112TH CONGRESS
1ST SESSION

S. 799

To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 12, 2011

Mr. KERRY (for himself and Mr. MCCAIN) 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, 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. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Commercial Privacy Bill of Rights Act of 2011''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. 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 information with respect and in accordance with common standards.

(5) To the extent that States regulate the treatment of personally identifiable information, their efforts to address Internet privacy could lead to a patchwork of inconsistent standards and protections.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

(10) 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.

(11) 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.

(12) 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).

(13) As in those instances, the Federal Government has a substantial interest in creating a level playing field of protection across all collectors of personally identifiable information, both in the United States and abroad.

(14) The Federal Trade Commission has called private self regulation efforts as of the day before the date of the introduction of this Act inadequate. The Commission has also distinguished publishers' first-party data collection practices from third-party practices related specifically to behavioral advertising. The Commission has noted that when dealing directly with an Internet website, consumers are likely to understand why they receive a recommenda-

tion or advertisement from that entity and may expect it.

(15) 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. 3. DEFINITIONS.

In this Act:

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

(2) COVERED ENTITY.—The term ''covered entity'' means any person to whom this Act applies under section 401.

(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 person-

ally 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

(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 information, 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.—The term ''third party'' means, with respect to a covered entity, a person that—

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

(B) is not a service provider used by the covered entity to receive personally identifiable information or sensitive personally identifiable information in performing services or functions on behalf of and under the instruction of the covered entity; and

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

(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 relating 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 individual 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 201(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.

TITLE I—RIGHT TO SECURITY AND ACCOUNTABILITY

SEC. 101. 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, and nature 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. 102. 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 Act;

(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 501.

SEC. 103. 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 Act;

(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 202.

TITLE II—RIGHT TO NOTICE AND INDIVIDUAL PARTICIPATION

SEC. 201. 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 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 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. 202. 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-out consent for any use of their covered information that would otherwise be unau-

thorized use, except with respect to any use requiring opt-in consent under paragraph (3);

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

(3) to offer individuals a clear and conspicuous mechanism for opt-in consent for—

(A) the collection, use, or transfer of sensitive personally identifiable information other than—

(i) to process or enforce a transaction or deliver a service requested by that individual;

(ii) for fraud prevention and detection; or

(iii) to provide for a secure physical or virtual environment; and

(B) the use of previously collected covered information or transfer to a third party for an unauthorized use of previously collected covered information, if—

(i) there is a material change in the covered entity's stated practices that requires notice under section 201(a)(2); and

(ii) such use or transfer creates a risk of economic or physical harm to an individual;

(4) 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

(5) 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 201(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 prohib-

iting 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 Act; 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 provider 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.

TITLE III—RIGHTS RELATING TO DATA MINIMIZATION, CONSTRAINTS ON DISTRIBUTION, AND DATA INTEGRITY

SEC. 301. 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;

(G) for research and development conducted for the improvement of carrying out a transaction or delivering a service; or

(H) 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; and

(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;

(B) with respect to research and development described in paragraph (1)(G), is necessary for such research and development; or

(C) is required by a provision of law.

SEC. 302. 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 Act; 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 parties from liability under any provision of title II 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. 303. 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; or

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

TITLE IV—ENFORCEMENT

SEC. 401. GENERAL APPLICATION.

The requirements of this Act 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 non-profit 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. 402. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A knowing or repetitive violation of a provision of this Act or a regulation promulgated under this Act 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.—The Commission shall enforce this Act 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 Act. Any person who violates this Act or the regulations issued under this Act shall be subject to

the penalties and entitled to the privileges and immunities provided in that Act.

(2) SPECIAL RULE.—The Commission shall enforce this Act under paragraph (1) of this subsection with respect to common carriers and non-profit organizations described in section 401 to the extent necessary to effectuate the purposes of this Act as if such carriers and non-profit 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 Act, 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 Act in accordance with section 553 of title 5, United States Code.

SEC. 403. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(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 Act 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 Act other than title III, 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 Act or a regulation promulgated under this Act by the defendant;

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

(3) for violations of this Act or a regulation promulgated under this Act to obtain civil penalties in the amount determined under section 404.

(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 Federal Trade 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 Federal Trade 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 Federal Trade Commission institutes a civil action for violation of this Act or a regulation promulgated under this Act, 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 Act or a regulation promulgated under this Act 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.

SEC. 404. CIVIL PENALTIES.

(a) IN GENERAL.—In an action brought under section 403, in addition to any other penalty otherwise applicable to a violation of this Act or any regulation promulgated under this Act, the following civil penalties shall apply:

(1) TITLE I VIOLATIONS.—A covered entity that knowingly or repeatedly violates title I 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 title by an amount not to exceed $16,500.

(2) TITLE II VIOLATIONS.—A covered entity that knowingly or repeatedly violates title II 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 title, or the number of individuals for whom the entity failed to obtain

consent as required by such title, whichever is greater, by an amount not to exceed $16,500.

(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 403, the maximum civil penalty for which any covered entity may be liable under this section in such actions shall not exceed—

(1) $3,000,000 for any related series of violations of any rule promulgated under title I; and

(2) $3,000,000 for any related series of violations of title II.

SEC. 405. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAWS.—The provisions of this Act shall supersede any provisions of the law of any State relating to those entities covered by the regula-

tions issued pursuant to this Act, to the extent that such provisions relate to the collection, use, or disclosure of—

(1) covered information addressed in this Act; 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 403 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 Act or a regulation promulgated under this Act.

(2) PROTECTION OF CERTAIN STATE LAWS.—This Act 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;

(B) State laws that address notification requirements in the event of a data breach; or

(C) 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 Act 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. 406. NO PRIVATE RIGHT OF ACTION.

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

TITLE V—CO-REGULATORY SAFE HARBOR PROGRAMS

SEC. 501. ESTABLISHMENT OF SAFE HARBOR PROGRAMS.

(a) IN GENERAL.—Not later than 365 days 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 Act 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 requirements 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 ap-

proval of safe harbor programs under this title; 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 Act.

(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 Act 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 title.

(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 title during the preceding year.

SEC. 502. PARTICIPATION IN SAFE HARBOR PROGRAM.

(a) EXEMPTION.—Any covered entity that participates in, and demonstrates compliance with, a safe harbor program administered under section 501 shall be exempt any provision of title II or title III 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 title 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 Act for which the safe harbor does not provide an exception.

TITLE VI—APPLICATION WITH OTHER FEDERAL LAWS

SEC. 601. 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 Act and a provision of a Federal privacy law described in subsection (d), such provision of this Act 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 Act 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 Act, such provision of such section 222 or 631 shall not apply to such person to the extent that such provision of this Act 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).

TITLE VII—DEVELOPMENT OF COMMERCIAL DATA PRIVACY POLICY IN THE DEPARTMENT OF COMMERCE

SEC. 701. 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 conduct in support of applications for safe harbor programs under title V;

(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 Act; and

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

○