II

[STAFF WORKING DRAFT]

MARCH 11, 2011

112TH CONGRESS
1ST SESSION

S. ——

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

MARCH ——, 2011

Mr. KERRY (for himself and Mr. MCCAIN) introduced the following bill; which was read twice and referred to the Committee on ——————————

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) Existing State, local, and Federal laws provide inadequate privacy protection for individuals engaging in and interacting with persons engaged in interstate commerce.

(7) With the exception of Federal Trade Commission enforcement of laws against unfair and de-

ceptive practices, the Federal Government thus far 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) 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 currently available today. 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 the 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).

(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) 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.—The term ''covered information'' means—

(A) personally identifiable information;

(B) unique identifier information; and

(C) any information that is collected, used, or maintained in connection with personally identifiable information or unique identifier information that may be used to identify an individual.

(4) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' includes 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 **[Note:** See clause (iii) for overlap and questions about ''name'' there.**]**.

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

(iii) An e-mail address of such individual if it contains the individual's name [First name? Last name? Full name? Legal name? Maiden name? Nickname? Initials? Embedded with other letters or characters, as in Danny123@xyz.com?].

(iv) A telephone number or mobile device number dedicated to contacting such individual at any place other than the individual's place of work.

(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) A unique persistent identifier associated with an individual or a networked device used by such individual, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number if used to identify a specific individual.

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

(B) If used, transferred, or maintained in connection with 1 or more of the items of information described in subparagraph (A)—

(i) a birth date, the number of a certificate of birth or adoption, or a place of birth;

(ii) a unique persistent identifier associated with an individual or a networked device used by such individual, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number;

(iii) precise geographic location; or

(iv) any other information concerning an individual that may reasonably be used to identify that individual.

(5) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means personally identifiable information which, if lost, compromised, or disclosed without authorization could result in harm to an individual.

(6) SERVICE PROVIDER.—The term ''service provider'' means, with respect to a covered entity, a person that—

(A) receives personally identifiable information or sensitive information from a covered entity as a service provider performing services or functions on behalf of and under the instruction of the covered entity, provided—

(i) the covered entity obtains the required consent for the initial collection of such information and provides notice as required under this Act;

(ii) the covered entity enters into a contractual agreement that prohibits the service provider from using or disclosing the information other than to carry out the purposes for which the information was disclosed; and

(iii) in such cases, the covered entity remains responsible and liable for the protection of covered information and sensitive information that has been transferred to a service provider for processing; **[Note:** This is a substantive rule applicable to cov-

ered entities, not part of the definition of ''service provider''**]**; or

(B) discloses, as a service provider for a covered entity, the information to another service provider in order to perform the same service or functions described in subparagraph (C) **[Note:** There is no subparagraph (C).**]** on behalf of the covered entity **[Note:** Redundancy of using ''as a service provider'' as part of the definition of ''service provider''. If a person is not a service provider under the subparagraph (A) definition, it cannot meet the ''as a service provider'' test of subparagraph (B).**]**.

(7) THIRD PARTY.—The term ''third party'' means, with respect to a covered entity, a person that is not related to the covered entity by common ownership or corporate control nor contractually required to comply with the covered entity's policies and controls related to privacy as well as with any applicable confidentiality agreement.

(8) UNAUTHORIZED USE.—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, other than use—

(A) to process a transaction or service requested by that individual;

(B) to operate the covered entity that is providing a transaction or service requested by that individual, such as inventory management, accounting, planning, product or service improvement or forecasting;

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

(D) to investigate a possible crime or that is required by law or legal process;

(E) to market or advertise to an individual from a covered entity if the personally identifiable information used for such marketing or advertising was collected directly by the covered entity;

(F) necessary for the improvement of the transaction or service through research and development; or

(G) necessary for internal operations, including collecting customer satisfaction surveys to improve customer service information, and website collection of information about visits and click-through rates to improve site navigation.

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

TITLE I—RIGHT TO SECURITY AND ACCOUNTABILITY

SEC. 101. SECURITY.

Within 180 days after the date of enactment of this Act the Commission shall initiate a rulemaking proceeding to require each covered entity to impose reasonable security measures to protect the covered information it collects and maintains. In the rulemaking, the Commission may not require a specific technological means of meeting the 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 for being responsive to non-frivolous complaint from individuals regarding the collection, use, transfer, or maintenance of their covered information; and

(3) describe its programmatic means of compliance with the requirements of this Act upon request from the Commission or an appropriate safe harbor program.

TITLE II—RIGHT TO NOTICE AND INDIVIDUAL PARTICIPATION

SEC. 201. TRANSPARENT NOTICE OF PRACTICES.

(a) IN GENERAL.—Within 18 months after the date of 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 regarding its collection, use, transfer, maintenance, and other practices related to covered information;

(2) to provide clear, concise, and timely notice to individuals before implementing a material change in its collection, use, transfer, maintenance, or other practices related to such information; 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, 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 a mechanism for an individual to obtain 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.—Within 24 months after the date of 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 unauthorized use of their personally identifiable information except with respect to any use requiring opt-in consent under paragraph (2);

(2) 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 to process a transaction or service requested by that individual or for fraud prevention and detection or to provide for a secure environment;

(B) the use or transfer of previously collected personally identifiable information if there is a material change in the covered entity's stated practices that requires notice under section 201(a)(2); and

(C) the transfer of covered information to a third party for an unauthorized use or public display of such personal information;

(3) to provide any individual whose personally identifiable information the covered entity maintains appropriate and reasonable access or correction re-

garding its use of that individual's personally identifiable information; and

(4) to permit an individual to easily request that all of the personally identifiable information the covered entity maintains about that individual be rendered not personally identifiable, and where this is not possible, to cease its collection, use, transfer, or maintenance of such information if—

(A) the covered entity enters bankruptcy; or

(B) the individual requests the termination of the service or other relationship with the covered entity.

(b) UNAUTHORIZED USE TRANSFERS.—In the rulemaking, the Commission shall provide that—

(1) 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 specified pursuant to section 301 and authorized by the individual when the individual granted consent for the transfer of the information to the third party; and

(2) the collection of covered information by a third party through a covered entity's website, mobile application, or other consumer interface constitutes a transfer of such information to the third party.

(c) ALTERNATIVE MEANS TO TERMINATE USE OF PERSONALLY IDENTIFIABLE INFORMATION.—In the rulemaking required by subsection (a), the Commission may 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.

TITLE III—RIGHT TO PURPOSE SPECIFICATION; DATA MINIMIZATION; CONSTRAINTS ON DISTRIBUTION; DATA INTEGRITY

SEC. 301. PURPOSE SPECIFICATION.

In each notice required under title II of this Act, each covered entity shall provide a clear and concise description of types of unauthorized uses for which it intends to transfer covered information to any third party.

SEC. 302. DATA MINIMIZATION.

Each covered entity shall seek—

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

(A) to provide a transaction or service requested by, or consented to by, the individual to whom the information relates;

(B) for the prevention of fraud; or

(C) for the improvement of the transaction or service through research and development; and

(2) to retain the information only as long as necessary to provide the transaction or service or for a reasonable period of time if the service is ongoing.

SEC. 303. 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 the purposes of this Act and as specified in the contract;

(2) require by contract that the third party will not combine information that is not personally identifiable information that the covered entity has transferred to it with other information in order to identify individuals from that information; and

(3) assure before executing a contract with a third party, through due diligence, that the third party is a legitimate organization and take appropriate action in the case of a material violation of the contract.

(b) TRANSFERS TO UNRELIABLE THIRD PARTIES PROHIBITED.—A covered entity may not transfer covered information to a third party that it knows has violated or is reasonably likely to violate the contract required by subsection (a).

(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 it finds that such class of third parties cannot reasonably comply with such provision or that compliance with such provision would not sufficiently benefit the individual whose personally identifiable information is being transferred to such class of third parties.

SEC. 304. DATA INTEGRITY.

Each covered entity shall attempt to establish and maintain reasonable procedures to ensure that personally identifiable information maintained by the covered entity is accurate, except for such information provided directly to the covered entity by the individual to whom it relates.

TITLE IV—APPLICATION AND ENFORCEMENT

SEC. 401. GENERAL APPLICATION.

The requirements of this Act shall apply to any person that—

(1) collects, uses, transfers, or maintains 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 violation of this Act or a regulation promulgated under this Act shall be treated as an unfair and 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) ADMINSTRATIVE 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 threatened or adversely affected by a covered entity who violates any part of this Act that results in economic harm or engages in a pattern or practice that violates any part of this Act other than title III, the attorney general, as parens patriae, may 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) INTERVENTION BY THE FTC.—

(1) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under subsection (a) to the Commission and provide the

Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein; and

(C) to file petitions for appeal.

(2) LIMITATION ON STATE ACTION WHEN FEDERAL ACTION IS FILED.—If the Commission has instituted a civil action for violation of this Act or a regulation promulgated under this Act no attorney general of a State may bring an action under this section for any violation of this Act or a regulation promulgated under this Act alleged in the complaint.

(c) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this Act 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—

(1) to conduct investigations;

(2) to administer oaths or affirmations; or

(3) 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 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.

(2) TITLE I OR III VIOLATIONS.—A covered entity that knowingly or repeatedly violates title I or title III 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.

(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 enactment of this Act, and each year thereafter, each of the amounts specified in subsection (a) shall be increased by the per-

centage 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;

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

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

SEC. 405. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this Act, to the extent that such statute, regulation, or rule relates to the collection, use, or disclosure of covered information addressed in this Act.

(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 considered or 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.—The Commission shall initiate a rulemaking proceeding to establish requirements for the establishment and administration of safe harbor programs under which a non-governmental organization will administer a program that—

(1) establishes a mechanism for participants to implement the requirements of this Act;

(2) offers consumers a clear, conspicuous, 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 any unauthorized use; and

(3) implements a comprehensive information privacy program by—

(A) incorporating necessary development processes and practices throughout the product life cycle, which are designed to safeguard the personal data of individuals based on their reasonable expectations of privacy and the relevant threats that need to be guarded against in meeting those expectations; and

(B) maintaining appropriate management processes and practices throughout the data life cycle, which are designed to ensure that information systems comply with this Act, the privacy policies of a covered entity, and the privacy preferences of individuals consistent with the consent choices and related mechanisms of individual participation as described in section 202.

(b) SUBMISSION AND APPROVAL OF APPLICATIONS.—Upon completion of the rulemaking proceedings required by this Act, the Commission shall publish a notice in the Federal Register that it will receive applications for approval of safe harbor programs under this title. Within 270 days after the date on which the Commission receives a completed application under this section, the Commission shall grant or deny the application on the basis of its evaluation of the applicant's capacity to provide protection of individuals' covered information that is substantially equivalent or superior to the protection otherwise provided under this Act, including implementing a comprehensive information privacy program.

(c) SUPERVISION BY FTC.—The Commission shall exercise oversight and supervisory authority of an approved safe harbor program through ongoing review of

practices, the imposition of civil penalties on non-compliant participants, and withdrawal of approval. An approved safe harbor program shall submit an annual report to the Commission on its activities during the preceding year, including data with respect to operations, and the results of a biennial survey of consumer satisfaction.

SEC. 502. PARTICIPATION IN SAFE HARBOR PROGRAM.

The Commission shall exempt any covered entity that participates in, and demonstrates compliance with, a safe harbor program approved by the Commission from compliance with any provision the safe harbor addresses of title II or title III if the Commission finds that the safe harbor program requires compliance with requirements that are the substantially the same as, or more protective of privacy than, the requirements of the provision from which the exemption sis granted.

SEC. 503. FTC WEBSITE SUPPORT.

(a) IN GENERAL.—The Commission may host an Internet website where consumers can access the opt-out tools offered by each approved safe harbor program for the transfer of covered information to third parties for unauthorized uses.

(b) PARTICIPATION BY SAFE HARBOR PROGRAMS.—Notwithstanding section 402(c)(3), the Commission may

require an approved safe harbor program to participate in the website.

TITLE VI—APPLICATION WITH OTHER FEDERAL LAWS.

SEC. 601. APPLICATION WITH OTHER LAWS.

This Act shall have no effect on activities covered by any of the following, except as provided expressly in this Act:

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

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

(3) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191).

(4) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).

(5) Sections 222 and 631 of the Communications Act of 1934 (47 U.S.C. 222 and 47 U.S.C. 551).

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

(7) The CAN–SPAM Act of 2003 (15 U.S.C. 7701 et seq.).

(8) The Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510 et seq.).

(9) The Video Privacy Protection Act (18 U.S.C. 2710 et seq.).

TITLE VII—DEVELOPMENT OF COMMERCE 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 of this Act;

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

(3) conducting research related to improving privacy protection under this Act.

○