116TH CONGRESS
1ST SESSION

S. [redacted]

To establish and protect individual and collective privacy rights, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MARKEY introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To establish and protect individual and collective privacy rights, 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 ''Privacy Bill of Rights Act''.
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—The term ''breach of security'' means any instance in which a person, without authorization or in violation of any authorization provided to the person, gains access to, uses, or discloses personal information.

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

(3) COVERED ENTITY.—The term ''covered entity'' means any person that collects or otherwise obtains personal information.

(4) DATA BROKER.—The term ''data broker'' means a commercial entity that collects, assembles, or maintains personal information concerning an individual who is not a customer or employee of the entity, and who has not established a subscription or account with the entity, in order to sell the information or provide third-party access to the information.

(5) DE-IDENTIFIED.—The term ''de-identified'', with respect to information, means information that cannot reasonably identify, relate to, describe, or be capable of being associated with or linked to, directly or indirectly, a particular individual.
(6) DISCLOSE.—The term ''disclose'' means to disclose, release, transfer, share, disseminate, make available, or otherwise communicate orally, in writing, electronically, or by any other means to any third party.

(7) MINOR.—The term ''minor'' means any individual who is under 16 years of age.
(8) MOBILE APPLICATION.—The term ''mobile application'' means a software program that runs on the operating system of a mobile device.
(9) OPT-IN APPROVAL.—The term ''opt-in approval'' means affirmative, express consent of an individual for a covered entity to use, disclose, or permit access to the individual's personal information after the individual has received explicit notification
of the request of the covered entity with respect to that information.
(10) PERSONAL INFORMATION.—
(A) IN GENERAL.—The term ''personal information'' means information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to, a particular individual.
(B) EXAMPLES.—The term ''personal information'' includes—
(i) an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifier;
(ii) information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other financial information, medical information, mental health information, or health insurance information;
(iii) commercial information, including a record of personal property, income, assets, leases, rentals, products or services purchased, obtained, or considered, or other purchasing or consuming history;
(iv) biometric information, including a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry;
(v) internet or other electronic network activity information, including browsing history, search history, content, including text, photographs, audio or video recordings, or other user generated-content, non-public communications, and information regarding an individual's interaction with an internet website, mobile application, or advertisement;
(vi) historical or real-time geolocation data;
(vii) audio, electronic, visual, thermal, olfactory, or similar information;
(viii) education records, as defined in section 99.3 of title 34, Code of Federal Regulations, or any successor regulation;
(ix) political information or information on criminal convictions or arrests;
(x) any required security code, access code, password, or username

necessary to permit access to the account of an individual;
(xi) characteristics of protected classes under Federal law, including race, color, national origin, religion, sex, age, or disability; or
(xii) an inference drawn from any of the information described in this subparagraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

(C) EXCLUSIONS.—
(i) IN GENERAL.—The term ''personal information'' does not include publicly available information.
(ii) PUBLICLY AVAILABLE INFORMATION.—For purposes of clause (i), the term ''publicly available information''—
(I) means information that is lawfully made available from Federal, State, or local government records; and
(II) does not include—
(aa) biometric information collected by a covered entity about an individual without the individual's knowledge;
(bb) information used for a purpose that is not compatible with the purpose for which the information is maintained and made available in government records; or
(cc) information of an individual that is de-identified.

(11) THIRD PARTY.—The term ''third party'', with respect to personal information of an individual, means any person that is not—

(A) the covered entity that is disclosing the personal information;

(B) solely performing an outsourced function of the covered entity disclosing the personal information if—

(i) the person is contractually or legally prohibited from using, retaining, sharing, or selling the personal information after the conclusion of the outsourced function; and
(ii) the person is complying with the regulations promulgated under this Act; or

(C) a person with respect to which the individual gave specific opt-in approval for the covered entity to disclose the personal information of the individual to the person.

SEC. 3. ACT PROHIBITED.

(a) IN GENERAL.—It shall be unlawful for a covered entity to violate the privacy of an individual in a manner that violates a regulation promulgated under this Act.

(b) REGULATIONS.—In carrying out this Act, the Commission shall—

(1) not later than 1 year after the date of enactment of this Act, promulgate regulations under section 553 of title 5, United States Code, to protect the individual and collective privacy rights set forth in this Act;

(2) ensure the regulations promulgated under paragraph (1) take effect not later than 90 days after the date on which the regulations are promulgated;

(3) establish a centralized internet website for the benefit of individuals that provides information to individuals about their rights under this Act in a clear, concise, well-organized, understandably written, and complete manner; and
(4) establish a centralized internet website for the benefit of individuals that lists each data broker in the United States.

SEC. 4. RIGHT TO NOTICE.

(a) IN GENERAL.—In promulgating regulations under section 3, the Commission shall require a covered entity to—
(1) develop and make available to customers a short-form notice about the collection, retention, use, and sharing of the personal information of individuals by the covered entity that includes—
(A) what personal information is being collected, used, or retained;
(B) the manner in which the personal information is collected;
(C) how and for what purpose the covered entity is collecting, using, retaining, sharing, or selling the personal information;
(D) how long the personal information will be held;

(E) which third parties the covered entity shares personal information with or leases or sells personal information to, not including—
(i) a governmental entity with which the covered entity shares personal information pursuant to a court order or law that prohibits the covered entity from revealing that instance of sharing to the individual to whom the personal information pertains;
(ii) a third party if the personal information is—
(I) made available to and readily accessible by the general public with the consent of the individual to whom the personal information pertains; and
(II) shared with, or leased or sold to, the third party through a mechanism available to any member of the general public; or
(iii) a third party with which the covered entity shares, or to which the covered entity leases or sells, personal information of an individual that the covered entity did not obtain from the individual, if revealing that instance of sharing, leasing, or selling personal information would expose another

individual to likely harm;

(F) in the case of the sharing, leasing, or selling of personal information described in sub- paragraph (E) that is not excluded under clause (i), (ii), or (iii) of that subparagraph, what personal information is shared with or leased or sold to third parties and for what purpose;

(G) how an individual can access, correct, and delete the personal information of the individual that the covered entity retains as required under section 6;

(H) the practices of the covered entity for collecting personal information of an individual, including offline practices, when the individual is not directly interacting with the covered entity;

(I) the practices of the covered entity for using personal information in automated decision-making; and

(J) the right of an individual to provide opt-in approval and revoke approval consistent with section 5;

(2) ensure that the short-form notice developed under paragraph (1)—

(A) is clear, concise, well-organized, understandably written, and complete;

(B) does not contain unrelated, confusing, or contradictory materials; and

(C) is in a format that is—

(i) prominent and easily accessible;

(ii) of reasonable length; and

(iii) clearly distinguishable from other matters;

(3) not later than 15 days after making a material change to the privacy practices or policies of the covered entity, update the short-form notice developed under paragraph (1);

(4) make the short-form notice required under paragraph (1) persistently and conspicuously available—

(A) on the website or mobile application of the covered entity, if the covered entity maintains a website or mobile application; and

(B) at the physical place of business or any other offline equivalent maintained by the covered entity; and

(5) ensure that the short-form notice required under paragraph (1) is made available to an individual—

(A)

(i) at the point of sale of a product or service of, subscription to a service of, or establishment of an account with, the covered entity, prior to the sale, subscription, or establishment, whether that point of sale, subscription, or establishment is in person, online, over the telephone, or through another means; or

(ii) if there is no such sale, subscription, or establishment, before the individual uses the product or service of the covered entity; and

(B) regardless of the decision of the individual as to whether to provide opt-in approval to the covered entity.

(b) REQUIREMENTS FOR UNEXPECTED COLLECTION OR USE OF PERSONAL INFORMATION.—

(1) IN GENERAL.—In promulgating regulations under section 3, the Commission shall apply the requirements under paragraph (2) of this subsection to any collection or use of personal information of an individual by a covered entity other than collection or use that—

(A) is necessary for the performance of a contract to which the individual is party;

(B) consists of actions that an individual would consider necessary in order to provide a requested product or service; or

(C) consists of actions taken at the request of the individual prior to entering into a contract to which the individual is party.

(2) REQUIREMENTS.—A covered entity that is subject to paragraph (1), with respect to any individual whose personal information the covered entity collects or uses as described in that paragraph—

(A) shall provide the short-form notice developed under subsection (a)(1) to the individual in a manner that ensures that the individual reviews the notice and can provide opt-in approval under section 5;

(B) shall notify the individual of any material change to the privacy practices or policies of the covered entity not later than the date on which the covered entity updates the short-form notice under subsection (a)(3);

(C) may not collect any personal information of the individual not specified in the short form notice most recently provided to the individual in accordance with subparagraph (A) unless the covered entity provides the individual with a new short-form notice consistent with that subparagraph at the point of collection of the additional information; and

(D) may not use personal information of the individual for a purpose not specified in the short-form notice most recently provided to the individual in accordance with subparagraph (A) unless the covered entity provides the individual with a new short-form notice consistent with that paragraph that discloses the additional purpose.

(c) STANDARDIZED SHORT-FORM PRIVACY NOTICE.—

(1) STANDARDIZED NOTICE.—The Commission shall establish standardized short-form privacy notices that comply with this section.

(2) USE OF STANDARDIZED NOTICE.—A covered entity may satisfy the requirements of sub-section (a) by adopting a standardized short-form privacy notice established by the Commission under paragraph (1) of this subsection.

(d) JOINT NOTICE FOR AFFILIATED COVERED ENTITIES.—Two or more affiliated covered entities may use a single joint short-form notice for purposes of this section if the short-form notice—

(1) states that the notice applies to multiple affiliated covered entities and names each such covered entity; and

(2) is accurate with respect to the actions of each covered entity using the notice.

SEC. 5. RIGHT TO CONTROL.

(a) OPT-IN APPROVAL REQUIRED.—In promulgating regulations under section 3, the Commission shall require a covered entity to obtain opt-in approval from an individual to—

(1) collect, use, retain, share, or sell the individual's personal information; or

(2) make any material changes in the collection, use, retention, sharing, or sale of the individual's personal information.

(b) RULES FOR APPROVAL.—

(1) PROCEDURES.—A covered entity shall obtain approval under subsection (a) in accordance with the procedures for notification under section 4.

(2) MANNER.—In order to satisfy subsection (a), approval shall be freely given, specific, informed, and unambiguous.

(3) WITHDRAWAL.—An individual shall have the right to withdraw his or her approval at any time.

(4) MEANS.—A covered entity shall seek to obtain approval through the primary medium used to offer or deliver the covered entity's product or service.

(c) EXCEPTIONS.—A covered entity shall not be required to obtain opt-in approval from an individual under subsection (a)—

(1) if collection is necessary for the performance of a contract to which the individual is party;

(2) to take steps that an individual would consider necessary in order to provide a requested product or service; or
(3) to take steps at the request of the individual prior to entering into a contract to which the individual is party.

(d) EMERGENCY OR EXIGENT CIRCUMSTANCES.—
(1) IN GENERAL.—Subject to paragraph (2), a covered entity shall not be required to obtain opt-in approval under subsection (a) if the covered entity, in good faith, believes danger of death or serious physical injury to any individual requires use, access, or disclosure without delay of personal information relating to the emergency.

(2) NOTICE REQUIREMENT.—Not later than 90 days after the date on which a covered entity uses, accesses, or discloses personal information of an individual without obtaining opt-in approval under paragraph (1), the covered entity shall inform the individual of—
(A) the personal information that the covered entity used, accessed, or disclosed;
(B) the details of the emergency or exigent circumstances; and
(C) the reasons why the covered entity needed to use, access, or disclose the personal information.

(e) EXEMPTIONS.—

(1) IN GENERAL.—In promulgating regulations under subsection (a), the Commission may grant an exemption to a specific covered entity from the control requirements under this section after taking into account—

(A) privacy risks posed by the use of personal information by the covered entity;

(B) the costs and benefits of applying the regulations to the covered entity; and

(C) whether—

(i) the personal information held by the covered entity is—

(I) necessary and used, retained, or shared only to protect the security of the covered entity's service;
(II)
(aa) necessary for providing a service requested by an individual; and
(bb) consistent with the context of the service provided;
(III) necessary to initiate, render, bill for, or collect payment for a

service or product requested by an individual from the covered entity; or

(IV) necessary to protect—

(aa) the rights or property of the covered entity; or

(bb) individuals who use the services or products provided by the covered entity or other covered entities from fraudulent, abusive, or unlawful use of the service or product; or

(ii) the covered entity—

(I) de-identifies the personal information held by the covered entity; and

(II) where possible, provides individuals with the choice to opt-out of the collection and use of the de-identified information of the individuals.

(2) REPORTING REQUIREMENT.—If the Commission grants an exemption to a covered entity under paragraph (1), the Commission shall list the covered entity on the website of the Commission established under section 3(b)(3) and provide a brief justification for granting the exemption to the covered entity.

SEC. 6. RIGHT TO ACCESS, CORRECTION, DELETION, AND DATA PORTABILITY.

(a) IN GENERAL.—In promulgating regulations under section 3, the Commission shall require a covered entity to—

(1) upon request, provide confirmation to an individual who uses a product or service of the covered entity, or has established a subscription or account with the covered entity, as to whether the covered entity retains personal information pertaining to the individual;

(2) if the covered entity retains the individual's personal information, provide to the individual—

(A) reasonable means to access the personal information;

(B) a description of—

(i) the personal information being retained;

(ii) each date on which the covered entity collected the personal information;

(iii) the third parties to which the covered entity has disclosed or will disclose the personal information; and

(iv) if possible, how long the personal information will be retained or stored, or if not possible, the criteria used for determining how long the personal information will be retained or stored; and

(C) notice of the right to correct and delete personal information;

(3) provide the access to the personal information under paragraph (2)(A) in the form of a portable electronic table that—

(A) is in a usable and searchable format;
(B) allows the individual to transfer the personal information from one entity to another entity without hindrance; and

(C) to the extent that the Commission determines practicable and appropriate, delineates between—
(i) personal information collected and shared in order to provide the individual with the desired product or service; and
(ii) personal information that was sold by the covered entity to a third party;
(4) provide an individual with a mechanism to correct inaccurate personal information retained or stored by the covered entity;
(5)
(A) provide an individual with a mechanism to request the deletion of the personal information of the individual that the covered entity retains or stores about the individual; and
(B) when the covered entity receives a request from an individual under subparagraph (A), delete the personal information collected from the individual unless the covered entity needs to retain the personal information in order to—
(i)
(I) complete the transaction for which the personal information was collected;
(II) provide a good or service requested by the individual or reasonably anticipated within the context of the covered entity's ongoing relationship with the individual; or
(III) otherwise perform a contract to which the individual is party;
(ii) detect security incidents, protect against activity that violates the covered entity's terms of service or malicious, deceptive, fraudulent, or illegal activity, or prosecute persons responsible for such activity;
(iii) debug to identify and repair errors that impair existing functionality;
(iv) exercise free speech, ensure the ability of another individual to exercise his or her right to free speech, or exercise another right provided for by law;
(v) comply with chapter 119, 121, or 206 of title 18, United States Code;
(vi) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, if—
(I) the covered entity's deletion of the information is likely to render impossible or seriously impair the achievement of such research;

(II) the individual has provided informed consent; and

(III) the research is already in progress at the time that deletion is requested; or

(vii) comply with a legal obligation;

(6) provide the mechanisms under paragraphs (4) and (5) in a form that is—

(A) clear and conspicuous; and

(B) made available—

(i) at no additional cost to the user;

(ii) without requiring an individual to establish an account with the covered entity;

(iii) in a language other than English, if the provider transacts business with individuals in that other language;

(iv) to individuals regardless of whether the information was obtained by the covered entity directly from the individual, not to include publicly available or de-identified personal information;

(v)

(I) through a toll-free number;

(II) on the covered entity's website, if the covered entity maintains a website; or

(III) through the primary mechanism through which the covered entity engages in a relationship with the individual in order to provide a product or service; and

(vi) such that an individual has the opportunity to request correction or deletion of personal information not less frequently than once every 6 months;

(7) inform any entity with which the covered entity has shared, sold, or disclosed an individual's personal information of any request from the individual for confirmation of, access to, correction of, or deletion of the individual's personal information under this subsection;

(8) comply with an individual's request for confirmation, access, correction, or deletion under this subsection even if the request is received from another covered entity, if the receiving covered entity can verify that the request is originally from the individual; and

(9) comply with an individual's request for confirmation, access, correction, or deletion under this subsection not later than 90 days after receiving a verifiable request from the individual or another covered entity.

(b) RIGHT OF PARENTS AND GUARDIANS OF MINORS.—For purposes of subsection (a), a parent or guardian of a minor may act on behalf of the minor with respect to personal information of the minor held by a covered entity, including by requesting confirmation of, access to, correction of, or deletion of the personal

information.

(c) PROHIBITION ON DE-IDENTIFYING PERSONAL INFORMATION SUBSEQUENT TO REQUEST.—A covered entity may not de-identify an individual's personal information during the 90-day period beginning on the date on which the covered entity receives a request from the individual for confirmation, access, correction, or deletion of the individual's personal information under subsection (a).

SEC. 7. PROHIBITION ON RE-IDENTIFYING PERSONAL INFORMATION.

(a) IN GENERAL.—In promulgating regulations under section 3, the Commission shall require a covered entity to ensure that personal information that has been de-identified is not restored such that the information can be linked to a specific individual or device.

(b) ACTIONS REQUIRED.—In carrying out subsection (a), the Commission shall—

(1) require a covered entity to implement—

(A) technical safeguards that prohibit identification of the individual to whom or device to which the information may pertain;

(B) processes that specifically prohibit re-identification of the information; and

(C) processes that prevent inadvertent release of de-identified information; and

(2) prohibit a covered entity from making any attempt to reidentify the information.

SEC. 8. PROHIBITION ON TAKE-IT-OR-LEAVE-IT.

A covered entity may not refuse to serve an individual who does not approve the collection, use, retention, sharing, or sale of the individual's personal information for commercial purposes on the basis of that lack of approval (commonly known as a ''take-it-or-leave-it-offer'').

SEC. 9. PROHIBITION ON FINANCIAL INCENTIVES.

(a) IN GENERAL.—A covered entity may not offer an individual a program that relates the price of a product or service to the privacy protections afforded the individual, including by providing a discount or other incentive in exchange for the opt-in approval of the individual to the use and sharing of the individual's personal information.

(b) RULE OF CONSTRUCTION.—Nothing in sub-section (a) shall be construed to prohibit the relation of price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and used only for the purpose of initiating, rendering, billing

for, or collecting payment for a service or product requested by the individual from the covered entity.

(c) EXEMPTIONS.—The Commission may exempt a specific type of financial incentive offered by a particular covered entity from the prohibition under subsection (a) if the Commission determines that the type of financial incentive, as offered by that covered entity, is reasonable, just, and non-coercive.

SEC. 10. PROHIBITION ON DISCLOSING INFORMATION TO THIRD PARTIES WITHOUT PROPER ASSURANCES.

(a) IN GENERAL.—A covered entity may not disclose the personal information of an individual to a third party under a written contract unless—

(1) the contract prohibits the third party from—

(A) using the personal information for any reason other than performing the specified service on behalf of the covered entity; or

(B) disclosing the personal information to another third party for any reason other than performing the specified service on behalf of the covered entity; and

(2) the covered entity ensures that the third party effectively enforces the prohibitions described in paragraph (1), including by auditing the data security and data information practices of the third party not less frequently than once every 2 years.

(b) RULE OF CONSTRUCTION.—Nothing in sub-section (a) shall be construed to prevent the disclosure of personal information of an individual—

(1) by a covered entity to a third party if necessary to comply with applicable law or a court-issued subpoena, warrant, or order;

(2) by a covered entity to a third party that is reasonably necessary to—

(A) address fraud, security, or technical issues;

(B) protect the individual's rights or property; or

(C) protect individuals or the public from illegal activities as required or permitted by law; or

(3) if the individual has specifically approved of the disclosure.

SEC. 11. USE LIMITATIONS.

(a) IN GENERAL.—In promulgating regulations under section 3, the Commission shall prohibit a covered entity from using personal information for unreasonable purposes, including—

(1) selling, leasing, trading, or otherwise profiting from an individual's biometric information;

(2) sharing, resharing, or otherwise disseminating an individual's biometric

information without first obtaining specific consent from the individual, unless—

(A) the dissemination is required by state or Federal law or municipal ordinance; or

(B) the dissemination is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction;

(3) processing personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, healthcare, credit, insurance, housing, or education opportunities, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person's or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability; or

(4) processing personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person's or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, or disability.

(b) DEFINITION OF PLACE OF PUBLIC ACCOMMODATION.—For purposes of subsection (a), the term ''place of public accommodation'' means—

(1) any entity considered a place of public accommodation under section 201(b) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(b)) or section 301 of the Americans with Disabilities Act of 1990 (42 U.S.C. 12181); and

(2) any entity that offers goods or services through the internet to the general public.

SEC. 12. DATA MINIMIZATION.

In promulgating regulations under section 3, the Commission shall prohibit a covered entity from—

(1) collecting personal information of an individual beyond what is adequate, relevant, and necessary—

(A) for the performance of a contract to which the individual is party;

(B) to provide a requested product or service; or

(C) to take steps at the request of the individual prior to entering into a contract to which the individual is party; or

(2) accessing the personal information of an individual later than 90 days after the latest date on which—

(A) the covered entity concludes the performance of a contract to which the individual is party;

(B) the covered entity concludes taking steps that an individual would consider necessary in order to provide a requested product or service, including steps to prevent fraud, ensure safety, or ensure compliance with the covered entity's terms of service; or
(C) the individual otherwise terminates his or her relationship with the covered entity.

SEC. 13. RIGHT TO DATA SECURITY.

(a) REASONABLE PROCEDURES.—
(1) IN GENERAL.—In promulgating regulations under section 3, the Commission shall require a covered entity to establish and maintain reasonable data security practices to protect the confidentiality, integrity, and availability of personal information.
(2) PROPORTIONALITY.—The requirements prescribed under paragraph (1) shall provide for security procedures that are proportional to the volume and nature of the personal information a covered entity collects.
(3) COMMISSION GUIDANCE; INDUSTRY PRACTICES.—The requirements prescribed under paragraph (1) shall be consistent with guidance provided by the Commission and recognized industry practices for safety and security, including administrative, technical, and physical safeguards to secure the personal information of users.
(4) TECHNOLOGICALLY NEUTRAL.—The Commission may not require a specific technological means of meeting a requirement under paragraph (1).
(b) OTHER REQUIREMENTS.—In promulgating regulations under section 3, the Commission shall require a covered entity—

(1) to make publicly available a description of the practices established by the covered entity under subsection (a) that details—
(A) how the covered entity will address privacy and security risks associated with the development of new products and services;
(B) the access that employees and contractors of the covered entity have to the personal information of an individual who uses a service or product of the covered entity; and
(C) the internal policies of the covered entity for the use of the personal information described in subparagraph (B);
(2)
(A) to notify an individual if the covered entity determines that—
(i) an unauthorized disclosure of the personal information of the individual has occurred; and
(ii) harm is reasonably likely to occur; and

(B) as part of the notification under subparagraph (A), to offer the individual—

(i) the option to prohibit the covered entity from collecting, using, retaining, sharing, or selling the personal information of the individual; and

(ii) the option to have the covered entity—

(I) erase all personal information of the individual held by the covered entity;

(II) cease sharing and selling the personal information of the individual;

(III) provide the individual a copy of the personal information of the individual that the covered entity holds about the individual in a format consistent with section 6(a)(3); or

(IV) close the individual's account or otherwise terminate the individual's relationship with the covered entity;

(3) not less frequently than once every 2 years—

(A) to audit the privacy and security practices in place that protect the confidentiality, integrity, and availability of personal information held by the covered entity; or

(B) if the Commission determines appropriate based on the volume and nature of the personal information collected by the covered entity, to—

(i) have an independent third party auditor conduct the audit described in subparagraph (A); and

(ii) make the results of the audit available to the Commission upon completion.

SEC. 14. PRIVACY AND SECURITY OFFICER.

In promulgating regulations under section 3, the Commission shall require a covered entity to—

(1) designate not less than 1 employee of the covered entity to coordinate the efforts to comply with and carry out the responsibilities of the covered entity under this Act, including any request or challenge related to personal information; and

(2) provide publicly accessible contact information for each employee designated under paragraph (1).

SEC. 15. FEDERAL ENFORCEMENT.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—Except as provided in subsection (b), a violation of this Act or a regulation promulgated under this

Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (b), the Commission shall enforce this Act and any regulations promulgated under 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.

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

(b) ENTITIES NOT REGULATED BY THE COMMISSION.—Compliance with this Act and the regulations promulgated under this Act shall be enforced as follows:

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

(2) Under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board, with respect to any Federal credit union.

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

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

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

(c) RELATION TO PRIVATE AGREEMENTS.—It shall be unlawful for any covered entity to commit an act prohibited under this Act or a regulation promulgated under this Act, regardless of any specific agreement between entities or individuals.

(d) NO WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided under this Act may not be waived or limited by contract or otherwise.

SEC. 16. STATE ENFORCEMENT.

(a) IN GENERAL.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any covered entity in a practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State 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 to—

(1) enjoin that practice;

(2) enforce compliance with this Act or the regulation;

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

(4) obtain any other relief that the court considers appropriate.

(b) NOTICE.—

(1) IN GENERAL.—Before filing an action under subsection (a), the attorney general of the State involved shall provide to the Commission—

(A) written notice of the action; and

(B) a copy of the complaint for the action.

(2) EXEMPTION.—

(A) IN GENERAL.—Paragraph (1) shall not apply with respect to the filing of an action by an attorney general of a State if the attorney general determines that it is not feasible to provide the notice described in that paragraph before the filing of the action.

(B) NOTIFICATION.—In an action described in subparagraph (A), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(c) INTERVENTION.—

(1) IN GENERAL.—Upon receiving notice under subsection (b), the Commission shall have the right to intervene in the action that is the subject of the notice.

(2) EFFECT.—If the Commission intervenes in an action under paragraph (1), the Commission shall have the right—

(A) to be heard with respect to any matter that arises in the action; and

(B) to file a petition for appeal.

(d) RULE OF CONSTRUCTION.—For purposes of bringing a civil action under subsection (a), nothing in this Act shall be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to—

(1) conduct investigations;
(2) administer oaths or affirmations; or
(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) PREEMPTIVE ACTION BY COMMISSION.—If the Commission institutes an action with respect to a violation of this Act or a regulation promulgated under this Act, a State may not, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in the action instituted by the Commission based on the same set of facts giving rise to the violation with respect to which the Commission instituted the action.

SEC. 17. PRIVATE RIGHT OF ACTION.

(a) RIGHT OF ACTION.—
(1) IN GENERAL.—Any individual alleging a violation of this Act or a regulation promulgated under this Act may bring a civil action in any court of competent jurisdiction.

(2) INJURY IN FACT.—A violation of this Act or a regulation promulgated under this Act with respect to the personal information of an individual constitutes an injury in fact to that individual.

(b) RELIEF.—In a civil action brought under sub-section (a) in which the plaintiff prevails, the court may award—
(1) actual damages;
(2) punitive damages;
(3) reasonable attorney's fees and costs; and
(4) any other relief, including an injunction, that the court determines appropriate.

(c) PRE-DISPUTE ARBITRATION AGREEMENTS.—
(1) IN GENERAL.—Notwithstanding any other provision of law, no pre-dispute arbitration agreement shall be valid or enforceable with respect to a dispute between a covered entity and an individual that relates to a violation of this Act or a regulation promulgated under this Act.
(2) APPLICABILITY.—An issue as to whether this subsection applies with respect to a dispute shall be determined by a court. The validity and enforceability of an agreement to which this subsection applies shall be determined by a court, rather than an arbitrator, irrespective of whether the agreement purports to delegate such determinations to an arbitrator.

SEC. 18. RELATION TO OTHER LAWS.

(a) IN GENERAL.—Except as provided in subsection (b), nothing in this Act shall be construed to—

(1) modify, limit, or supersede the operation of any privacy or security provision in—

(A) section 552a of title 5, United States Code (commonly known as the ''Privacy Act of 1974'');

(B) the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.);

(C) the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(D) the Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq.);

(E) the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.);

(F) title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(G) chapters 119, 123, and 206 of title 18, United States Code;

(H) 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'');

(I) section 445 of the General Education Provisions Act (20 U.S.C. 1232h);

(J) the Privacy Protection Act of 1980 (42 U.S.C. 2000aa et seq.);

(K) 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 those regulations relate to—

(i) a person described in section 1172(a) of the Social Security Act (42 U.S.C. 1320d–1(a)); or

(ii) transactions referred to in section 1173(a)(1) of the Social Security Act (42 U.S.C. 1320d–2(a)(1));

(L) the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.);

(M) sections 222 and 227 of the Communications Act of 1934 (47 U.S.C. 222, 227); or

(N) any other privacy or security provision of Federal law;

(2) limit the authority of the Commission under any other provision of law; or

(3) limit the authority of the Federal Communications Commission to promulgate regulations and enforce any privacy law not in contradiction with this Act.

(b) APPLICABILITY TO MINORS.—To the extent that a provision of this Act or a regulation promulgated under this Act is inconsistent with a provision of any other Federal law relating to the protection and control of the personal information of minors, the provision that provides the most protection and control to minors and their parents or guardians shall apply.

SEC. 19. EFFECTIVE DATE.

This Act shall take effect on the date that is 90 days after the date of enactment of this Act.