ADMINISTRATION DISCUSSION DRAFT
CONSUMER PRIVACY BILL OF RIGHTS ACT

Bill

To establish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders.

SEC. 1. Short Title. This Act may be cited as the Consumer Privacy Bill of Rights Act of 2015.

SEC. 2. Table of Contents.

SEC. 3. Findings. The Congress finds that:

(a) Americans cherish privacy as an element of their individual freedom.
(b) American laws, regulations, and enforcement entities provide robust privacy safeguards for consumers.
(c) There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. This growth has the potential for great benefits to human knowledge, technological innovation, and economic growth, but also the potential to harm individual privacy and freedom.
(d) Laws must keep pace as technology and businesses practices evolve.
(e) Preserving individuals' trust and confidence that personal data will be protected appropriately, while supporting flexibility and the free flow of information, will promote continued innovation and economic growth in the networked economy.
(f) Enforcement of general principles in law will ensure that individuals continue to enjoy meaningful privacy protections while affording ample flexibility for technologies and business models to evolve.
(g) Enforceable codes of conduct developed through open, transparent processes will provide certainty for businesses and strong privacy protections for individuals.
(h) It is the sense of Congress that each covered entity should provide, when reasonable, a version of the notice required under this Act in a format that is computer-readable, to facilitate the development of information technology tools that will help individuals compare covered entities' personal data practices.

SEC. 4. Definitions.

(a) "Personal data"

(1) In General.—"Personal data" means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual, including but not limited to—
(A) the first name (or initial) and last name;

(B) a postal or email address;
(C) a telephone or fax number;
(D) a social security number, tax identification number, passport number, driver's license number, or any other unique government-issued identification number;
(E) any biometric identifier, such as a fingerprint or voice print;
(F) any unique persistent identifier, including a number or alphanumeric string that uniquely identifies a networked device; commercially issued identification numbers and service account numbers, such as a financial account number, credit card or debit card number, health care account number, retail account number; unique vehicle identifiers, including Vehicle Identification Numbers or license plate numbers; or any required security code, access code, or password that is necessary to access an individual's service account;
(G) unique identifiers or other uniquely assigned or descriptive information about personal computing or communication devices; or
(H) any data that are collected, created, processed, used, disclosed, stored, or otherwise maintained and linked, or as a practical matter linkable by the covered entity, to any of the foregoing.

(2) Exceptions.—
(A) De-identified data.—The term "personal data" shall not include data otherwise described by paragraph (1) that a covered entity (either directly or through an agent)—
(i) alters such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device;
(ii) publicly commits to refrain from attempting to identify with an individual or device and adopts relevant controls to prevent such identification;
(iii) causes to be covered by a contractual or other legally enforceable prohibition on each entity to which the covered entity discloses the data from attempting to link the data to a specific individual or device, and requires the same of all onward disclosures; and
(iv) requires each entity to which the covered entity discloses the data to publicly commit to refrain from attempting to link to a specific individual or device.
(B) Deleted data.—The term "personal data" shall not include data otherwise described by paragraph (1) that a covered entity deletes.
(C) Employee information.—The term "personal data" shall not include an employee's name, title, business address, business email address, business telephone number, business fax number, or any public licenses or records associated with the employment, when such information is collected or used by the employee's employer or another covered entity, in connection with such employment status.
(D) Cybersecurity data.—The term "personal data" shall not include cyber threat indicators collected, processed, created, used, retained, or disclosed in order to investigate, mitigate, or otherwise respond to a cybersecurity threat or incident, when processed for those purposes.

(i) The term "cyber threat indicator" means information—
(I) that is necessary to indicate, describe or identify—
(a) malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat;
(b) a method of defeating a technical or operational control;
(c) a technical vulnerability;
(d) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system inadvertently to enable the defeat of a technical control or an operational control;
(e) malicious cyber command and control;
(f) any combination of (a)-(e).
(II) from which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat.

(b) "Covered entity"

(1) In General.—"Covered entity" means a person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce. Such term does not include—
(A) the Federal Government, the Government of any State, the Government of any Indian tribe, or any political subdivision, department, agency, component, entity, or instrumentality thereof;
(B) any employee, officer, agent, contractor, or organization working on behalf of an entity described in subparagraph (A), with regard to data processed on behalf of such entity;
(C) a natural person, unless acting in a non-de-minimis commercial capacity;
(D) any person that—
(i) collects, creates, processes, uses, retains, or discloses personal data of fewer than 10,000 individuals and devices during any 12-month period, or has 5 or fewer employees; and
(ii) does not knowingly collect, use, retain, or disclose any information that is linked with personal data and includes, or relates directly to, that individual's medical history; national origin; sexual orientation; gender identity; religious beliefs or affiliation; income, assets, or liabilities; precise geolocation information; unique biometric data; or Social Security number.
(iii) notwithstanding the foregoing, any person that is a covered entity solely because of clause (ii) shall be a covered entity only with regard to the data described in clause (ii).
(iv) notwithstanding the foregoing, any person described in clauses (i)-(ii) may elect to become a covered entity through public election;
(E) any person that has 25 or fewer employees, and would otherwise be a covered entity solely because of data that the person processes related to job applicants and employees in the ordinary course; or

(F) any other exceptions established pursuant to section 405 of this Act.

(2) Exception.—
(A) To the extent that a person collects, creates, processes, uses, retains, or discloses personal data needed to conduct research relating directly to security threats to or vulnerabilities in devices or networks, or to address threats or vulnerabilities identified by that research, such person shall not be deemed a covered entity for purposes of sections 101, 102, 103, 104, or 106 of Title I of this Act.
(B) This exception shall apply only so long as such person—
(i) uses such personal data exclusively for the activities described by subparagraph (A);
(ii) takes reasonable steps to mitigate privacy risks when conducting the activities permitted by subparagraph (A); and
(iii) destroys, deletes, or de-identifies such personal data within a reasonable time after such person has completed the activities permitted by subparagraph (A).

(c) "Collect" means acquire by any means, including but not limited to, direct or indirect interaction with an individual or purchase, lease, or rental.

(d) "Means to/of control" mean enabling individuals to make decisions about the processing of their personal data, including but not limited to, providing mechanisms to obtain consent, withdraw consent, correct inaccurate data, permit or restrict access to data, or otherwise identify and implement the privacy preferences of individuals.

(e) "Deletion" or "delete" means remove or destroy data (either directly or through an agent) such that there is a reasonable basis for expecting that the data could not be retrieved in the ordinary course. No requirement to delete, destroy, or de-identify data under this Act shall require a covered entity to delete, destroy, or de-identify data that are retained for backup or archival purposes to the extent that such systems are not accessed in the ordinary course. To the extent such backup or archival systems are accessed in the ordinary course, this Act's deletion requirements shall apply.

(f) "Minor" means an individual who is under 18 years of age.

(g) "Privacy risk" means the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional or other harm to an individual.

(h) "Commission" means the Federal Trade Commission.

(i) "State" includes the several States, the District of Columbia, Federally recognized Indian tribes, the Commonwealth of Puerto Rico, the Commonwealth of the

Northern Mariana Islands, American Samoa, Guam, the Virgin Islands, and any other territory or possession of the United States.

(j) "Customary business records" mean data, including personal data, typically collected in the ordinary course of conducting business and that is retained for generally accepted purposes for that business, including accounting, auditing, tax, fraud prevention, warranty fulfillment, billing, or other customary business purposes.

(k) "Context" means the circumstances surrounding a covered entity's processing of personal data, including but not limited to—

(1) the extent and frequency of direct interactions between individuals and the covered entity, if any;

(2) the nature and history of the interactions described in paragraph (1);

(3) the level of understanding that reasonable users of the covered entity's goods or services would have of how the covered entity processes the personal data that it collects, including through any notice provided by the covered entity;

(4) the range of goods or services that the covered entity offers, the use of such goods or services by individuals, the benefits of such goods or services to individuals, and the brand names that the covered entity uses to offer such goods or services;

(5) information known by the covered entity about the privacy preferences of individual users of its goods or services;

(6) the types of personal data foreseeably processed in order to provide a good or service that an individual requests from the covered entity;

(7) the types of personal data foreseeably processed in order to improve or market a good or service that an individual requests from the covered entity;

(8) the types of personal data foreseeably processed as customary business records;

(9) the age and sophistication of individuals who use the covered entity's goods or services, including whether the covered entity's goods or services are directed toward minors or the elderly;

(10) the extent to which personal data under the control of the covered entity are exposed to public view; and

(11) the extent to which personal data under the control of the covered entity are obscured.

(l) "Process personal data" or "personal data processing" means taking any action regarding data that is linked to an individual or a specific device, including but not limited to collecting, retaining, disclosing, using, merging, linking, and combining data.

(m) "Adverse action" has the same meaning as in section 701(d) of the Fair Credit Opportunity Act of 1974 (15 U.S.C. § 1691(d)(6)) and section 603(k)(1)(B)(i)-(iii) of the Fair Credit Reporting Act (15 U.S.C. § 1681a(k)(1)(B)(i)-(iii)).

(n) "Enumerated exceptions" means:

(1) Preventing or detecting fraud;

(2) Preventing or detecting child exploitation or serious violent crime;

(3) Protecting the security of devices, networks, or facilities;

(4) Protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer;

(5) Monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity;

(6) Processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or

(7) Complying with a legal requirement or responding to an authorized governmental request.

TITLE I—Privacy Bill of Rights

SEC. 101. Transparency.

(a) In General.—Each covered entity shall provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous notice about the covered entity's privacy and security practices. Such notice shall be reasonable in light of context. Covered entities shall provide convenient and reasonable access to such notice, and any updates or modifications to such notice, to individuals about whom it processes personal data.

(b) Contents of Notice.—The notice required by subsection (a) shall include but is not limited to—

(1) The personal data the covered entity processes, including the sources of data collection if the collection is not directly from the individual;

(2) The purposes for which the covered entity collects, uses, and retains such personal data;

(3) The persons, or categories of persons, to which, and purposes for which, the covered entity discloses such personal data;

(4) When such personal data will be destroyed, deleted, or de-identified. If the covered entity will not destroy, delete, or de-identify personal data, it shall specify this in the notice;

(5) The mechanisms to grant individuals a meaningful opportunity to access their personal data and grant, refuse, or revoke consent for the processing of personal data;

(6) Whom individuals may contact with inquiries or complaints concerning the covered entity's personal data processing; and

(7) The measures taken to secure personal data.

(c) Trade Secrets.—Nothing in this section shall require a covered entity to reveal trade secret information. For the purposes of this subsection, "trade secret" is defined as stated in 18 U.S.C. § 1839. However, for the purposes of this subsection, the categories of personal data that a covered entity collects shall not be considered a trade secret.

SEC. 102. Individual Control.

(a) In General.—Each covered entity shall provide individuals with reasonable means to control the processing of personal data about them in proportion to the privacy risk to the individual and consistent with context.

(b) Manner of Providing Individual Control.—In providing the means of control pursuant to subsection (a), the covered entity shall offer mechanisms that are—

(1) reasonably accessible, understandable, and usable to individuals; and

(2) available at times and in manners that reasonably enable individuals to make decisions about the processing of their personal data.

(c) Withdrawal of Consent.—Each covered entity shall provide individuals a means to withdraw any consent granted under subsection (b) that is reasonably comparable to the means used to grant such consent.

(1) Deletion in response to withdrawal of consent.—Within a reasonable period of time that need not be less than 45 days after receiving an individual's withdrawal of consent for data retention, a covered entity shall delete the

personal data associated with the withdrawal of consent.

(2) Alternative means of compliance.—A covered entity may meet the requirement of this subsection by providing individuals with the means to request that the covered entity de-identify personal data pertaining to such individuals.

(3) Limitation on the obligation of covered entities.—The obligation of a covered entity under this subsection shall be limited to—

(A) Responding in a manner that is compatible with a legal obligation of the covered entity, or any applicable First Amendment interest of the covered entity in the personal data;

(B) Processing of personal data other than those specified in subsection (d); and

(C) Personal data under the control of the covered entity.

(d) Exceptions.—A covered entity shall not be subject to the requirements of subsection (a), subsection (c), or a requirement to provide heightened individual control under section 103(b)(1) of this Act, to the extent that the collection, creation, processing, retention, use, or disclosure of personal data is for purposes set forth in the enumerated exceptions.

(e) Material Changes.—Covered entities shall, upon any material changes to a practice or service that affect the prior or ongoing collection, use, dissemination, or maintenance of personal data—

(1) provide in advance clear and conspicuous descriptions of the changes; and

(2) with respect to previously collected personal data, provide individuals with compensating controls designed to mitigate privacy risks that may arise from the material changes, which may include seeking express affirmative consent from individuals.

SEC. 103. Respect for Context.

(a) In General.—If a covered entity processes personal data in a manner that is reasonable in light of context, this section does not apply. Personal data processing that fulfills an individual's request shall be presumed to be reasonable in light of context.

(b) Privacy Risk Management.—If a covered entity processes personal data in a manner that is not reasonable in light of context, the covered entity shall conduct a privacy risk analysis including, but not limited to, reviews of data sources, systems, information flows, partnering entities, and data and analysis uses to examine the potential for privacy risk. Covered entities shall take reasonable steps to mitigate

any identified privacy risks, which shall include, but are not limited to, providing heightened transparency and individual control.

(1) Heightened Transparency and Individual Control.—Covered entities shall provide individuals with notice regarding personal data practices that are not reasonable in light of context at times and in a manner reasonably designed to enable individuals to decide whether to reduce their exposure to the associated privacy risk, as well as a mechanism for control that is reasonably designed to permit individuals to exercise choice to reduce such privacy risk. The factors relevant to determining whether such notice and mechanism for control are reasonably designed shall include, but are not limited to—

(A) The placement and visibility of such notices, taking into account the size and capability of the device that will display the notice;

(B) The timing and frequency of such notices in relationship to when personal data is collected, used, and disclosed; and

(C) The relationship of the notice to the means that the covered entity provides to permit individuals to exercise control over personal data processing.

(c) Exception for certain personal data analysis.—Nothing in subsection (b) shall require a covered entity to provide heightened transparency and individual control when a covered entity analyzes personal data in a manner that is not reasonable in light of context if such analysis is supervised by a Privacy Review Board approved by the Federal Trade Commission and—

(1) The Privacy Review Board determines that it is impractical to provide heightened transparency and individual control;

(2) The Privacy Review Board determines that the goals of the covered entity's analysis are likely to provide substantial benefits that do not exclusively accrue to the covered entity;

(3) The Privacy Review Board determines that the covered entity has taken reasonable steps to mitigate privacy risks associated with the analysis, including risks associated with the absence of heightened transparency and individual control; and

(4) The Privacy Review Board determines that the likely benefits of the analysis outweigh the likely privacy risks.

(d) Disparate Impact.—When analyzing personal data in a manner that is not reasonable in light of context and results in adverse actions concerning multiple individuals, a covered entity shall—

(1) Conduct a disparate impact analysis to determine whether the analysis of personal data described in subsection (d) results in a disparate impact on individuals on the basis of age, race, color, religion, sex, sexual orientation, gender identity, disability, or national origin;

(2) Ensure that the scope, rigor, and sophistication of the disparate impact analysis are consistent with widely accepted analytic and technical practices; and

(3) Document the methodology and results of the disparate impact analysis and retain such documentation consistent with widely accepted analytic and technical practices.

(e) Rulemaking.—Within 180 days after enactment of this Act, the Commission shall promulgate regulations under 5 U.S.C. § 553 to establish the minimum requirements for Privacy Review Boards to qualify for Commission approval, forms and procedures for submission of applications for approval, and a process for review and revocation of such approval. When promulgating regulations under this subsection, the Commission shall consider, among other factors: the range of evaluation processes suitable for covered entities of various sizes, experiences, and resources; the range of evaluation processes suitable for the privacy risks posed by various types of personal data; the costs and benefits of levels of independence and expertise; the costs and benefits of levels of transparency and confidentiality; the importance of mitigating privacy risks; the importance of expedient determinations; and whether differing requirements are appropriate for Boards that are internal or external to covered entities. Within 90 days of receipt, following public comment, the Commission shall approve or deny an application for Privacy Review Board approval, and explain in writing the reasons for any denial.

(f) Appeals.—A person aggrieved may obtain review by a district court of the United States of appropriate jurisdiction, as provided for in 5 U.S.C. § 706 of—

(1) any Commission decision on an application submitted under subsection (c); or

(2) a failure by the Commission, within the period specified in subsection (e) to approve or deny an application for Privacy Review Board approval.

SEC. 104. Focused Collection and Responsible Use.

(a) In General.—Each covered entity may only collect, retain, and use personal data in a manner that is reasonable in light of context. A covered entity shall consider ways to minimize privacy risk when determining its personal data collection, retention, and use practices.

(b) A covered entity shall delete, destroy, or de-identify personal data within a reasonable time after it has fulfilled the purpose or purposes for which such personal data were first collected.

(c) Exceptions.—Nothing in this section shall be construed to prohibit a covered entity from collecting, creating, processing, retaining, using, or disclosing personal data for—

(1) Purposes set forth in the enumerated exceptions;

(2) Processing personal data if the covered entity provides heightened transparency and individual control in a manner that satisfies the requirements of section 103(b) of this Act; or

(3) Performing an analysis under the supervision of a Privacy Review Board pursuant to section 103(c) of this Act.

SEC. 105. Security.

(a) In General.—Each covered entity shall—

(1) identify reasonably foreseeable internal and external risks to the privacy and security of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information;

(2) establish, implement, and maintain safeguards reasonably designed to ensure the security of such personal data, including but not limited to protecting against unauthorized loss, misuse, alteration, destruction, access to, or use of such information;

(3) regularly assess the sufficiency of any safeguards in place to control reasonably foreseeable internal and external risks; and

(4) evaluate and adjust such safeguards in light of the assessment in paragraph (3); any material changes in the operations or business arrangements of the covered entity; or any other circumstances that create a material impact on the privacy or security of personal data under control of the covered entity.

(b) Factors for safeguards.—The reasonableness of the safeguards that a covered entity adopts under subsection (a) shall be determined in light of—

(1) The degree of the privacy risk associated with the personal data under the covered entity's control;

(2) The foreseeability of threats to the security of such data;

(3) Widely accepted practices in administrative, technical, and physical safeguards for protecting personal data; and

(4) The cost of implementing and regularly reviewing such safeguards.

SEC. 106. Access and Accuracy.

(a) Access.—

(1) In General.—Each covered entity shall, upon the request of an individual, provide that individual with reasonable access to, or an accurate representation of, personal data that both pertains to such individual and is under the control of such covered entity. The degree and means of any access shall be reasonable and appropriate for the privacy risks associated with the personal data, the risk of adverse action against the individual if the data is inaccurate, and the cost to the covered entity of providing access to the individual.

(2) Limitations.—A covered entity shall not be required to provide such access if—
(A) the individual requesting access cannot reasonably verify his or her identity as the person to whom the personal data pertains;
(B) access by the individual to the personal data is limited by applicable law or legally recognized privilege, or any applicable First Amendment interest of the covered entity in that personal data;
(C) access by the individual would compromise a fraud investigation or a law enforcement, intelligence or national security purpose; or
(D) such request for access is frivolous or vexatious.

(b) Accuracy.—

(1) In General.—Each covered entity shall, in a manner that is reasonable and appropriate for the privacy risks associated with such personal data, establish, implement, and maintain procedures to ensure that the personal data under its control is accurate. In developing such procedures, the covered entity shall consider the costs and benefits of ensuring the accuracy of the personal data.

(2) Limitations.—The obligations in paragraph (1) do not apply to personal data that a covered entity obtains—
(A) From records made public by the Federal Government, the Government of any State, the Government of any Indian tribe, or any political subdivision of a State, provided that the covered entity at reasonable and regular intervals verifies that it is obtaining current versions of such sources; or
(B) Directly from the individual to whom the personal data pertains.

(c) Correction or Deletion.—

(1) In General.—Each covered entity shall, within a reasonable period of time after receiving a request from an individual, provide the individual with a means to dispute and resolve the accuracy or completeness of the personal data pertaining to that individual that is under the control of such entity. The means of resolving a dispute shall be reasonable and appropriate for the privacy risks and the risk of an adverse action against an individual that are associated with such personal data.

(2) Option to Decline Correction or Amendment.—When a covered entity uses or discloses personal data for purposes that could not reasonably result in an adverse action against an individual, the covered entity may decline to correct or amend the personal data. If the covered entity declines to correct or amend the personal data, the covered entity shall, upon request and authentication of the person making the request, destroy or delete the personal data that the covered entity maintains within a reasonable period of time that need not be less than 45 days, unless the data are exempt under subsection (b)(2)(A).

(3) Limitations.—A covered entity is not required under this subsection to—
(A) Fulfill a correction or deletion request when doing so would be incompatible with a legal obligation of the covered entity, or any applicable First Amendment interest of the covered entity in that personal data;
(B) Retain, maintain, reorganize, or restructure personal data;
(C) Correct personal data that it obtained under one or more of the conditions listed in subsection (b)(2)(A), except to the extent that an individual asserts that personal data derived from records made public by a governmental entity relate to a different individual; or
(D) Fulfill a deletion request if the data are processed or retained for purposes set forth in the enumerated exceptions.

(4) Additional Requirements Where Correction or Amendment Is Declined.—If the covered entity declines to correct or amend personal data at the request of an individual, and the covered entity obtained such personal data from another person or entity, the covered entity shall—
(A) correct any inaccuracy in the covered entity's records if the individual provides sufficient information to show that the personal data is incorrect; and
(B) inform the individual of the source of the data and, if reasonably available, where a request for correction may be directed.

(d) Activities Subject to the Fair Credit Reporting Act.—To the extent that the personal data pertaining to an individual is used for purposes covered by the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), covered entities subject to the Fair Credit Reporting Act shall be exempt from the requirements of section 106 of this Act.

SEC. 107. Accountability.

(a) In General.—Each covered entity shall take measures appropriate to the privacy risks associated with its personal data practices to ensure compliance with its obligations pursuant to this Act, including but not limited to—

(1) Providing training to employees who access, collect, create, use, process, maintain, or disclose personal data;

(2) Conducting internal or independent evaluation of its privacy and data protections;

(3) Building appropriate consideration for privacy and data protections into the design of its systems and practices; and

(4) Binding any person to whom the covered entity discloses personal data to use such data consistently with the covered entity's commitments with respect to the personal data and with the requirements set forth in Title I of this Act.

TITLE II.—Enforcement

SEC. 201. Enforcement by the Federal Trade Commission.

(a) Unfair or Deceptive Acts or Practices.—A violation of Title I of this Act shall be treated as an unfair or deceptive act or practice in violation of section 5 of the Federal Trade Commission Act (15 U.S.C. § 45).

(b) Powers of Commission—

(1) In General.—

(A) Any covered entity who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act, except that liability for and the amount of civil penalties shall be governed by section 203 of this Act.

(B) Exception.—The Commission shall not bring an enforcement action for violations of Title I of this Act seeking civil penalties based on a covered entity's conduct undertaken within the first eighteen months after the date the covered entity first created or processed personal data.

(c) General Application.—The requirements of this Act apply to—

(1) those "persons, partnerships, or corporations" 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)); and

(2) notwithstanding section 4 and section 5(a)(2) of that Act (15 U.S.C. §§ 44 and 45(a)(2)), any 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.

(d) In enforcing this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific device software or hardware.

SEC. 202. Enforcement by State Attorneys General.

(a) Civil Action.—If the attorney general of any State has reason to believe that the action of a covered entity in violation of Title I of this Act has caused or is causing harm to a substantial number of that State's residents, such attorney general may bring a civil action on behalf of those residents exclusively in an appropriate district court of the United States. Unless the Commission brings an action under section 201 of this Act or intervenes and prosecutes an action brought under this section, as described in subsections (b)(2)(A) and (b)(2)(B), the only remedy that may be sought or awarded in any action under this Act is injunctive relief, and nothing in this Act may be construed to provide for any other relief.

(b) Federal Trade Commission.—

(1) Notice to Federal Trade Commission.—At least 30 days prior to initiating any action under subsection (a), an attorney general shall provide the Commission with a copy of the entire court complaint and written disclosure of substantially all material evidence and information the attorney general possesses.

(2) Upon receiving notice from an attorney general of a proposed civil action, the Commission may—

(A) intervene as a matter of right as a party to that civil action;
(B) intervene as a matter of right as a party to that civil action and assume lead responsibility for the prosecution of the action; or
(C) permit the attorney general to proceed with the action without direct Commission participation.

(3) In the event that an attorney general believes that immediate action is necessary to protect the residents of the State from a substantial harm, the attorney general may request that the Commission expedite its review of the proposed action, and the Commission shall afford such request appropriate consideration as the circumstances may warrant.

(4) In any action brought under Title II of this Act, the district court, and any courts that review the district court's decision, shall accord substantial weight to the Commission's interpretations as to the legal requirements of this Act.

(c) 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. 203. Civil Penalties.

(a) In General.—In an action brought by the Commission or prosecuted by the Commission pursuant to section 202(b)(2)(A) or section 202(b)(2)(B), in addition to any injunctive relief arising from a violation of Title I of this Act, the covered entity is liable for a civil penalty if the covered entity, with actual knowledge or knowledge fairly implied on the basis of objective circumstances, violates the Act. Both the amount of such civil penalty sought by the Commission and the amount of such civil penalty determined by the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(1) The civil penalty shall be calculated by multiplying the number of days that the covered entity violates the Act by an amount not to exceed $35,000; or

(2) If the Commission provides notice to a covered entity, stated with particularity, that identifies a violation of this Act, the civil penalty shall be calculated by multiplying the number of directly affected consumers by an amount not to exceed $5,000, unless, within 45 days of receiving such a notice, the covered entity files with the Commission an objection that satisfies the requirements of subparagraph (A).

(A) An objection shall include an affidavit by the covered entity that to the best of the covered entity's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances—

(i) it is not being filed for any improper purpose;
(ii) the defenses and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law;
(iii) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation; and
(iv) the denial of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.

(3) The total civil penalty determined by the court shall not exceed $25,000,000.

(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.

TITLE III.—Codes of Conduct to Implement the Consumer Privacy Bill of Rights

SEC. 301. Safe Harbor Through Enforceable Codes of Conduct.

(a) Commission Review of Codes of Conduct.—

(1) Beginning 1 day after the effective date of Commission regulations adopted under subsection (c), any person may apply to the Commission for approval of one or more codes of conduct governing the processing of personal data by a covered entity. Such application shall include—

(A) A description of how the proposed code provides equivalent or greater protections for personal data than are provided by the relevant section of Title I;

(B) A description of entities or activities the code is designed to cover;

(C) A description of the process by which the code was derived;

(D) A list of covered entities, if any are known at the time that the application under this subsection is made, that plan to adopt the code; and

(E) Such additional information as the Commission determines is appropriate.

(2) Timeline for Commission Review.—

(A) Department of Commerce Multistakeholder Processes.—The Secretary of Commerce may convene interested stakeholders, such as members of industry, civil society, the public safety community, and academia, to develop codes of conduct through an open, transparent process. The Commission shall approve or deny an application developed through a Department of Commerce multistakeholder process within 90 days after receipt.

(B) Within 120 days of receipt, and consistent with the other regulations adopted under subsection (c), the Commission shall approve or deny an application that concerns a code of conduct that was developed through a process that—

(i) Is open to all interested participants and allows them to participate on equal footing in the deliberations and discussions that lead to the code; and

(ii) Maintains transparency by, at minimum, making decisional documents readily available to the public at a time and in manner that permits meaningful review prior to any decision based upon such documents.

(C) Consistent with the other regulations adopted under subsection (c), the Commission shall approve or deny a code of conduct developed through any process not covered by subparagraph (A) or (B) within 180 days of receipt.

(3) Public Comment and Explanation of Decisions.—

(A) As soon as feasible after receipt of any proposed code of conduct, the Commission shall provide an opportunity for public comment on the code.

(B) The Commission shall publicly explain in writing the reasons for approving or denying each proposed code of conduct that it reviews pursuant to this section.

(4) Initial Approval.—The Commission shall approve an application only if the applicant demonstrates that the associated code of conduct—

(A) provides equivalent or greater protections for personal data pertaining to individuals than those provided by Title I of this Act; and

(B) contains provisions for periodic review of the code of conduct to ensure that it continues to provide sufficient protection over time for personal data pertaining to individuals.

(5) Presumption of Sufficiency.—Codes of conduct developed through a multistakeholder process pursuant to paragraph (2)(A) that meet the requirements established by the Commission shall be presumed to provide equivalent or greater protections for personal data as those provided by Title I of this Act. A Commission finding to the contrary shall be supported by a decision in writing.

(6) Duration.—

(A) No sooner than 3 years and no later than 5 years after approving a code of conduct, the Commission shall reassess such code. If the Commission determines that the code continues to provide equivalent or greater protections for personal data pertaining to individuals than those provided by Title I of this Act, in light of changes in consumer expectations, technology, and market conditions, the code shall continue to qualify as a safe harbor pursuant to subsection (d) for a period of no longer than 5 years following the determination.

(B) Notwithstanding subparagraph (A), the Commission, upon request or on its own motion, may reconsider an approval granted under paragraph (4). After receiving public comment, if the Commission determines, based on specific factors or evidence not available in the prior proceeding, that clearly demonstrate that a code of conduct does not or no longer provides equivalent or greater protections for personal data pertaining to individuals

than those provided by Title I of this Act, it shall withdraw its approval of such code of conduct.

(b) Non-Governmental Administration of Codes of Conduct.—

(1) Beginning 1 day after the effective date of Commission regulations adopted under subsection (c), any person may apply to the Commission for certification to administer and enforce one or more codes of conduct that have been approved by the Commission under subsection (a).

(2) The Commission shall approve an application only if an applicant demonstrates that it can effectively and expeditiously address and resolve alleged violations of each code of conduct administered by that applicant.

(3) Commission certification under this subsection shall be effective for no more than 5 years. The Commission, upon request or on its own motion, may review a person's administration of a code of conduct to determine whether, in light of changes in consumer expectations, technology, and market conditions, such person continues to provide adequate protection for individuals and their personal data. If the Commission determines, after receiving public comment, that a person's administration or enforcement of a code of conduct does not adequately protect individuals and their personal data, the Commission shall withdraw its certification under this subsection.

(4) Each year, each person certified by the Commission under this subsection shall submit to the Commission, in a form specified by the Commission, a report of its activities under this Title during the preceding year.

(c) Rulemaking.—Within 180 days after enactment of this Act, the Commission shall promulgate regulations under 5 U.S.C. § 553 to implement this Title, including regulations establishing—

(1) the minimum requirements for a process to qualify for the presumption in subsection (a)(5);

(2) procedural requirements for codes of conduct under subsection (a);

(3) procedural requirements for entities that wish to administer codes of conduct under subsection (b);

(4) forms and procedures for the submission of applications under subsections (a) and (b); and

(5) methods and procedures for receiving input from governmental agencies regarding the approval of codes of conduct, including procedures that govern submittal of classified or otherwise confidential information.

(d) Safe Harbor Protection.—In any suit or action brought under Title II of this Act for alleged violations of Title I of this Act, the defendant shall have a complete defense to each alleged violation of Title I of this Act if it demonstrates with respect to such an alleged violation that it has maintained a public commitment to adhere to a Commission-approved code of conduct that covers the practices that underlie the suit or action and is in compliance with such code of conduct.

(e) Appeals.—A person aggrieved may obtain review by a district court of the United States of appropriate jurisdiction, as provided for in 5 U.S.C. § 706 of—

(1) any Commission decision approving or denying an application submitted under subsections (a) or (b); or

(2) a failure by the Commission, within the periods specified in subsections (a)(2) and (c), to approve or deny a code of conduct.

TITLE IV.—Miscellaneous

SEC. 401. Preemption.

(a) In General.—This Act preempts any provision of a statute, regulation, or rule of a State or local government, with respect to those entities covered pursuant to this Act, to the extent that the provision imposes requirements on covered entities with respect to personal data processing.

(b) Safe Harbor Protection.—No State or local government may enforce any personal data processing law against a covered entity to the extent that that entity is entitled to safe harbor protection under section 301(d) of this Act.

(c) Protection of State Consumer Protection Laws.—This section shall not be construed to limit the enforcement by an attorney general or other official of a State of any State consumer protection law of general application and not specific to personal data processing.

(d) Protection of Certain State and Local Laws.—This Act shall not be construed to preempt the applicability of the following, to the extent that the claim in question is not based on a failure to comply with this Act—

(1) State or local laws that address the processing of health information or financial information;

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

(3) State or local trespass, contract, or tort law;

(4) State or local laws that address the privacy of minors or K-12 students; or

(5) Other State or local laws to the extent that those laws relate to fraud or public safety.

SEC. 402. Preservation of Federal Trade Commission Authority.

(a) Deception.—Nothing in this Act shall be construed to limit the Commission's authority under section 5 of the FTC Act (15 U.S.C. § 41 *et seq.*) to prevent any deceptive act or practice relating to personal data processing.

(b) Unfairness.—Nothing in this Act shall be construed to limit the Commission's authority to prevent unfair acts or practices relating to personal data processing, except the conduct that underlies a claim by the Commission that a covered entity breached a commitment that it made as part of its adherence to a code of conduct approved under section 301 of this Act.

SEC. 403. Private Right of Action.

There shall be no private right of action under this Act, and nothing in this Act may be construed to provide a private right of action.

SEC. 404. Application with Other Laws.

(a) Rule of Construction.—Nothing in this Act shall be construed or applied so as to abridge the exercise of rights guaranteed under the First Amendment to the Constitution of the United States.

(b) Exemption for Certain Internet Intermediaries.—To the extent that a covered entity qualifies for protection under section 230(c) of the Communications Act of 1934 (47 U.S.C. § 230(c)), processing of personal data protected by section 230(c) is exempt from the requirements of this Act with regard to a request from a person other than the original "information content provider" as defined in 47 U.S.C. § 230(f)(3).

(c) Qualified Exemption for Persons Subject to Other Federal Privacy and Security Laws.—If a covered entity is subject to a provision of this Act and a comparable provision of a Federal privacy or security 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 or security law applies to such person.

(d) Effect on Other Federal Laws—

(1) Protection of Other Federal Privacy and Security Laws.—Nothing in this Act may be construed to modify, limit, or supersede the operation of privacy or security provisions in Federal laws, including those described in subsection (d), or the regulations established pursuant to such laws, or the provision of information

permitted or required, expressly or by implication, by such laws, with respect to Federal rights and practices.

(2) Effect on FTC Act.—Notwithstanding paragraph (1), the Federal Trade Commission Act shall be modified as described in Section 402 of this Act.

(e) The Federal privacy and security 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 (15 U.S.C. § 6801 *et seq.*).

(7) Chapters 119, 123, 206, and 121 of Title 18, United States Code.

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

(9) Sections 444 and 445 of the General Education Provisions Act (20 U.S.C. §§ 1232g, 1232h), commonly known as the "Family Educational Rights and Privacy Act of 1974" and the "Protection of Pupil Rights Amendment," respectively.

(10) Sections 5701 and 7332 of Title 38, United States Code.

(11) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-2 *et seq.*).

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

(13) The provisions of part C of title XI of the Social Security Act, section 264 of the Health Insurance Portability and Accountability Act of 1996, and subtitle D of title IV of the Health Information Technology for Economic and Clinical Health Act, and regulations under such provisions.

(14) The E-Government Act of 2002 (44 U.S.C. § 101 *et seq.*).

(15) The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 *et seq.*).

(16) Federal Information Security Management Act of 2002 (44 U.S.C. § 3541 *et seq.*).

(17) The Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

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

(19) The Currency and Foreign Transactions Reporting Act of 1970, as amended (commonly known as the Bank Secrecy Act) (12 U.S.C. §§ 1829b and 1951-1959, 31 U.S.C. §§ 5311-5314 and 5316-5332), including the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, Title III of P.L. 107-56, as amended.

(20) Executive Order 12333, as amended, "United States Intelligence Activities, July 30, 2008," and any successor orders.

(21) National Security Act of 1947.

(22) Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. § 1801 *et seq.*).

SEC. 405. Exceptions to the Definition of Covered Entity.

Rulemaking.—The Commission may promulgate regulations under 5 U.S.C. § 553 to establish additional exceptions from the definition of covered entity for categories of persons. When promulgating regulations under this section, the Commission shall consider, among other factors, the privacy risks posed by personal data processing by categories of persons of various sizes, experiences, resources, and types of commercial activity, including nonprofit activity; the importance of mitigating privacy risks; and the costs and benefits of including those categories of persons as covered entities. A person aggrieved by a regulation promulgated under this subsection may obtain review by a district court of the United States of appropriate jurisdiction, as provided for in 5 U.S.C. § 706. The Commission may modify or revoke such an exception in light of changes in consumer expectations, technology, and market conditions, but no sooner than 3 years after initial promulgation absent materially changed circumstances.

SEC. 406. Effective Date.

(a) The provisions of this Act will take effect as of the date of enactment.

(b) The obligations of covered entities under Title I of this Act shall not give rise to a cause of action based on this Act less than 2 years after the date of enactment of this Act.

SEC. 407. Severability.

If any provision of this Act, or the application thereof to any person or circumstance, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other persons and circumstances shall not be affected thereby.