by multiplying the number of days that such

an entity is not in compliance with such subtitle, or the number of individuals for whom the entity failed to obtain consent as required by such subtitle, whichever is greater, by an amount not to exceed $33,000.

(3) SUBTITLE D VIOLATIONS.—A covered entity that recklessly or repeatedly violates section 142 is liable for a civil penalty equal to the amount calculated by multiplying the number of violations of such section by an amount not to exceed $33,000. Each failure to send notification as required under such section to a resident of the State shall be treated as a separate violation.

(b) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index for All Urban Consumers is first published by the Bureau of Labor Statistics that is after 1 year after the date of the enactment of this Act, and each year thereafter, each of the amounts specified in subsection (a) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(c) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under section 154, the maximum civil pen-

alty for which any covered entity may be liable under this section in such actions shall not exceed—

(1) $6,000,000 for any related series of violations of any rule promulgated under subtitle A;

(2) $6,000,000 for any related series of violations of subtitle B; and

(3) $6,000,000 for any related series of violations of section 142.

SEC. 156. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAWS.—The provisions of this title shall supersede any provisions of the law of any State relating to those entities covered by the regulations issued pursuant to this title, to the extent that such provisions relate to the collection, use, or disclosure of—

(1) covered information addressed in this title; or

(2) personally identifiable information or personal identification information addressed in provisions of the law of a State.

(b) UNAUTHORIZED CIVIL ACTIONS; CERTAIN STATE LAWS.—

(1) UNAUTHORIZED ACTIONS.—No person other than a person specified in section 154 may bring a civil action under the laws of any State if such action is premised in whole or in part upon the

defendant violating this title or a regulation promulgated under this title.

(2) PROTECTION OF CERTAIN STATE LAWS.—This title shall not be construed to preempt the applicability of—

(A) State laws that address the collection, use, or disclosure of health information or financial information; or

(B) other State laws to the extent that those laws relate to acts of fraud.

(c) RULE OF CONSTRUCTION RELATING TO REQUIRED DISCLOSURES TO GOVERNMENT ENTITIES.—This title shall not be construed to expand or limit the duty or authority of a covered entity or third party to disclose personally identifiable information to a government entity under any provision of law.

SEC. 157. NO PRIVATE RIGHT OF ACTION.

This title may not be construed to provide any private right of action.

Subtitle F—Co-Regulatory Safe Harbor Programs

SEC. 161. ESTABLISHMENT OF SAFE HARBOR PROGRAMS.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall initiate a rulemaking proceeding to establish requirements

for the establishment and administration of safe harbor programs under which a nongovernmental organization will administer a program that—

(1) establishes a mechanism for participants to implement the requirements of this title with regards to—

(A) certain types of unauthorized uses of covered information as described in paragraph (2); or

(B) any unauthorized use of covered information; and

(2) offers consumers a clear, conspicuous, persistent, and effective means of opting out of the transfer of covered information by a covered entity participating in the safe harbor program to a third party for—

(A) behavioral advertising purposes;

(B) location-based advertising purposes;

(C) other specific types of unauthorized use; or

(D) any unauthorized use.

(b) SELECTION OF NONGOVERNMENTAL ORGANIZATIONS TO ADMINISTER PROGRAM.—

(1) SUBMITTAL OF APPLICATIONS.—An applicant seeking to administer a program under the re-

quirements established pursuant to subsection (a) shall submit to the Commission an application therefor at such time, in such manner, and containing such information as the Commission may require.

(2) NOTICE AND RECEIPT OF APPLICATIONS.—Upon completion of the rulemaking proceedings required by subsection (a), the Commission shall—

(A) publish a notice in the Federal Register that it will receive applications for approval of safe harbor programs under this subtitle; and

(B) begin receiving applications under paragraph (1).

(3) SELECTION.—Not later than 270 days after the date on which the Commission receives a completed application under this subsection, the Commission shall grant or deny the application on the basis of the Commission's evaluation of the applicant's capacity to provide protection of individuals' covered information with regard to specific types of unauthorized uses of covered information as described in subsection (a)(2) that is substantially equivalent to or superior to the protection otherwise provided under this title.

(4) WRITTEN FINDINGS.—Any decision reached by the Commission under this subsection shall be accompanied by written findings setting forth the basis for and reasons supporting such decision.

(c) SCOPE OF SAFE HARBOR PROTECTION.—The scope of protection offered by safe harbor programs approved by the Commission that establish mechanisms for participants to implement the requirements of the title only for certain uses of covered information as described in subsection (a)(2) shall be limited to participating entities' use of those particular types of covered information.

(d) SUPERVISION BY FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—The Commission shall exercise oversight and supervisory authority of a safe harbor program approved under this section through—

(A) ongoing review of the practices of the nongovernmental organization administering the program;

(B) the imposition of civil penalties on the nongovernmental organization if it is not compliant with the requirements established under subsection (a); and

(C) withdrawal of authorization to administer the safe harbor program under this subtitle.

(2) ANNUAL REPORTS BY NONGOVERNMENTAL ORGANIZATIONS.—Each year, each nongovernmental organization administering a safe harbor program under this section shall submit to the Commission a report on its activities under this subtitle during the preceding year.

SEC. 162. PARTICIPATION IN SAFE HARBOR PROGRAM.

(a) EXEMPTION.—Any covered entity that participates in, and demonstrates compliance with, a safe harbor program administered under section 161 shall be exempt from any provision of subtitle B or subtitle C if the Commission finds that the requirements of the safe harbor program are substantially the same as or more protective of privacy of individuals than the requirements of the provision from which the exemption is granted.

(b) LIMITATION.—Nothing in this subtitle shall be construed to exempt any covered entity participating in a safe harbor program from compliance with any other requirement of the regulations promulgated under this title for which the safe harbor does not provide an exception.

Subtitle G—Application With Other Federal Laws

SEC. 171. APPLICATION WITH OTHER FEDERAL LAWS.

(a) QUALIFIED EXEMPTION FOR PERSONS SUBJECT TO OTHER FEDERAL PRIVACY LAWS.—If a person is subject to a provision of this title and a provision of a Federal privacy law described in subsection (d), such provision of this title shall not apply to such person to the extent that such provision of Federal privacy law applies to such person.

(b) PROTECTION OF OTHER FEDERAL PRIVACY LAWS.—Nothing in this title may be construed to modify, limit, or supersede the operation of the Federal privacy laws described in subsection (d) or the provision of information permitted or required, expressly or by implication, by such laws, with respect to Federal rights and practices.

(c) COMMUNICATIONS INFRASTRUCTURE AND PRIVACY.—If a person is subject to a provision of section 222 or 631 of the Communications Act of 1934 (47 U.S.C. 222 and 551) and a provision of this title, such provision of such section 222 or 631 shall not apply to such person to the extent that such provision of this title applies to such person.

(d) OTHER FEDERAL PRIVACY LAWS DESCRIBED.—The Federal privacy laws described in this subsection are as follows:

(1) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974).

(2) The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.).

(3) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(4) The Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq.).

(5) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(6) Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 et seq.).

(7) Chapters 119, 123, and 206 of title 18, United States Code.

(8) Section 2710 of title 18, United States Code.

(9) Section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly referred to as the ''Family Educational Rights and Privacy Act of 1974'').

(10) Section 445 of the General Education Provisions Act (20 U.S.C. 1232h).

(11) The Privacy Protection Act of 1980 (42 U.S.C. 2000aa et seq.).

(12) The regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), as such regulations relate to a person described in section 1172(a) of the Social Security Act (42 U.S.C. 1320d–1(a)) or to transactions referred to in section 1173(a)(1) of such Act (42 U.S.C. 1320d–2(a)(1)).

(13) The Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(14) Section 227 of the Communications Act of 1934 (47 U.S.C. 227).

Subtitle H—Development of Commercial Data Privacy Policy in the Department of Commerce

SEC. 181. DIRECTION TO DEVELOP COMMERCIAL DATA PRIVACY POLICY.

The Secretary of Commerce shall contribute to the development of commercial data privacy policy by—

(1) convening private sector stakeholders, including members of industry, civil society groups, academia, in open forums, to develop codes of con-

duct in support of applications for safe harbor programs under subtitle F;

(2) expanding interoperability between the United States commercial data privacy framework and other national and regional privacy frameworks;

(3) conducting research related to improving privacy protection under this title; and

(4) conducting research related to improving data sharing practices, including the use of anonymised data, and growing the information economy.

TITLE II—ONLINE PRIVACY OF CHILDREN

SEC. 201. SHORT TITLE.

This title may be cited as the ''Do Not Track Kids Act of 2014''.

SEC. 202. FINDINGS.

Congress finds the following:

(1) Since the enactment of the Children's Online Privacy Protection Act of 1998, the World Wide Web has changed dramatically, with the creation of tens of millions of websites, the proliferation of entirely new media platforms, and the emergence of a diverse ecosystem of services, devices, and applications that enable users to connect wirelessly within

an online environment without being tethered to a desktop computer.

(2) The explosive growth of the Internet ecosystem has unleashed a wide array of opportunities to learn, communicate, participate in civic life, access entertainment, and engage in commerce.

(3) In addition to these significant benefits, the Internet also presents challenges, particularly with respect to the efforts of entities to track the online activities of children and minors and to collect, use, and disclose personal information about them, including their geolocation, for commercial purposes.

(4) Children and teens are visiting numerous companies' websites, and marketers are using multimedia games, online quizzes, and mobile phone and tablet applications to create ties to children and teens.

(5) According to a study by the Wall Street Journal in 2010, websites directed to children and teens were more likely to use cookies and other tracking tools than sites directed to a general audience.

(6) This study examined 50 popular websites for children and teens in the United States and found that these 50 sites placed 4,123 cookies, bea-

cons, and other tracking tools on the test computer used for the study.

(7) This is 30 percent greater than the number of such tracking tools that were placed on the test computer in a similar study of the 50 overall most popular websites in the United States, which are generally directed to adults.

(8) Children and teens lack the cognitive ability to distinguish advertising from program content and to understand that the purpose of advertising is to persuade them, making them unable to activate the defenses on which adults rely.

(9) Children and teens are less able than adults to understand the potential long-term consequences of having their information available to third parties, including advertisers, and other individuals.

(10) According to Common Sense Media and the Center for Digital Democracy, 90 percent of teens have used some form of social media, 75 percent have a social networking site, and 51 percent check their social networking site at least once a day.

(11) Ninety-one percent of parents and 91 percent of adults believe it is not okay for advertisers

to collect information about a child's location from that child's mobile phone.

(12) Ninety-four percent of parents and 91 percent of adults agree that advertisers should receive the parent's permission before putting tracking software on a child's computer.

(13) Ninety-six percent of parents and 94 percent of adults expressed disapproval when asked if it is ''okay for a website to ask children for personal information about their friends''.

(14) Eighty-eight percent of parents would support a law that requires search engines and social networking sites to get users' permission before using their personal information.

(15) A Commonsense Media/Zogby poll found that 94 percent of parents and 94 percent of adults believe individuals should have the ability to request the deletion, after a specific period of time, of all of their personal information held by an online search engine, social networking site, or marketing company.

(16) According to a Pew/Berkman Center poll, 69 percent of parents of teens who engage in online activity are concerned about how that activity might

affect their children's future academic or employment opportunities.

(17) Eighty-one percent of parents of teens who engage in online activity say they are concerned about how much information advertisers can learn about their children's online activity.

SEC. 203. DEFINITIONS.

(a) IN GENERAL.—In this title:

(1) MINOR.—The term ''minor'' means an individual over the age of 12 and under the age of 16.

(2) TARGETED MARKETING.—The term ''targeted marketing'' means advertising or other efforts to market a product or service that are directed to a specific individual or device—

(A) based on the personal information of the individual or a unique identifier of the device; and

(B) as a result of use by the individual, or access by the device, of a website, online service, online application, or mobile application.

(b) TERMS DEFINED BY COMMISSION.—In this title, the terms ''directed to minors'' and ''geolocation information'' shall have the meanings given such terms by the Commission by regulation. Not later than 1 year after the date of the enactment of this Act, the Commission shall

promulgate, under section 553 of title 5, United States Code, regulations that define such terms broadly enough so that they are not limited to current technology, consistent with the principles articulated by the Commission regarding the definition of the term ''Internet'' in its statement of basis and purpose on the final rule under the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) promulgated on November 3, 1999 (64 Fed. Reg. 59891).

(c) OTHER DEFINITIONS.—The definitions set forth in section 1302 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501), as amended by section 3(a), shall apply in this title, except to the extent the Commission provides otherwise by regulations issued under section 553 of title 5, United States Code.

SEC. 204. ONLINE COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION OF CHILDREN.

(a) DEFINITIONS.—Section 1302 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501) is amended—

(1) by amending paragraph (2) to read as follows:

''(2) OPERATOR.—The term 'operator'—

''(A) means any person who, for commercial purposes, in interstate or foreign commerce,

operates or provides a website on the Internet, online service, online application, or mobile application, and who—

"(i) collects or maintains, either directly or through a service provider, personal information from or about the users of such website, service, or application;

"(ii) allows another person to collect personal information directly from users of such website, service, or application (in which case the operator is deemed to have collected the information); or

"(iii) allows users of such website, service, or application to publicly disclose personal information (in which case the operator is deemed to have collected the information); and

"(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).";

(2) in paragraph (4)—

(A) by amending subparagraph (A) to read as follows:

''(A) the release of personal information for any purpose, except where such information is provided to a person other than an operator who provides support for the internal operations of the website, online service, online application, or mobile application of the operator and does not disclose or use that information for any other purpose; and''; and

(B) in subparagraph (B), by striking ''website or online service'' and inserting ''website, online service, online application, or mobile application'';

(3) in paragraph (8)—

(A) by amending subparagraph (G) to read as follows:

''(G) information concerning a child or the parents of that child (including any unique or substantially unique identifier, such as a customer number) that an operator collects online from the child and combines with an identifier described in subparagraphs (A) through (G).'';

(B) by redesignating subparagraphs (F) and (G) as subparagraphs (G) and (H), respectively; and

(C) by inserting after subparagraph (E) the following new subparagraph:

''(F) information (including an Internet protocol address) that permits the identification of an individual, the computer of an individual, or any other device used by an individual to access the Internet or an online service, online application, or mobile application;'';

(4) by striking paragraph (10) and redesignating paragraphs (11) and (12) as paragraphs (10) and (11), respectively; and

(5) by adding at the end the following new paragraph:

''(12) ONLINE, ONLINE SERVICE, ONLINE APPLICATION, MOBILE APPLICATION, DIRECTED TO CHILDREN.—The terms 'online', 'online service', 'online application', 'mobile application', and 'directed to children' shall have the meanings given such terms by the Commission by regulation. Not later than 1 year after the date of the enactment of the Commercial Privacy Bill of Rights Act of 2014, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that define such terms broadly enough so that they are not limited to current technology, consistent with the prin-

ciples articulated by the Commission regarding the definition of the term 'Internet' in its statement of basis and purpose on the final rule under this title promulgated on November 3, 1999 (64 Fed. Reg. 59891). The definition of the term 'online service' in such regulations shall include broadband Internet access service (as defined in the Report and Order of the Federal Communications Commission relating to the matter of preserving the open Internet and broadband industry practices (FCC 10–201, adopted by the Commission on December 21, 2010)).''.

(b) ONLINE COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION OF CHILDREN.—Section 1303 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6502) is amended—

(1) by striking the heading and inserting the following: ''**ONLINE COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION OF CHILDREN.**'';

(2) in subsection (a)—

(A) by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children, or an op-

erator having actual knowledge that personal information being collected is from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).''; and

(B) in paragraph (2)—

(i) by striking ''of such a website or online service''; and

(ii) by striking ''subsection (b)(1)(B)(iii)'' and inserting ''subsection (b)(1)(C)(iii)''; and

(3) in subsection (b)—

(A) by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—Not later than 1 year after the date of the enactment of the Commercial Privacy Bill of Rights Act of 2014, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to require an operator of a website, online service, online application, or mobile application directed to children, or an operator having actual knowledge that personal information being collected is from a child—

''(A) to provide clear and conspicuous notice in clear and plain language of the types of

personal information the operator collects, how the operator uses such information, whether the operator discloses such information, and the procedures or mechanisms the operator uses to ensure that personal information is not collected from children except in accordance with the regulations promulgated under this paragraph;

''(B) to obtain verifiable parental consent for the collection, use, or disclosure of personal information of a child;

''(C) to provide to a parent whose child has provided personal information to the operator, upon request by and proper identification of the parent—

''(i) a description of the specific types of personal information collected from the child by the operator;

''(ii) the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, by the operator of personal information collected from the child; and

''(iii) a means that is reasonable under the circumstances for the parent to

obtain any personal information collected from the child, if such information is available to the operator at the time the parent makes the request;

''(D) not to condition participation in a game, or use of a website, service, or application, by a child on the provision by the child of more personal information than is reasonably required to participate in the game or use the website, service, or application; and

''(E) to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.'';

(B) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by striking ''paragraph (1)(A)(ii)'' and inserting ''paragraph (1)(B)''; and

(ii) in subparagraph (A), by inserting ''or to contact a different child'' after ''to recontact the child'';

(C) by amending paragraph (3) to read as follows:

''(3) CONTINUATION OF SERVICE.—The regulations shall prohibit an operator from discontinuing service provided to a child on the basis of refusal by the parent of the child, under the regulations prescribed under paragraph (1)(C)(ii), to permit the further use or maintenance in retrievable form, or future collection, by the operator of personal information collected from the child, to the extent that the operator is capable of providing such service without such information.''; and

(D) by adding at the end the following:

''(4) RULE FOR TREATMENT OF USERS OF WEBSITES, SERVICES, AND APPLICATIONS DIRECTED TO CHILDREN.—An operator of a website, online service, online application, or mobile application that is directed to children shall treat all users of such website, service, or application as children for purposes of this title, except as permitted by the Commission by a regulation promulgated under this title.''.

(c) ADMINISTRATION AND APPLICABILITY OF ACT.—Section 1306 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6505) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking ", in the case of" and all that follows and inserting the following: "by the appropriate Federal banking agency with respect to any insured depository institution (as such terms are defined in section 3 of such Act (12 U.S.C. 1813));"; and

(B) by striking paragraph (2) and redesignating paragraphs (3) through (6) as paragraphs (2) through (5), respectively; and

(2) by adding at the end the following new subsection:

"(f) TELECOMMUNICATIONS CARRIERS AND CABLE OPERATORS.—

"(1) ENFORCEMENT BY FTC.—Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), compliance with the requirements imposed under this title shall be enforced by the Commission with respect to any telecommunications carrier (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)).

"(2) RELATIONSHIP TO OTHER LAW.—To the extent that sections 222, 338(i), and 631 of the Communications Act of 1934 (47 U.S.C. 222; 338(i); 551) are inconsistent with this title, this title controls.".

SEC. 205. TARGETED MARKETING TO CHILDREN OR MINORS.

(a) ACTS PROHIBITED.—It is unlawful for—

(1) an operator of a website, online service, online application, or mobile application directed to children, or an operator having actual knowledge that personal information being collected is from a child, to use, disclose to third parties, or compile personal information for targeted marketing purposes without verifiable parental consent; or

(2) an operator of a website, online service, online application, or mobile application directed to minors, or an operator having actual knowledge that personal information being collected is from a minor, to use, disclose to third parties, or compile personal information for targeted marketing purposes without the consent of the minor.

(b) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to implement this section.

SEC. 206. DIGITAL MARKETING BILL OF RIGHTS FOR TEENS AND FAIR INFORMATION PRACTICES PRINCIPLES.

(a) ACTS PROHIBITED.—It is unlawful for an operator of a website, online service, online application, or mo-

bile application directed to minors, or an operator having actual knowledge that personal information being collected is from a minor, to collect personal information from a minor 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 described in subsection (b).

(b) FAIR INFORMATION PRACTICES PRINCIPLES.—The Fair Information Practices Principles described in this subsection are the following:

(1) COLLECTION LIMITATION PRINCIPLE.—Except as provided in paragraph (3), personal information should be collected from a minor only when collection of the personal information is—

(A) consistent with the context of a particular transaction or service or the relationship of the minor with the operator, including collection necessary to fulfill a transaction or provide a service requested by the minor; or

(B) required or specifically authorized by law.

(2) DATA QUALITY PRINCIPLE.—The personal information of a minor should be accurate, complete, and kept up-to-date to the extent necessary to fulfill

the purposes described in subparagraphs (A) through (D) of paragraph (3).

(3) PURPOSE SPECIFICATION PRINCIPLE.—The purposes for which personal information is collected should be specified to the minor not later than at the time of the collection of the information. The subsequent use or disclosure of the information should be limited to—

(A) fulfillment of the transaction or service requested by the minor;

(B) support for the internal operations of the website, service, or application, as described in section 312.2 of title 16, Code of Federal Regulations;

(C) compliance with legal process or other purposes expressly authorized under specific legal authority; or

(D) other purposes—

(i) that are specified in a notice to the minor; and

(ii) to which the minor has consented under paragraph (7) before the information is used or disclosed for such other purposes.

(4) RETENTION LIMITATION PRINCIPLE.—The personal information of a minor should not be retained for longer than is necessary to fulfill a transaction or provide a service requested by the minor or such other purposes specified in subparagraphs (A) through (D) of paragraph (3). The operator should implement a reasonable and appropriate data disposal policy based on the nature and sensitivity of such personal information.

(5) SECURITY SAFEGUARDS PRINCIPLE.—The personal information of a minor should be protected by reasonable and appropriate security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.

(6) OPENNESS PRINCIPLE.—

(A) IN GENERAL.—The operator should maintain a general policy of openness about developments, practices, and policies with respect to the personal information of a minor. The operator should provide each minor using the website, online service, online application, or mobile application of the operator with a clear and prominent means—

(i) to identify and contact the operator, by, at a minimum, disclosing, clearly

and prominently, the identity of the operator and—

(I) in the case of an operator who is an individual, the address of the principal residence of the operator and an e-mail address and telephone number for the operator; or

(II) in the case of any other operator, the address of the principal place of business of the operator and an e-mail address and telephone number for the operator;

(ii) to determine whether the operator possesses any personal information of the minor, the nature of any such information, and the purposes for which the information was collected and is being retained;

(iii) to obtain any personal information of the minor that is in the possession of the operator from the operator, or from a person specified by the operator, within a reasonable time after making a request, at a charge (if any) that is not excessive, in a reasonable manner, and in a form that is readily intelligible to the minor;

(iv) to challenge the accuracy of personal information of the minor that is in the possession of the operator; and

(v) if the minor establishes the inaccuracy of personal information in a challenge under clause (iv), to have such information erased, corrected, completed, or otherwise amended.

(B) LIMITATION.—Nothing in this paragraph shall be construed to permit an operator to erase or otherwise modify personal information requested by a law enforcement agency pursuant to legal authority.

(7) INDIVIDUAL PARTICIPATION PRINCIPLE.—The operator should—

(A) obtain consent from a minor before using or disclosing the personal information of the minor for any purpose other than the purposes described in subparagraphs (A) through (C) of paragraph (3); and

(B) obtain affirmative express consent from a minor before using or disclosing previously collected personal information of the minor for purposes that constitute a material

change in practice from the original purposes specified to the minor under paragraph (3).

(c) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to implement this section, including regulations further defining the Fair Information Practices Principles described in subsection (b).

SEC. 207. ONLINE COLLECTION OF GEOLOCATION INFORMATION OF CHILDREN AND MINORS.

(a) ACTS PROHIBITED.—

(1) IN GENERAL.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or minors, or an operator having actual knowledge that geolocation information being collected is from a child or minor, to collect geolocation information from a child or minor in a manner that violates the regulations prescribed under subsection (b).

(2) DISCLOSURE TO PARENT OR MINOR PROTECTED.—Notwithstanding paragraph (1), neither an operator nor the operator's agent shall be held to be liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure

of geolocation information under subparagraph (C)(ii)(III) or (D)(ii)(III) of subsection (b)(1).

(b) REGULATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that require an operator of a website, online service, online application, or mobile application directed to children or minors, or an operator having actual knowledge that geolocation information being collected is from a child or minor—

(A) to provide clear and conspicuous notice in clear and plain language of any geolocation information the operator collects, how the operator uses such information, and whether the operator discloses such information;

(B) to establish procedures or mechanisms to ensure that geolocation information is not collected from children or minors except in accordance with regulations promulgated under this paragraph;

(C) in the case of collection of geolocation information from a child—

(i) prior to collecting such information, to obtain verifiable parental consent; and

(ii) after collecting such information, to provide to the parent of the child, upon request by and proper identification of the parent—

(I) a description of the geolocation information collected from the child by the operator;

(II) the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, by the operator of geolocation information from the child; and

(III) a means that is reasonable under the circumstances for the parent to obtain any geolocation information collected from the child, if such information is available to the operator at the time the parent makes the request; and

(D) in the case of collection of geolocation information from a minor—

(i) prior to collecting such information, to obtain affirmative express consent from such minor; and

(ii) after collecting such information, to provide to the minor, upon request—

(I) a description of the geolocation information collected from the minor by the operator;

(II) the opportunity at any time to refuse to permit the further use or maintenance in retrievable form, or future collection, by the operator of geolocation information from the minor; and

(III) a means that is reasonable under the circumstances for the minor to obtain any geolocation information collected from the minor, if such information is available to the operator at the time the minor makes the request.

(2) WHEN CONSENT NOT REQUIRED.—The regulations promulgated under paragraph (1) shall provide that verifiable parental consent under subparagraph (C)(i) of such paragraph or affirmative ex-

press consent under subparagraph (D)(i) of such paragraph is not required when the collection of the geolocation information of a child or minor is necessary, to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

(3) CONTINUATION OF SERVICE.—The regulations promulgated under paragraph (1) shall prohibit an operator from discontinuing service provided to—

(A) a child on the basis of refusal by the parent of the child, under subparagraph (C)(ii)(II) of such paragraph, to permit the further use or maintenance in retrievable form, or future online collection, of geolocation information from the child by the operator, to the extent that the operator is capable of providing such service without such information; or

(B) a minor on the basis of refusal by the minor, under subparagraph (D)(ii)(II) of such paragraph, to permit the further use or maintenance in retrievable form, or future online collection, of geolocation information from the minor by the operator, to the extent that the

operator is capable of providing such service without such information.

(c) INCONSISTENT STATE LAW.—No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this section that is inconsistent with the treatment of those activities or actions under this section.

SEC. 208. REMOVAL OF CONTENT.

(a) ACTS PROHIBITED.—It is unlawful for an operator of a website, online service, online application, or mobile application to make publicly available through the website, service, or application content or information that contains or displays personal information of children or minors in a manner that violates the regulations prescribed under subsection (b).

(b) REGULATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations that require an operator—

(A) to the extent technologically feasible, to implement mechanisms that permit a user of the website, service, or application of the oper-

ator to erase or otherwise eliminate content or information submitted to the website, service, or application by such user that is publicly available through the website, service, or application and contains or displays personal information of children or minors; and

(B) to take appropriate steps to make users aware of such mechanisms and to provide notice to users that such mechanisms do not necessarily provide comprehensive removal of the content or information submitted by such users.

(2) EXCEPTION.—The regulations promulgated under paragraph (1) may not require an operator or third party to erase or otherwise eliminate content or information that—

(A) any other provision of Federal or State law requires the operator or third party to maintain; or

(B) was submitted to the website, service, or application of the operator by any person other than the user who is attempting to erase or otherwise eliminate such content or information, including content or information submitted

by such user that was republished or resubmitted by another person.

(3) LIMITATION.—Nothing in this section shall be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

SEC. 209. ENFORCEMENT AND APPLICABILITY.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) IN GENERAL.—Except as otherwise provided, this title and the regulations prescribed under this title shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(2) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—Subject to subsection (b), a violation of this title or a regulation prescribed under this title shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(3) ACTIONS BY THE COMMISSION.—

(A) IN GENERAL.—Subject to subsection (b), and except as provided in subsection (d)(1), the Commission shall prevent any person from

violating this title or a regulation prescribed under this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates this title or a regulation prescribed under this title shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES.—Notwithstanding subsection (a), compliance with the requirements imposed under this title shall be enforced as follows:

(1) Under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818) by the appropriate Federal banking agency, with respect to an insured depository institution (as such terms are defined in section 3 of such Act (12 U.S.C. 1813)).

(2) Under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union

Administration Board, with respect to any Federal credit union.

(3) Under part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation, with respect to any air carrier or foreign air carrier subject to such part.

(4) Under the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of such Act (7 U.S.C. 226; 227)) by the Secretary of Agriculture, with respect to any activities subject to such Act.

(5) Under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration, with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(c) ENFORCEMENT BY STATES.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this title or a regulation prescribed under this title, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district

court of the United States of appropriate jurisdiction to—

(A) enjoin that practice;

(B) enforce compliance with this title or such regulation;

(C) obtain damages, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider to be appropriate.

(2) RIGHTS OF FEDERAL TRADE COMMISSION.—

(A) NOTICE TO FEDERAL TRADE COMMISSION.—

(i) IN GENERAL.—Except as provided in clause (iii), the attorney general of a State shall notify the Federal Trade Commission in writing that the attorney general intends to bring a civil action under paragraph (1) before initiating the civil action.

(ii) CONTENTS.—The notification required by clause (i) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(iii) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notification required by clause (i) before initiating a civil action under paragraph (1), the attorney general shall notify the Federal Trade Commission immediately upon instituting the civil action.

(B) INTERVENTION BY FEDERAL TRADE COMMISSION.—The Federal Trade Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening—

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(3) INVESTIGATORY POWERS.—For purposes of bringing any civil action under paragraph (1), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(4) PREEMPTIVE ACTION BY FEDERAL TRADE COMMISSION.—If the Federal Trade Commission institutes a civil action or an administrative action with respect to a violation of this title, the attorney general of a State may not, during the pendency of such action, bring a civil action under paragraph (1) against any defendant named in the complaint of the Commission for the violation with respect to which the Commission instituted such action.

(5) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(6) ACTIONS BY OTHER STATE OFFICIALS.—

(A) IN GENERAL.—In addition to civil actions brought by attorneys general under paragraph (1), any other officer of a State who is authorized by the State to do so may bring a civil action under paragraph (1), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(B) SAVINGS PROVISION.—Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(d) TELECOMMUNICATIONS CARRIERS AND CABLE OPERATORS.—

(1) ENFORCEMENT BY FTC.—Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), compliance with the requirements imposed under this title shall be enforced by the Commission with respect to any telecommunications carrier (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)).

(2) RELATIONSHIP TO OTHER LAW.—To the extent that sections 222, 338(i), and 631 of the Com-

munications Act of 1934 (47 U.S.C. 222; 338(i); 551) are inconsistent with this title, this title controls.

SEC. 210. RULE FOR TREATMENT OF USERS OF WEBSITES, SERVICES, AND APPLICATIONS DIRECTED TO CHILDREN OR MINORS.

An operator of a website, online service, online application, or mobile application that is directed to children or minors shall treat all users of such website, service, or application as children or minors (as the case may be) for purposes of this title, except as permitted by the Commission by a regulation promulgated under this title.

SEC. 211. EFFECTIVE DATES.

(a) IN GENERAL.—Except as provided in subsections (b) and (c), this title and the amendments made by this title shall take effect on the date that is 1 year after the date of the enactment of this Act.

(b) AUTHORITY TO PROMULGATE REGULATIONS.—The following shall take effect on the date of the enactment of this Act:

(1) The amendments made by subsections (a)(5) and (b)(3)(A) of section 204.

(2) Sections 205(b), 206(c), 207(b), and 208(b).

(3) Subsections (b) and (c) of section 203.

(c) DIGITAL MARKETING BILL OF RIGHTS FOR TEENS.—Section 206, except for subsection (c) of such section, shall take effect on the date that is 180 days after the promulgation of regulations under such subsection.

○