119TH CONGRESS
2D SESSION

S. _____

To establish the Data Protection Agency, protect the privacy of individuals, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mrs. GILLIBRAND introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish the Data Protection Agency, protect the privacy of individuals, 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 ''Data Protection Act of 2026''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—DATA PROTECTION AUTHORITY

Sec. 101. Establishment; purpose, objectives, and functions.
Sec. 102. Administration.

Sec. 103. Implementation and enforcement.
Sec. 104. Relation to other laws and agencies.
Sec. 105. Funding.

TITLE II—PRIVACY PROTECTIONS

Sec. 201. Prohibited acts.
Sec. 202. Supervision of data aggregators.

TITLE III—MISCELLANEOUS

Sec. 301. Initial regulations.
Sec. 302. Severability.
Sec. 303. Relation to Federal and State law.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''Agency'' means the Data Protection Agency established under section 101.

(2) AGENCY INVESTIGATION.—The term ''Agency investigation'' means any inquiry conducted by an Agency investigator for the purpose of ascertaining whether any person is or has been engaged in any conduct that is a violation, as defined in section 103(b)(1).

(3) AGENCY INVESTIGATOR.—The term ''Agency investigator'' means any attorney or investigator employed by the Agency who is charged with the duty of enforcing or carrying into effect this Act or any other Federal privacy law.

(4) ANONYMIZED DATA.—The term ''anonymized data'' means information—

(A) that does not identify an individual; and

(B) with respect to which there is no reasonable basis to believe that the information can be used on its own or in combination with other reasonably available information to identify an individual.

(5) AUTOMATED DECISION SYSTEM.—The term ''automated decision system'' means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that automates, analyzes, aids, or augments decisions.

(6) BIOMETRIC INFORMATION.—The term ''biometric information''—

(A) means information regarding the physiological or biological characteristics of an individual that may be used, singly or in combination with each other or with other identifying data, to establish the identity of an individual;

(B) includes—

(i) genetic information;

(ii) imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier

template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted;

(iii) keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information; and

(iv) any mathematical code, profile, or algorithmic model derived from information regarding the physiological or biological characteristics of an individual;

(C) does not include information captured from a patient in a health care setting for a medical purpose or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191); and

(D) does not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

(7) COLLECT.—The term ''collect''—

(A) means buying, renting, gathering, obtaining, receiving, or accessing any personal data by any means; and

(B) includes—

(i) receiving personal data from an individual or device; and

(ii) creating, deriving, or inferring personal data by analyzing data about an individual or about groups of individuals similar to the individual.

(8) CUSTODIAN.—The term ''custodian'' means the custodian or any deputy custodian designated by the Agency.

(9) DATA AGGREGATOR.—The term ''data aggregator''—

(A) means any person that collects, uses, or shares, in or affecting interstate commerce, an amount of personal data that is not de minimis, as well as entities related to that person by common ownership or corporate control; and

(B) does not include an individual who collects, uses, or shares personal data solely for non-commercial reasons.

(10) DEVICE.—The term ''device'' means any physical object that—

(A) is capable of connecting to the internet or other communication network; or

(B) has computer processing capabilities that can collect, send, receive, or store data.

(11) DIRECTOR.—The term ''Director'' means the Director of the Data Protection Agency.

(12) DOCUMENTARY MATERIAL.—The term ''documentary material'' includes the original or any copy of any book, document, record, report, memorandum, paper, communication, tabulation, chart, logs, electronic files, or other data or data compilations stored in any medium.

(13) ELECTRONIC DATA.—The term ''electronic data'' means any information that is in an electronic or digital format or any electronic or digital reference that contains information about an individual or device.

(14) FEDERAL PRIVACY LAW.—The term ''Federal privacy law'' means the provisions of this Act, any other rule or order prescribed by the Agency under this Act, and the following laws (including any amendments made to such laws and regulations promulgated under such laws):

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

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

(C) The Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. 6101 et seq.).

(D) The Fair and Accurate Credit Transactions Act of 2003 (Public Law 108–159; 117 Stat. 1952).

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

(F) Sections 222, 227, 338(l), 631, and 705 of the Communications Act of 1934 (47 U.S.C. 222, 227, 338(l), 551, 705).

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

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

(I) The Identity Theft Assumption and Deterrence Act of 1998 (Public Law 105–318; 117 Stat. 3007).

(J) Sections 444 and 445 of the General Education Provisions Act (20 U.S.C. 1232g, 1232h).

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

(L) The E-Government Act of 2002 (Public Law 107–347; 116 Stat. 2899).

(M) The Computer Security Act of 1987 (40 U.S.C. 1441 note).

(N) The Employee Polygraph Protection Act of 1988 (29 U.S.C. 2001 et seq.).

(O) The Communications Assistance for Law Enforcement Act (Public Law 103–414; 108 Stat. 4279).

(P) Sections 1028A, 1030, and 1801 and chapter 119, of title 18, United States Code.

(Q) The Genetic Information Nondiscrimination Act of 2008 (Public Law 110–233; 122 Stat. 881).

(R) The Taxpayer Browsing Protection Act (Public Law 105–35; 111 Stat. 1104).

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

(T) The Cable Communications Policy Act of 1984 (Public Law 98–549; 98 Stat. 2779).

(U) The Do-Not-Call Implementation Act (Public Law 108–10; 117 Stat. 557).

(V) The Wireless Communications and Public Safety Act of 1999 (Public Law 106–81; 113 Stat. 1286).

(W) Title XXX of the Public Health Service Act (42 U.S.C. 300jj et seq.).

(X) 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 a person described in section 1172(a) of the Social Security Act (42 U.S.C. 1320d–1(a)) and transactions referred to in section 1173(a)(1) of the Social Security Act (42 U.S.C. 1320d–2(a)(1)).

(Y) Chapter 123 of title 18, United States Code.

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

(AA) Chapters 61, 68, 75, and 76 of the Internal Revenue Code of 1986.

(BB) Section 1106 of the Social Security Act (42 U.S.C. 1306).

(CC) Chapter 121 of title 18, United States Code.

(DD) Subpart A of part 46 of title 45, Code of Federal Regulations (commonly known as the ''Common Rule'').

(15) GENETIC INFORMATION.—The term ''genetic information'' has the meaning given the term in section 201 of the Genetic Information Nondiscrimination Act of 2008 (42 U.S.C. 2000ff).

(16) HIGH-RISK DATA PRACTICE.—The term ''high-risk data practice'' means an action by a data aggregator that involves—

(A) the use of an automated decision system;

(B) the processing of data in a manner that involves an individual's protected class, familial status, lawful source of income, financial status such as the individual's income or assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, or any other factor used as a proxy for identifying any of these characteristics;

(C) a systematic processing of publicly accessible data on a large scale;

(D) processing involving the use of new technologies, or combinations of technologies,

that causes or materially contributes to privacy harm;

(E) decisions about an individual's access to a product, service, opportunity, or benefit which is based to any extent on automated decision system processing;

(F) any profiling of individuals on a large scale;

(G) any processing of biometric information for the purpose of uniquely identifying an individual, with the exception of one-to-one biometric authentication;

(H) combining, comparing, or matching personal data obtained from multiple sources;

(I) processing which involves an individual's precise geolocation;

(J) the processing of personal data of children and teens under 17 or other vulnerable individuals such as the elderly, people with disabilities, and other groups known to be susceptible for exploitation for marketing purposes, profiling, or automated processing;

(K) consumer scoring or other business practices that pertain to the eligibility of an individual, and related terms, rights, benefits, and

privileges, for employment (including hiring, firing, promotion, demotion, and compensation), credit, insurance, housing, education, professional certification, or the provision of health care and related services; or

(L) any other practice that has comparable legal, material, or similarly significant effect or harm on an individual's life, as determined by the Agency through rules promulgated pursuant to this Act.

(17) HIGH-RISK DATA PRACTICE IMPACT EVALUATION.—The term ''high-risk data practice impact evaluation'' means a study conducted after deployment of a high-risk data practice that includes, at a minimum—

(A) an evaluation of a high-risk data practice's accuracy, disparate impacts on the basis of protected class, and privacy harms;

(B) an evaluation of the effectiveness of measures taken to minimize risks as outlined in any prior high-risk data practice risk assessments; and

(C) recommended measures to further minimize risks to accuracy, disparate impacts on the basis of protected class, and privacy harms.

(18) HIGH-RISK DATA PRACTICE RISK ASSESSMENT.—The term ''high-risk data practice risk assessment'' means a study evaluating a high-risk data practice and the high-risk data practice's development process, including the design and training data of the high-risk data practice, if applicable, for likelihood and severity of risks to accuracy, bias, discrimination, and privacy harms that includes, at a minimum—

(A) a detailed description of the high-risk data practice, including—

(i) its design and methodologies;

(ii) any applicable training data characteristics;

(iii) a data description of the categories of personal data collected or processed in connection with the high-risk data practice, the sources of such categories of person data, and the purpose; and

(iv) the purpose, including what context the practice will be deployed and how individuals will interact with the system and what categories of data the data aggregator will create, infer, or generate

about consumers as a result of the high-risk data practice;

(B) an assessment of the relative benefits and costs of the high-risk data practice in light of its purpose, potential unintended consequences, and taking into account relevant factors, including—

(i) data minimization practices;

(ii) the duration and methods for which personal data and the results of the high-risk data practice are stored;

(iii) what information about the high-risk data practice is available to individuals;

(iv) the extent to which individuals have access to the results of the high-risk data practice and may correct or object to its results; and

(v) the recipients of the results of the high-risk data practice;

(C) an assessment of the risks of privacy harm posed by the high-risk data practice and the risks that the high-risk data practice may result in or contribute to inaccurate, biased, or

discriminatory decisions impacting individuals or groups of individuals;

(D) the decision to accept, reject, or mitigate and minimize risks and the measures a data aggregator will employ including to minimize the risks described in subparagraph (C), including technological and physical safeguards;

(E) an assessment of the environmental footprint on the development and use system in terms of carbon emissions and water use; and

(F) any potential or permitted use of the outputs of the high-risk data for other decisions or purposes such as advertising targeting.

(19) INDIVIDUAL.—The term ''individual'' means a natural person.

(20) PERSON.—The term ''person'' means an individual, a local, State, or Federal governmental entity, a partnership, a company, a corporation, an association (incorporated or unincorporated), a trust, an estate, a cooperative organization, another entity, or any other organization or group of such entities acting in concert.

(21) PERSONAL DATA.—The term ''personal data'' means electronic data that, alone or in combination with other data—

(A) identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, household, or device; or

(B) could be used to determine that an individual or household is part of a protected class.

(22) PRECISE GEOLOCATION.—The term ''precise geolocation'' means any data that is derived from a device and that is used or intended to be used to locate an individual within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.

(23) PRIVACY HARM.—The term ''privacy harm'' means an adverse consequence, or a potential adverse consequence, to an individual, a group of individuals, or society caused, in whole or in part, by the collection, processing, or sharing of personal data, including—

(A) direct or indirect financial loss or economic harm, including financial loss or economic harm arising from fraudulent activities or data security breaches;

(B) physical harm, harassment, or a threat to an individual or property;

(C) psychological harm, including anxiety, embarrassment, fear, other trauma, stigmatization, reputational harm, or the revealing or exposing of an individual, or a characteristic of an individual, in an unexpected way;

(D) an adverse outcome or decision, including relating to the eligibility of an individual for the rights, benefits, or privileges in credit and insurance (including the denial of an application or obtaining less favorable terms), housing, education, professional certification, employment (including hiring, firing, promotion, demotion, and compensation), or the provision of health care and related services;

(E) discrimination, including both differential treatment on the basis of a protected class and disparate impact on a protected class;

(F) the chilling of free expression or action of an individual, or society generally, due to perceived or actual pervasive and excessive collection, processing, or sharing of personal data;

(G) the use of information technology to covertly influence an individual's decision-making, by targeting and exploiting decision-making vulnerabilities; and

(H) any other adverse consequence, or potential adverse consequence, prohibited by or defined by Federal privacy laws; provisions of Federal civil rights laws related to the processing of personal information; provisions of Federal consumer protection laws related to the processing of personal information; the First Amendment; and other constitutional rights protecting privacy.

(24) PROCESS.—The term ''process'' means to perform an operation or set of operations on personal data, either manually or by automated means, including collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, sorting, classifying, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

(25) PROFILE.—The term ''profile'' means the use of an automated decision system to process data (including personal data and other data) to derive, infer, predict or evaluate information about an individual or group, such as the processing of data to analyze or predict an individual's identity, attributes, interests or behavior.

(26) PROTECTED CLASS.—The term ''protected class'' means the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity or expression, sexual orientation, familial status, biometric information, genetic information, or disability of an individual or a group of individuals.

(27) SERVICE PROVIDER.—The term ''service provider'' means a data aggregator that collects, uses, or shares personal data only on behalf of another data aggregator in order to carry out a permissible purpose, and only to the extent of such activity.

(28) SHARE.—The term ''share'' means disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, personal data.

TITLE I—DATA PROTECTION AUTHORITY

SEC. 101. ESTABLISHMENT; PURPOSE, OBJECTIVES, AND FUNCTIONS.

(a) ESTABLISHMENT.—There is established in the Executive branch an independent agency to be known as the ''Data Protection Agency'', which shall implement and enforce this Act, including by regulating high-risk data

practices and the collection, processing, and sharing of personal data.

(b) PURPOSE, OBJECTIVES, AND FUNCTIONS.—

(1) PURPOSE.—The Agency shall seek to—

(A) protect individuals' privacy;

(B) prevent and remediate privacy harms;

(C) prevent, remediate, and reduce discrimination on the basis of protected class through the processing of personal information, including both differential treatment on the basis of a protected class and disparate impact on a protected class; and

(D) limit the collection, processing, and sharing of personal data; and is authorized to exercise its authorities under this Act for such purposes.

(2) OBJECTIVES.—The Agency is authorized to exercise its authorities under this Act to—

(A) protect individuals from violations of this Act, other Federal privacy laws, or rules and orders issued under this Act or other Federal privacy laws;

(B) promote and affirmatively further equal opportunity in all aspects of economic life

as it relates to the fair and non-discriminatory processing of personal information;

(C) oversee the use of high-risk data practices;

(D) promote the minimization of collection of personal data for commercial purposes;

(E) prevent and remediate privacy harms; and

(F) ensure that Federal privacy law is enforced consistently and in order to protect individuals' privacy.

(3) FUNCTIONS.—The primary functions of the Agency are—

(A) providing leadership and coordination to the efforts of all Federal departments and agencies to enforce all Federal statutes, Executive orders, regulations and policies which involve privacy or data protection;

(B) maximizing effort, promoting efficiency, and eliminating conflict, competition, duplication, and inconsistency among the operations, functions, and jurisdictions of Federal departments and agencies responsible for privacy or data protection, and data protection rights and standards;

(C) providing active leadership, guidance, education, and appropriate assistance to private sector businesses, organizations, groups, institutions, and individuals regarding privacy and data protection rights and standards;

(D) requiring and overseeing ex-ante high-risk data practice risk assessments and ex-post high-risk data practice impact evaluations to advance fair and just data practices, including making the assessments available to the public as practical under the law;

(E) protecting individuals and groups of individuals from privacy harms;

(F) examining the social, ethical, economic, and civil rights impacts of data collection and processing practices and proposing remedies;

(G) protecting civil rights, combating unlawful discrimination, and affirmatively furthering equal opportunity as they relate to the processing of personal information;

(H) ensuring that high-risk data privacy practices are fair, just, non-deceptive, and do not discriminate against a protected class;

(I) collecting, researching, and responding to complaints;

(J) developing model privacy and data protection standards, guidelines, and policies for use by the private sector; and

(K) enforcing other privacy statutes and rules as authorized by Congress.

SEC. 102. ADMINISTRATION.

(a) EXECUTIVE AND ADMINISTRATIVE POWERS.—

(1) POWERS OF THE AGENCY.—The Director is authorized to establish the general powers of the Agency with respect to all executive and administrative functions, including—

(A) the establishment of rules for conducting the general business of the Agency, in a manner not inconsistent with this Act;

(B) to bind the Agency and enter into contracts;

(C) directing the establishment and maintenance of divisions or other offices within the Agency, in order to carry out the responsibilities under this Act and Federal privacy law, and to satisfy the requirements of applicable law;

(D) to coordinate and oversee the operation of all administrative, enforcement, and research activities of the Agency;

(E) to adopt and use a seal;

(F) to determine the character of and necessity for the obligations by the Agency;

(G) the appointment and supervision of personnel employed by the Agency;

(H) the distribution of business among personnel appointed and supervised by the Agency;

(I) the use and expenditure of funds;

(J) implementing this Act and Federal privacy laws through rules, orders, guidance, interpretations, statements of policy, examinations, and enforcement actions; and

(K) performing such other functions as may be authorized or required by law.

(2) DELEGATION OF AUTHORITY.—The Director may delegate to any duly authorized employee, representative, or agent any power vested in the Agency by law.

(3) OFFICE RESPONSIBILITIES.—Notwithstanding paragraphs (1) and (2), section 101(a), and any other provision of law, with respect to the specific functional units and offices described in subsection (b)(2), the Director—

(A) shall ensure that such functional units and offices perform the functions, duties, and coordination assigned to them under the applicable provision of subsection (b); and

(B) may not reorganize or rename such units or offices in a manner not provided for under the applicable provisions of subsection (b).

(b) ADMINISTRATION.—

(1) PERSONNEL.—

(A) DIRECTOR AND DEPUTY DIRECTOR.—

(i) IN GENERAL.—There is established a position of the Director of the Data Protection Agency (referred to in this Act as the ''Director''), who shall serve as the head of the Agency.

(ii) APPOINTMENT.—Subject to subparagraph (C), the Director shall be appointed by the President, by and with the advice and consent of the Senate.

(iii) QUALIFICATION.—The President shall nominate the Director from among members of the public at large who are well qualified for service at the Agency

based on their knowledge and expertise in—

(I) technology;

(II) privacy and protection of personal data;

(III) civil rights and liberties;

(IV) law; and

(V) social sciences.

(iv) COMPENSATION.—

(I) IN GENERAL.—The Director shall be compensated at the rate prescribed for level II of the Executive Schedule under section 5313 of title 5, United States Code.

(II) CONFORMING AMENDMENT.—Section 5313 of title 5, United States Code, is amended by inserting after the item relating to the Federal Transit Administrator, the following new item: ''Director of the Data Protection Agency.''.

(v) DEPUTY DIRECTOR.—There is established the position of Deputy Director, who shall—

(I) be appointed by the Director; and

(II) serve as the acting Director in the absence or unavailability of the Director.

(vi) ACTING DIRECTOR.—In the event of the death, resignation, sickness, or absence of the Director, the President shall designate the Deputy Director to serve as acting Director until the return of the Director, or the appointment of a successor pursuant to paragraph (2).

(B) TERM.—

(i) IN GENERAL.—The Director shall serve for a term of 5 years.

(ii) EXPIRATION OF TERM.—An individual may serve as Director after the expiration of the term for which appointed until a successor has been appointed and qualified.

(iii) REMOVAL.—The President may remove the Director at will.

(iv) VACANCY.—A vacancy in the position of Director that occurs before the expiration of the term for which a Director

was appointed shall be filled in the manner established under subparagraph (B), and the Director appointed to fill such vacancy shall be appointed only for the remainder of such term.

(C) SERVICE RESTRICTION.—No Director or Deputy Director may engage in any other employment during the period of service of such person as Director or Deputy Director.

(D) APPOINTMENT.—

(i) IN GENERAL.—The Director may fix the number of, and appoint and direct, all employees of the Agency, in accordance with the applicable provisions of title 5, United States Code.

(ii) EMPLOYEES OF THE AGENCY.—The Director may employ attorneys, compliance examiners, compliance supervision analysts, economists, technologists, data scientists, designers, ethicists, privacy experts, statisticians, and other employees as may be deemed necessary to conduct the business of the Agency. Unless otherwise provided expressly by law, any individual appointed under this section shall be an

employee, as defined in section 2105 of title 5, United States Code, and subject to the provisions of such title and other laws generally applicable to the employees of an Executive agency.

(iii) WAIVER AUTHORITY.—

(I) IN GENERAL.—In making any appointment under subparagraph (A), the Director may waive the requirements of chapter 33 of title 5, United States Code, and the regulations implementing such chapter, to the extent necessary to appoint employees on terms and conditions that are consistent with those set forth in section 11(1) of the Federal Reserve Act (12 U.S.C. 248(1)), while providing for—

(aa) fair, credible, and transparent methods of establishing qualification requirements for, recruitment for, and appointments to positions;

(bb) fair and open competition and equitable treatment in

the consideration and selection of individuals to positions; and

(cc) fair, credible, and transparent methods of assigning, reassigning, detailing, transferring, and promoting employees.

(II) VETERANS PREFERENCES.—In implementing this subparagraph, the Director shall comply with the provisions of section 2302(b)(11) of title 5, United States Code, regarding veterans' preference requirements, in a manner consistent with that in which such provisions are applied under chapter 33 of that title. The authority under this subparagraph to waive the requirements of that chapter 33 shall expire 5 years after the date of enactment of this Act.

(iv) DUTY TO PROVIDE ADEQUATE STAFFING.—The Director shall ensure that the specific functional units and offices established under paragraph (2), as well as other units and offices with supervisory, rulemaking, and enforcement duties, are

provided with sufficient staff to carry out the functions, duties, and coordination of those units and offices.

(v) LIMITATION ON POLITICAL APPOINTEES.—

(I) IN GENERAL.—In appointing employees of the Agency who are political appointees, the Director shall ensure that the number and duties of such political appointees are as similar as possible to those of other Federal regulatory agencies.

(II) POLITICAL APPOINTEES DEFINED.—For purposes of this subparagraph, the term ''political appointee'' means an employee who holds—

(aa) a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policymaking, or policy-advocating character;

(bb) a position in the Senior Executive Service as a noncareer

appointee (as such term is defined in section 3132(a) of title 5, United States Code); or

(cc) a position under the Executive Schedule (subchapter II of chapter 53 of title 5, United States Code).

(E) COMPENSATION.—Notwithstanding any otherwise applicable provision of title 5, United States Code, concerning compensation, including the provisions of chapter 51 and chapter 53, the following provisions shall apply with respect to employees of the Agency:

(i) The rates of basic pay for all employees of the Agency may be set and adjusted by the Director.

(ii) The Director shall at all times provide compensation (including benefits) to each class of employees that, at a minimum, are comparable to the compensation and benefits then being provided by the Board of Governors of the Federal Reserve System or the Bureau of Consumer Financial Protection for the corresponding class of employees.

(iii) All such employees shall be compensated (including benefits) on terms and conditions that are consistent with the terms and conditions set forth in section 11(l) of the Federal Reserve Act (12 U.S.C. 248(l)).

(F) LABOR-MANAGEMENT RELATIONS.—Chapter 71 of title 5, United States Code, shall apply to the Agency and the employees of the Agency.

(G) APPLICABILITY OF OTHER LAWS.—Except as otherwise provided expressly by law, all Federal laws dealing with public or Federal contracts, property, works, officers, employees, budgets, or funds, including the provisions of chapter 5 and 7 of title 5, United States Codes, shall apply to the exercise of the powers of the Agency.

(2) SPECIFIC FUNCTIONAL UNITS.—

(A) OFFICE OF CIVIL RIGHTS.—The Director shall establish an office whose powers and duties shall include—

(i) providing oversight and enforcement of this Act, rules and orders promulgated under this Act, and Federal privacy

laws to ensure that the collection, processing, and sharing of personal data is fair, equitable, and non-discriminatory in treatment and effect;

(ii) developing, establishing, and promoting data processing practices that affirmatively further equal opportunity to and expand access to housing, employment, credit, insurance, education, healthcare, and other aspects of interstate commerce;

(iii) coordinating the Agency's civil rights efforts with other Federal agencies and State regulators, as appropriate, to promote consistent, efficient, and effective enforcement of Federal civil rights laws;

(iv) working with civil rights advocates, privacy organizations, and data aggregators on the promotion of compliance with the civil rights provisions under this Act, rules and orders promulgated under this Act, and Federal privacy laws;

(v) liaising with communities and consumers impacted by practices regulated by this Act and the Agency, to ensure that

their needs and views are appropriately taken into account;

(vi) providing annual reports to Congress on the efforts of the Agency to fulfill its civil rights mandate; and

(vii) such additional powers and duties as the Director may determine are appropriate.

(B) RESEARCH.—The Director shall establish a unit whose functions shall include researching, analyzing, assessing, and reporting on—

(i) the collection and processing of personal data, including automated decision systems;

(ii) the collection and processing of personal data by government agencies, including contracts between government agencies and data aggregators; and

(iii) unfair, deceptive, or discriminatory outcomes that result or are likely to result from the use of automated decision systems, including disparate treatment or disparate impact on the basis of protected class or proxies for protected class.

(C) COLLECTING AND TRACKING COMPLAINTS.—

(i) IN GENERAL.—

(I) ESTABLISHMENT OF UNIT.—The Director shall establish a unit, the functions of which shall include identifying and facilitating the development of best practices for consumers to file a complaint, and establishing a single toll-free telephone number, a publicly available website, and a publicly available database, or utilizing an existing publicly available database, to facilitate the centralized collection of, monitoring of, and response to complaints regarding the collection, processing, and sharing of personal data.

(II) WEBSITE REQUIREMENTS.—The Director shall ensure that—

(aa) the landing page of the main website of the Agency contains a clear and conspicuous hyperlink to the complaint database described in clause (i) and

shall ensure that such database is user-friendly and in plain writing, as that term is defined in section 3 of the Plain Writing Act of 2010 (5 U.S.C. 301 note); and

(bb) that all information on the website or the database that explains how a complaint with the Agency, as well as reports of the Agency with respect to information contained in that database, shall be provided in each of the 5 most commonly spoken languages, other than English, in the United States, as determined by the Bureau of the Census on an ongoing basis, and in formats accessible to individuals with hearing or vision impairments.

(ii) PUBLIC AVAILABILITY OF INFORMATION.—

(I) IN GENERAL.—The Director shall—

(aa) make all complaints available to the public on a website of the Agency;

(bb) place a clear and conspicuous hyperlink on the landing page of the main website of the Agency to the website described under subclause (I); and

(cc) ensure that such website—

(AA) is searchable and sortable by an data aggregator; and

(BB) is user-friendly and written in plain language.

(II) REMOVAL OF PERSONAL DATA.—In making the information described under clause (i) available to the public, the Director shall remove all personal data.

(3) AGENCY OMBUDSMAN.—

(A) ESTABLISHMENT REQUIRED.—The Director shall appoint an ombudsman.

(B) DUTIES OF OMBUDSMAN.—The ombudsman appointed in accordance with paragraph (1) shall—

(i) act as a liaison between the Agency and any affected person with respect to any problem that such person may have in dealing with the Agency, resulting from the regulatory activities of the Agency; and

(ii) assure that safeguards exist to encourage complainants to come forward and preserve confidentiality.

(4) AUTONOMY OF AGENCY.—No officer or agency of the United States shall have any authority to require the Director or any other officer of the Agency to submit legislative recommendations, or testimony or comments on legislation, to any officer or agency of the United States for approval, comments, or review prior to the submission of such recommendations, testimony, or comments to the Congress, if such recommendations, testimony, or comments to the Congress include a statement indicating that the views expressed therein are those of the Director or such officer, and do not necessarily reflect the views of the President.

(c) APPEARANCES BEFORE AND REPORTS TO CONGRESS.—

(1) APPEARANCES BEFORE CONGRESS.—The Director of the Agency shall appear before Congress at semi-annual hearings regarding the reports required under subsection (b).

(2) REPORTS REQUIRED.—The Agency shall, concurrent with each semi-annual hearing referred to in subsection (a), prepare and submit to the President and Congress, a report, beginning with the session following the designated transfer date, and shall publish such report on the website of the Agency.

(3) CONTENTS.—The reports required by subsection (b) shall include—

(A) a discussion of the significant problems faced by persons in exercising their rights under this Act and Federal privacy laws;

(B) a justification of the budget request of the previous year;

(C) a list of the significant rules and orders adopted by the Agency, as well as other significant initiatives conducted by the Agency, during the preceding year and the plan of the

Agency for rules, orders, or other initiatives to be undertaken during the upcoming period;

(D) an analysis of complaints about practices relating to the collection, processing, or sharing of personal data that the Agency has received and collected in its central database on complaints during the preceding year;

(E) a list, with a brief statement of the issues, of the public supervisory and enforcement actions to which the Agency was a party during the preceding year;

(F) the actions taken regarding rules, orders, and supervisory actions with respect to data aggregators;

(G) an assessment of significant actions by State attorneys general or State regulators relating to this Act or other Federal privacy laws;

(H) an analysis of the efforts of the Agency to fulfill the civil rights mandate of the Agency; and

(I) an analysis of the efforts of the Agency to increase workforce and contracting diversity.

(d) INSPECTOR GENERAL.—Section 401 of title 5, United States Code, is amended—

(1) in paragraph (1), by inserting ''the Data Protection Agency,'' after ''Export-Import Bank of the United States,''; and

(2) in paragraph (3), by inserting ''the Director of the Data Protection Agency;'' after ''Export-Import Bank of the United States;''.

(e) OFFICES.—The principal office of the Agency shall be in the District of Columbia. The Director may establish regional offices of the Agency.

SEC. 103. IMPLEMENTATION AND ENFORCEMENT.

(a) RULEMAKING AUTHORITY.—

(1) IN GENERAL.—The Agency is authorized to exercise its authorities under this Act to administer, enforce, and otherwise implement the provisions of this Act and Federal privacy law.

(2) RULEMAKING, ORDERS, AND GUIDANCE.—

(A) GENERAL AUTHORITY.—The Director may prescribe rules and issue orders and guidance, as may be necessary or appropriate to enable the Agency to administer and carry out the purposes and objectives of this Act and other Federal privacy laws, and to prevent evasions of this Act and other Federal privacy laws.

(B) NO LIMITATION.—Rules prescribed under this section shall not limit the authority

of the Agency to administer, enforce, and otherwise implement the provisions of this Act and Federal privacy law.

(C) STANDARDS FOR RULEMAKING.—In prescribing a rule under this Act or Federal privacy laws—

(i) the Agency shall consider the impact of proposed rules on an individual or groups of individuals;

(ii) the Agency may provide that a rule shall only apply to a subcategory of data aggregators, as defined by the Agency; and

(iii) the Agency shall consult with civil society groups and members of the public.

(D) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to require the Agency to engage in cost-benefit analysis or submit a rulemaking for review to the President or the Office of Management and Budget.

(E) STANDARD FOR REVIEW.—If this Act is silent or ambiguous, and the Agency has followed the procedures in section 553 or 554 of title 5, United States Code, as applicable, a reviewing court shall defer to the Agency's rea-

sonable or permissible interpretation of this Act.

(3) MONITORING.—In order to support its rulemaking and other functions, the Agency shall monitor for risks to individuals or groups of individuals in the collection, processing, or sharing of personal data.

(b) ENFORCEMENT POWERS.—

(1) DEFINITIONS.—In this section, the term ''violation'' means any act or omission that, if proved, would constitute a violation of any provision of this Act or any other Federal privacy law.

(2) INVESTIGATIONS AND ADMINISTRATIVE DISCOVERY.—

(A) JOINT INVESTIGATIONS.—

(i) IN GENERAL.—The Agency or, where appropriate, an Agency investigator, may engage in joint investigations and requests for information, as authorized under this Act.

(ii) CIVIL RIGHTS.—The authority under subparagraph (A) includes matters relating to protection of individuals' civil rights under this Act and joint investigations with, and requests for information

from, the Director of the Bureau of Consumer Financial Protection, the Federal Trade Commission, the Secretary of Housing and Urban Development, the Department of Education, the Equal Employment Opportunity Commission, the Department of Health and Human Services, or the Attorney General.

(B) SUBPOENAS.—

(i) IN GENERAL.—The Agency or an Agency investigator may issue subpoenas for the attendance and testimony of witnesses and the production of relevant papers, books, documents, or other material in connection with hearings under this Act.

(ii) FAILURE TO OBEY.—In the case of contumacy or refusal to obey a subpoena issued pursuant to this subparagraph and served upon any person, the district court of the United States for any district in which such person is found, resides, or transacts business, upon application by the Agency or an Agency investigator and after notice to such person, may issue an order requiring such person to ap-

pear and give testimony or to appear and produce documents or other material.

(iii) CONTEMPT.—Any failure to obey an order of the court under this subparagraph may be punished by the court as a contempt thereof.

(C) DEMANDS.—

(i) IN GENERAL.—Whenever the Agency has reason to believe that any person may be in possession, custody, or control of any documentary material or tangible things, or may have any information, relevant to a violation, the Agency may, before the institution of any proceedings under this Act, issue in writing, and cause to be served upon such person, a civil investigative demand requiring such person to—

(I) produce such documentary material for inspection and copying or reproduction in the form or medium requested by the Agency;

(II) submit such tangible things;

(III) file written reports or answers to questions;

(IV) give oral testimony concerning documentary material, tangible things, or other information; or

(V) furnish any combination of such material, answers, or testimony.

(ii) REQUIREMENTS.—Each civil investigative demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.

(iii) PRODUCTION OF DOCUMENTS.—Each civil investigative demand for the production of documentary material shall—

(I) describe each class of documentary material to be produced under the demand with such definiteness and certainty as to permit such material to be fairly identified;

(II) prescribe a return date or dates which will provide a reasonable period of time within which the material so demanded may be assembled

and made available for inspection and copying or reproduction; and

(III) identify the custodian to whom such material shall be made available.

(iv) PRODUCTION OF THINGS.—Each civil investigative demand for the submission of tangible things shall—

(I) describe each class of tangible things to be submitted under the demand with such definiteness and certainty as to permit such things to be fairly identified;

(II) prescribe a return date or dates which will provide a reasonable period of time within which the things so demanded may be assembled and submitted; and

(III) identify the custodian to whom such things shall be submitted.

(v) DEMAND FOR WRITTEN REPORTS OR ANSWERS.—Each civil investigative demand for written reports or answers to questions shall—

(I) propound with definiteness and certainty the reports to be produced or the questions to be answered;

(II) prescribe a date or dates at which time written reports or answers to questions shall be submitted; and

(III) identify the custodian to whom such reports or answers shall be submitted.

(vi) ORAL TESTIMONY.—Each civil investigative demand for the giving of oral testimony shall—

(I) prescribe a date, time, and place at which oral testimony shall be commenced; and

(II) identify an Agency investigator who shall conduct the investigation and the custodian to whom the transcript of such investigation shall be submitted.

(vii) SERVICE.—Any civil investigative demand issued, and any enforcement petition filed, under this paragraph may be served—

(I) by any Agency investigator at any place within the territorial jurisdiction of any court of the United States; and

(II) upon any person who is not found within the territorial jurisdiction of any court of the United States—

(aa) in such manner as the Federal Rules of Civil Procedure prescribe for service in a foreign nation; and

(bb) to the extent that the courts of the United States have authority to assert jurisdiction over such person, consistent with due process, the United States District Court for the District of Columbia shall have the same jurisdiction to take any action respecting compliance with this section by such person that such district court would have if such person were personally within the jurisdiction of such district court.

(viii) METHOD OF SERVICE.—Service of any civil investigative demand or any enforcement petition filed under this paragraph may be made upon a person, including any legal entity, by—

(I) delivering a duly executed copy of such demand or petition to the individual or to any partner, executive officer, managing agent, or general agent of such person, or to any agent of such person authorized by appointment or by law to receive service of process on behalf of such person;

(II) delivering a duly executed copy of such demand or petition to the principal office or place of business of the person to be served; or

(III) depositing a duly executed copy in the United States mails, by registered or certified mail, return receipt requested, duly addressed to such person at the principal office or place of business of such person.

(ix) PROOF OF SERVICE.—

(I) IN GENERAL.—A verified return by the individual serving any civil investigative demand or any enforcement petition filed under this paragraph setting forth the manner of such service shall be proof of such service.

(II) RETURN RECEIPTS.—In the case of service by registered or certified mail, such return shall be accompanied by the return post office receipt of delivery of such demand or enforcement petition.

(x) PRODUCTION OF DOCUMENTARY MATERIAL.—The production of documentary material in response to a civil investigative demand shall be made under a sworn certificate, in such form as the demand designates, by the person, if a natural person, to whom the demand is directed or, if not a natural person, by any person having knowledge of the facts and circumstances relating to such production, to the effect that all of the documentary material required by the demand and in

the possession, custody, or control of the person to whom the demand is directed has been produced and made available to the custodian.

(xi) SUBMISSION OF TANGIBLE THINGS.—The submission of tangible things in response to a civil investigative demand shall be made under a sworn certificate, in such form as the demand designates, by the person to whom the demand is directed or, if not a natural person, by any person having knowledge of the facts and circumstances relating to such production, to the effect that all of the tangible things required by the demand and in the possession, custody, or control of the person to whom the demand is directed have been submitted to the custodian.

(xii) SEPARATE ANSWERS.—Each reporting requirement or question in a civil investigative demand shall be answered separately and fully in writing under oath, unless it is objected to, in which event the reasons for the objection shall be stated in

lieu of an answer, and it shall be submitted under a sworn certificate, in such form as the demand designates, by the person, if a natural person, to whom the demand is directed or, if not a natural person, by any person responsible for answering each reporting requirement or question, to the effect that all information required by the demand and in the possession, custody, control, or knowledge of the person to whom the demand is directed has been submitted.

(xiii) TESTIMONY.—

(I) IN GENERAL.—

(aa) OATH AND RECORDATION.—The examination of any person pursuant to a demand for oral testimony served under this paragraph shall be taken before an officer authorized to administer oaths and affirmations by the laws of the United States or of the place at which the examination is held. The officer before whom oral testimony is to be

taken shall put the witness on oath or affirmation and shall personally, or by any individual acting under the direction of and in the presence of the officer, record the testimony of the witness.

(bb) TRANSCRIPTION.—The testimony shall be taken stenographically and transcribed.

(cc) TRANSMISSION TO CUSTODIAN.—After the testimony is fully transcribed, the officer investigator before whom the testimony is taken shall promptly transmit a copy of the transcript of the testimony to the custodian.

(II) PARTIES PRESENT.—Any Agency investigator before whom oral testimony is to be taken shall exclude from the place where the testimony is to be taken all other persons, except the person giving the testimony, the attorney for that person, the officer before whom the testimony is to be taken, an investigator or representa-

tive of an agency with which the Agency is engaged in a joint investigation, and any stenographer taking such testimony.

(III) LOCATION.—The oral testimony of any person taken pursuant to a civil investigative demand shall be taken in the judicial district of the United States in which such person resides, is found, or transacts business, or in such other place as may be agreed upon by the Agency investigator before whom the oral testimony of such person is to be taken and such person.

(IV) ATTORNEY REPRESENTATION.—

(aa) IN GENERAL.—Any person compelled to appear under a civil investigative demand for oral testimony pursuant to this section may be accompanied, represented, and advised by an attorney.

(bb) AUTHORITY.—The attorney may advise a person described in subclause (I), in confidence, either upon the request of such person or upon the initiative of the attorney, with respect to any question asked of such person.

(cc) OBJECTIONS.—A person described in subclause (I), or the attorney for that person, may object on the record to any question, in whole or in part, and such person shall briefly state for the record the reason for the objection. An objection may properly be made, received, and entered upon the record when it is claimed that such person is entitled to refuse to answer the question on grounds of any constitutional or other legal right or privilege, including the privilege against self-incrimination, but such person shall not otherwise

object to or refuse to answer any question, and such person or attorney shall not otherwise interrupt the oral examination.

(dd) REFUSAL TO ANSWER.—If a person described in subclause (I) refuses to answer any question—

(AA) the Agency may petition the district court of the United States pursuant to this section for an order compelling such person to answer such question; and

(BB) if the refusal is on grounds of the privilege against self-incrimination, the testimony of such person may be compelled in accordance with the provisions of section 6004 of title 18, United States Code.

(V) TRANSCRIPTS.—For purposes of this paragraph—

(aa) after the testimony of any witness is fully transcribed, the Agency investigator shall afford the witness (who may be accompanied by an attorney) a reasonable opportunity to examine the transcript;

(bb) the transcript shall be read to or by the witness, unless such examination and reading are waived by the witness;

(cc) any changes in form or substance which the witness desires to make shall be entered and identified upon the transcript by the Agency investigator, with a statement of the reasons given by the witness for making such changes;

(dd) the transcript shall be signed by the witness, unless the witness in writing waives the signing, is ill, cannot be found, or refuses to sign; and

(ee) if the transcript is not signed by the witness during the 30-day period following the date on which the witness is first afforded a reasonable opportunity to examine the transcript, the Agency investigator shall sign the transcript and state on the record the fact of the waiver, illness, absence of the witness, or the refusal to sign, together with any reasons given for the failure to sign.

(VI) CERTIFICATION BY INVESTIGATOR.—The Agency investigator shall certify on the transcript that the witness was duly sworn by him or her and that the transcript is a true record of the testimony given by the witness, and the Agency investigator shall promptly deliver the transcript or send it by registered or certified mail to the custodian.

(VII) COPY OF TRANSCRIPT.—The Agency investigator shall furnish

a copy of the transcript (upon payment of reasonable charges for the transcript) to the witness only, except that the Agency may for good cause limit such witness to inspection of the official transcript of his testimony.

(VIII) WITNESS FEES.—Any witness appearing for the taking of oral testimony pursuant to a civil investigative demand shall be entitled to the same fees and mileage which are paid to witnesses in the district courts of the United States.

(D) CONFIDENTIAL TREATMENT OF DEMAND MATERIAL.—

(i) IN GENERAL.—Documentary materials and tangible things received as a result of a civil investigative demand shall be subject to requirements and procedures regarding confidentiality, in accordance with rules established by the Agency.

(ii) DISCLOSURE TO CONGRESS.—No rule established by the Agency regarding the confidentiality of materials submitted to, or otherwise obtained by, the Agency

shall be intended to prevent disclosure to either House of Congress or to an appropriate committee of the Congress, except that the Agency is permitted to adopt rules allowing prior notice to any party that owns or otherwise provided the material to the Agency and had designated such material as confidential.

(E) PETITION FOR ENFORCEMENT.—

(i) IN GENERAL.—Whenever any person fails to comply with any civil investigative demand duly served upon such person under this section, or whenever satisfactory copying or reproduction of material requested pursuant to the demand cannot be accomplished and such person refuses to surrender such material, the Agency, through such officers or attorneys as it may designate, may file, in the district court of the United States for any judicial district in which such person resides, is found, or transacts business, and serve upon such person, a petition for an order of such court for the enforcement of this paragraph.

(ii) SERVICE OF PROCESS.—All process of any court to which application may be made as provided in this subparagraph may be served in any judicial district.

(F) PETITION FOR ORDER MODIFYING OR SETTING ASIDE DEMAND.—

(i) IN GENERAL.—Not later than 20 days after the service of any civil investigative demand upon any person under subparagraph (B), or at any time before the return date specified in the demand, whichever period is shorter, or within such period exceeding 20 days after service or in excess of such return date as may be prescribed in writing, subsequent to service, by any Agency investigator named in the demand, such person may file with the Agency a petition for an order by the Agency modifying or setting aside the demand.

(ii) COMPLIANCE DURING PENDENCY.—The time permitted for compliance with the demand in whole or in part, as determined proper and ordered by the Agency, shall not run during the pendency

of a petition under clause (i) at the Agency, except that such person shall comply with any portions of the demand not sought to be modified or set aside.

(iii) SPECIFIC GROUNDS.—A petition under subparagraph (A) shall specify each ground upon which the petitioner relies in seeking relief, and may be based upon any failure of the demand to comply with the provisions of this section, or upon any constitutional or other legal right or privilege of such person.

(G) CUSTODIAL CONTROL.—At any time during which any custodian is in custody or control of any documentary material, tangible things, reports, answers to questions, or transcripts of oral testimony given by any person in compliance with any civil investigative demand, such person may file, in the district court of the United States for the judicial district within which the office of such custodian is situated, and serve upon such custodian, a petition for an order of such court requiring the performance by such custodian of any duty imposed

upon him by this section or rule promulgated by the Agency.

(H) JURISDICTION OF COURT.—

(i) IN GENERAL.—Whenever any petition is filed in any district court of the United States under this paragraph, such court shall have jurisdiction to hear and determine the matter so presented, and to enter such order or orders as may be required to carry out the provisions of this section.

(ii) APPEAL.—Any final order entered as described in subparagraph (A) shall be subject to appeal pursuant to section 1291 of title 28, United States Code.

(3) HEARINGS AND ADJUDICATORY PROCEEDINGS.—

(A) IN GENERAL.—The Agency is authorized to conduct hearings and adjudication proceedings with respect to any person in the manner prescribed by chapter 5 of title 5, United States Code in order to ensure or enforce compliance with—

(i) the provisions of this Act and other Federal privacy laws, including any

rules prescribed by the Agency under this Act and other Federal privacy laws; and

(ii) any other Federal privacy law that the Agency is authorized to enforce, and any rules or order prescribed thereunder, unless such Federal privacy law specifically limits the Agency from conducting a hearing or adjudication proceeding and only to the extent of such limitation.

(B) SPECIAL RULES FOR CEASE-AND-DESIST PROCEEDINGS.—

(i) ORDERS AUTHORIZED.—

(I) IN GENERAL.—If, in the opinion of the Agency, any data aggregator is engaging or has engaged in an activity that violates a law, rule, or any condition imposed in writing on the person by the Agency, the Agency may issue and serve upon the data aggregator or service provider a notice of charges in respect thereof.

(II) CONTENT OF NOTICE.—The notice under clause (i) shall contain a statement of the facts constituting the alleged violation or violations, and

shall fix a time and place at which a hearing will be held to determine whether an order to cease and desist should issue against the data aggregator or service provider, such hearing to be held not earlier than 30 days nor later than 60 days after the date of service of such notice, unless an earlier or a later date is set by the Agency, at the request of any party so served.

(III) CONSENT.—Unless the party or parties served under clause (ii) appear at the hearing personally or by a duly authorized representative, such person shall be deemed to have consented to the issuance of the cease-and-desist order.

(IV) PROCEDURE.—In the event of consent under clause (ii), or if, upon the record made at any such hearing, the Agency finds that any violation specified in the notice of charges has been established, the Agency may issue and serve upon the

data aggregator or service provider an order to cease and desist from the violation or practice. Such order may, by provisions which may be mandatory or otherwise, require the data aggregator or service provider to cease and desist from the subject activity, and to take affirmative action to correct the conditions resulting from any such violation.

(ii) EFFECTIVENESS OF ORDER.—A cease-and-desist order shall become effective at the expiration of 30 days after the date of service of an order under subparagraph (A) upon the data aggregator or service provider concerned (except in the case of a cease-and-desist order issued upon consent, which shall become effective at the time specified therein), and shall remain effective and enforceable as provided therein, except to such extent as the order is stayed, modified, terminated, or set aside by action of the Agency or a reviewing court.

(iii) DECISION AND APPEAL.—Any hearing provided for in this subsection shall be held in the Federal judicial district or in the territory in which the residence or principal office or place of business of the person is located unless the person consents to another place, and shall be conducted in accordance with the provisions of chapter 5 of title 5 of the United States Code. After such hearing, and within 90 days after the Agency has notified the parties that the case has been submitted to the Agency for final decision, the Agency shall render its decision (which shall include findings of fact upon which its decision is predicated) and shall issue and serve upon each party to the proceeding an order or orders consistent with the provisions of this section. Judicial review of any such order shall be exclusively as provided in this subsection. Unless a petition for review is timely filed in a court of appeals of the United States, as provided in subparagraph (D), and thereafter until the record in the proceeding has been

filed as provided in subparagraph (D), the Agency may at any time, upon such notice and in such manner as the Agency shall determine proper, modify, terminate, or set aside any such order. Upon filing of the record as provided, the Agency may modify, terminate, or set aside any such order with permission of the court.

(iv) APPEAL TO COURT OF APPEALS.—Any party to any proceeding under this subsection may obtain a review of any order served pursuant to this subparagraph (other than an order issued with the consent of the person concerned) by the filing in the court of appeals of the United States for the circuit in which the principal office of the covered person is located, or in the United States Court of Appeals for the District of Columbia Circuit, within 30 days after the date of service of such order, a written petition praying that the order of the Agency be modified, terminated, or set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Agency, and thereupon

the Agency shall file in the court the record in the proceeding, as provided in section 2112 of title 28 of the United States Code. Upon the filing of such petition, such court shall have jurisdiction, which upon the filing of the record shall except as provided in the last sentence of subparagraph (C) be exclusive, to affirm, modify, terminate, or set aside, in whole or in part, the order of the Agency. Review of such proceedings shall be had as provided in chapter 7 of title 5 of the United States Code. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court of the United States, upon certiorari, as provided in section 1254 of title 28 of the United States Code.

(v) NO STAY.—The commencement of proceedings for judicial review under clause (iv) shall not, unless specifically ordered by the court, operate as a stay of any order issued by the Agency.

(C) SPECIAL RULES FOR TEMPORARY CEASE-AND-DESIST PROCEEDINGS.—

(i) IN GENERAL.—Whenever the Agency determines that the violation specified in the notice of charges served upon a data aggregator, including a service provider, pursuant to paragraph (2), or the continuation thereof, is likely to cause the person to be insolvent or otherwise prejudice the interests of individuals before the completion of the proceedings conducted pursuant to paragraph (2), the Agency may issue a temporary order requiring the data aggregator or service provider to cease and desist from any such violation or practice and to take affirmative action to prevent or remedy such insolvency or other condition pending completion of such proceedings. Such order may include any requirement authorized under this Act. Such order shall become effective upon service upon the data aggregator or servicer provider and, unless set aside, limited, or suspended by a court in proceedings authorized by clause (ii), shall remain effective and enforceable pending the completion of the administrative proceedings pursuant to

such notice and until such time as the Agency shall dismiss the charges specified in such notice, or if a cease-and-desist order is issued against the person, until the effective date of such order.

(ii) APPEAL.—Not later than 10 days after the data aggregator or service provider concerned has been served with a temporary cease-and-desist order, the data aggregator or service provider may apply to the United States district court for the judicial district in which the residence or principal office or place of business of such data aggregator or servicer provider is located, or the United States District Court for the District of Columbia, for an injunction setting aside, limiting, or suspending the enforcement, operation, or effectiveness of such order pending the completion of the administrative proceedings pursuant to the notice of charges served upon the data aggregator or servicer provider under subparagraph (B), and such court shall have jurisdiction to issue such injunction.

(iii) INCOMPLETE OR INACCURATE RECORDS.—

(I) TEMPORARY ORDER.—If a notice of charges served under paragraph (2) specifies, on the basis of particular facts and circumstances, that the books and records of a data aggregator or service provider are so incomplete or inaccurate that the Agency is unable to determine the financial condition of that data aggregator or service provider or the details or purpose of any transaction or transactions that may have a material effect on the financial condition of that person, the Agency may issue a temporary order requiring—

(aa) the cessation of any activity or practice which gave rise, whether in whole or in part, to the incomplete or inaccurate state of the books or records; or

(bb) affirmative action to restore such books or records to a complete and accurate state,

until the completion of the proceedings under paragraph (2)(A).

(II) EFFECTIVE PERIOD.—Any temporary order issued under clause (i)—

(aa) shall become effective upon service; and

(bb) unless set aside, limited, or suspended by a court in proceedings under subparagraph (B), shall remain in effect and enforceable until the earlier of—

(AA) the completion of the proceeding initiated under paragraph (2) in connection with the notice of charges; or

(BB) the date the Agency determines, by examination or otherwise, that the books and records of the covered person or service provider are accurate and reflect the financial condition thereof.

(D) SPECIAL RULES FOR ENFORCEMENT OF ORDERS.—

(i) IN GENERAL.—The Agency may in its discretion apply to the United States district court within the jurisdiction of which the principal office or place of business of the person is located, for the enforcement of any effective and outstanding notice or order issued under this section, and such court shall have jurisdiction and power to order and require compliance herewith.

(ii) EXCEPTION.—Except as otherwise provided in this subparagraph, no court shall have jurisdiction to affect by injunction or otherwise the issuance or enforcement of any notice or order or to review, modify, suspend, terminate, or set aside any such notice or order.

(E) RULES.—The Agency shall prescribe rules establishing such procedures as may be necessary to carry out this paragraph.

(4) LITIGATION AUTHORITY.—

(A) IN GENERAL.—If any person violates this Act, a rule or order issued under this Act,

or a Federal privacy law, the Agency may commence a civil action against such person to impose a civil penalty or to seek all appropriate legal and equitable relief including a permanent or temporary injunction as permitted by law.

(B) REPRESENTATION.—The Agency may act in its own name and through its own attorneys in enforcing any provision of this Act, rules thereunder, or any other law or regulation, or in any action, suit, or proceeding to which the Agency is a party.

(C) COMPROMISE OF ACTIONS.—The Agency may compromise or settle any action if such compromise is approved by the court.

(D) NOTICE TO THE ATTORNEY GENERAL.—

(i) IN GENERAL.—When commencing a civil action under this Act or any Federal privacy law, or any rule thereunder, the Agency shall notify the Attorney General.

(ii) NOTICE AND COORDINATION.—

(I) NOTICE OF OTHER ACTIONS.—In addition to any notice required under subparagraph (A), the Agency shall notify the Attorney Gen-

eral concerning any action, suit, or proceeding to which the Agency is a party, except an action, suit, or proceeding that involves a violation of this Act or a Federal privacy law.

(II) COORDINATION.—In order to avoid conflicts and promote consistency regarding litigation of matters under Federal law, the Attorney General and the Agency shall consult regarding the coordination of investigations and proceedings, including by negotiating an agreement for coordination by not later than 180 days after the designated transfer date. The agreement under this subclause shall include provisions to ensure that parallel investigations and proceedings involving the Federal privacy laws are conducted in a manner that avoids conflicts and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(III) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Agency under this title, including the authority to interpret Federal privacy law.

(E) APPEARANCE BEFORE THE SUPREME COURT.—The Agency may represent itself in its own name before the Supreme Court of the United States, if the Agency makes a written request to the Attorney General within the 10-day period that begins on the date of entry of the judgment that would permit any party to file a petition for writ of certiorari, and the Attorney General concurs with such request or fails to take action within 60 days of the request of the Agency.

(F) FORUM.—Any civil action brought under a Federal privacy law may be brought in a United States district court or in any court of competent jurisdiction of a State in a district in which the defendant is located or resides or is doing business, and such court shall have jurisdiction to enjoin such person and to require compliance with any Federal privacy law.

(G) TIME FOR BRINGING ACTION.—Except as otherwise permitted by law or equity, no action may be brought under this Act or other Federal privacy law more than 5 years after the date of discovery of the violation to which an action relates.

(5) RELIEF AVAILABLE.—

(A) ADMINISTRATIVE PROCEEDINGS OR COURT ACTIONS.—

(i) JURISDICTION.—The court (or the Agency, as the case may be) in an action or adjudication proceeding brought under this Act or a Federal privacy law, shall have jurisdiction to grant any appropriate legal or equitable relief with respect to a violation of this Act or Federal privacy law, including a violation of a rule or order prescribed under this Act or Federal privacy law.

(ii) RELIEF.—Relief under this section may include, without limitation—

(I) rescission or reformation of contracts;

(II) refund of moneys or return of real property;

(III) restitution;

(IV) disgorgement of any revenue, data, or technologies, including automated decision systems, data sets, or algorithms, attributable to a violation of this Act, Federal privacy law, or any rule or order issued by the Agency under this Act;

(V) payment of damages or other monetary relief;

(VI) public notification regarding the violation, including the costs of notification;

(VII) limits on the activities or functions of the person; and

(VIII) civil money penalties, as set forth more fully in paragraph (3).

(iii) NO EXEMPLARY OR PUNITIVE DAMAGES.—Nothing in this subparagraph shall be construed as authorizing the imposition of exemplary or punitive damages in an action brought by the Agency.

(B) RECOVERY OF COSTS.—In any action brought by the Agency, a State attorney general, or any State regulator to enforce this Act

or any Federal privacy law, the Agency, the State attorney general, or the State regulator may recover its costs in connection with prosecuting such action if the Agency, the State attorney general, or the State regulator is the prevailing party in the action.

(C) CIVIL MONEY PENALTY IN COURT AND ADMINISTRATIVE ACTIONS.—

(i) IN GENERAL.—Any person that violates, through any act or omission, any provision of this Act or any Federal privacy law shall forfeit and pay a civil penalty pursuant to this subparagraph.

(ii) PENALTY AMOUNTS.—

(I) FIRST TIER.—For any violation of a law, rule, or final order or condition imposed in writing by the Agency, a civil penalty may not exceed—

(aa) $5,000 for each day during which such violation or failure to pay continues; or

(bb) $15,000 for each day during which such violation or failure to pay continues if such

violation involves the personal data of individuals under the age of 13.

(II) SECOND TIER.—Notwithstanding clause (i), for any person that recklessly engages in a violation of this Act or any Federal privacy law, a civil penalty may not exceed—

(aa) $25,000 for each day during which such violation or failure to pay continues; or

(bb) $75,000 for each day during which such violation or failure to pay continues if such violation involves the personal data of individuals under the age of 13.

(III) THIRD TIER.—Notwithstanding clauses (i) and (ii), for any person that knowingly violates this Act or any Federal privacy law, a civil penalty may not exceed—

(aa) $1,000,000 for each day during which such violation continues; or

(bb) $3,000,000 for each day during which such violation or failure to pay continues if such violation involves the personal data of individuals under the age of 13.

(iii) PENALTIES FOR RE-IDENTIFYING DATA.—Any person that re-identifies, or attempts to re-identify, anonymized data shall be assessed a third tier civil penalty under subparagraph (B), unless conducting authorized testing to prove personal data has been anonymized.

(iv) MITIGATING FACTORS.—In determining the amount of any penalty assessed under subparagraph (B), the Agency or the court shall take into account the appropriateness of the penalty with respect to—

(I) the size of financial resources and good faith of the person charged;

(II) the gravity of the violation or failure to pay;

(III) the severity of the risks or harms to individuals;

(IV) the history of previous violations; and

(V) such other matters as justice may require.

(v) AUTHORITY TO MODIFY OR REMIT PENALTY.—The Agency may compromise, modify, or remit any penalty which may be assessed or had already been assessed under subparagraph (B). The amount of such penalty, when finally determined, shall be exclusive of any sums owed by the person to the United States in connection with the costs of the proceeding, and may be deducted from any sums owed by the United States to the person charged.

(vi) NOTICE AND HEARING.—No civil penalty may be assessed under this subsection with respect to a violation of this Act or any Federal privacy law, unless—

(I) the Agency gives notice and an opportunity for a hearing to the person accused of the violation; or

(II) the appropriate court has ordered such assessment and entered judgment in favor of the Agency.

(6) REFERRALS FOR CRIMINAL PROCEEDINGS.—If the Agency obtains evidence that any person, domestic or foreign, has engaged in conduct that may constitute a violation of Federal criminal law, the Agency shall transmit such evidence to the Attorney General of the United States, who may institute criminal proceedings under appropriate law. Nothing in this section affects any other authority of the Agency to disclose information.

SEC. 104. RELATION TO OTHER LAWS AND AGENCIES.

(a) TRANSFERS OF FUNCTIONS.—

(1) FEDERAL TRADE COMMISSION.—The authority of the Federal Trade Commission under a Federal privacy law to prescribe rules, issue guidelines, or conduct a study or issue a report mandated under such law shall be transferred to the Agency on the transfer date. Nothing in this Act shall be construed to require a mandatory transfer of any employee of the Federal Trade Commission.

(2) AGENCY AUTHORITY.—

(A) IN GENERAL.—The Agency shall have all powers and duties under the Federal privacy laws to prescribe rules, issue guidelines, or to conduct studies or issue reports mandated by such laws, that were vested in the Federal

Trade Commission on the day before the transfer date.

(B) FEDERAL TRADE COMMISSION ACT.—The Agency may enforce a rule prescribed under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to the collection, disclosure, processing and misuse of personal data.

(3) AUTHORITY OF THE FEDERAL TRADE COMMISSION.—No provision of this Act shall be construed as modifying, limiting, or otherwise affecting the authority of the Federal Trade Commission, including the authority with respect to large data collectors described in section 202(a)(1) of this Act, under the Federal Trade Commission Act (15 U.S.C. 41 et seq.), or any other law, other than the authority under a Federal privacy law to prescribe rules, issue official guidelines, or conduct a study or issue a report mandated under such law.

(4) AUTHORITY OF THE BUREAU OF CONSUMER FINANCIAL PROTECTION.—No provision of this Act shall be construed as modifying, limiting, or otherwise affecting the authority of the Bureau of Consumer Financial Protection under the Dodd-Frank

Wall Street Reform and Consumer Protection Act (12 U.S.C. 5301 et seq.) or any other law.

(b) COORDINATION.—The Agency shall coordinate with the Consumer Financial Protection Bureau, the Federal Communications Commission, the Federal Trade Commission, the Department of Commerce, the Department of Health and Human Services, the Department of Housing and Urban Development, the Department of Education, the Equal Employment Opportunity Commission, the National Security Agency, the National Institute of Standards and Technology, the White House Office of Science and Technology Policy, the Cybersecurity and Infrastructure Security Agency, and other Federal agencies that implement, enforce or otherwise have responsibilities relating to privacy or data protection, and State regulators, as appropriate, to promote consistent regulatory treatment of personal data.

SEC. 105. FUNDING.

(a) FUNDING; PENALTIES AND FINES.—

(1) FUNDING.—

(A) ASSESSMENTS, FEES, CHARGES.—

(i) GENERAL AUTHORITY.—The Director may collect an assessment, fee, or other charge from a data aggregator that has annual gross revenues that exceed

$25,000,000 or annually collects, uses, or shares, alone or in combination, the personal data of 50,000 or more individuals, households, or devices.

(ii) DETERMINATION OF AMOUNT.—In establishing the amount of any assessment, fee, or charge collected from a data aggregator under this section, the Director may take into account any factor that the Director determines is appropriate.

(B) AUTHORITY OF DIRECTOR.—The Director shall have sole authority to determine the manner in which the obligations of the Agency shall be incurred and its disbursements and expenses allowed and paid, in accordance with this section, except as provided in chapter 71 of title 5, United States Code (with respect to compensation).

(2) DATA PROTECTION AGENCY FUND.—

(A) SEPARATE FUND IN FEDERAL RESERVE ESTABLISHED.—There is established in the Federal Reserve a separate fund, to be known as the ''Data Protection Agency Fund'' (referred to in this section as the ''Agency Fund''). The Agency Fund shall be maintained

and established at a Federal reserve bank, in accordance with such requirements as the Board of Governors may impose.

(B) FUND RECEIPTS.—All amounts transferred to the Agency under subsection (a) shall be deposited into the Agency Fund.

(C) INVESTMENT AUTHORITY.—

(i) AMOUNTS IN AGENCY FUND MAY BE INVESTED.—The Agency may request the Board of Governors to direct the investment of the portion of the Agency Fund that is not, in the judgment of the Agency, required to meet the current needs of the Agency.

(ii) ELIGIBLE INVESTMENTS.—Investments authorized by this paragraph shall be made in obligations of the United States or obligations that are guaranteed as to principal and interest by the United States, with maturities suitable to the needs of the Agency Fund, as determined by the Agency.

(iii) INTEREST AND PROCEEDS CREDITED.—The interest on, and the proceeds from the sale or redemption of, any obliga-

tions held in the Agency Fund shall be credited to the Agency Fund.

(3) USE OF FUNDS.—

(A) IN GENERAL.—Funds obtained by, transferred to, or credited to the Agency Fund shall be immediately available to the Agency and under the control of the Director, and shall remain available until expended, to pay the expenses of the Agency in carrying out its duties and responsibilities. The compensation of the Director and other employees of the Agency and all other expenses thereof may be paid from, obtained by, transferred to, or credited to the Agency Fund under this section.

(B) FUNDS THAT ARE NOT GOVERNMENT FUNDS.—Funds obtained by or transferred to the Agency Fund shall not be construed to be Government funds or appropriated monies.

(C) AMOUNTS NOT SUBJECT TO APPORTIONMENT.—Notwithstanding any other provision of law, amounts in the Agency Fund and in the Civil Penalty Fund established under subsection (d) shall not be subject to apportionment for purposes of chapter 15 of title 31,

United States Code, or under any other authority.

(4) PENALTIES AND FINES.—

(A) ESTABLISHMENT OF VICTIMS RELIEF FUND .—There is established in the Federal Reserve a separate fund, to be known as the ''Data Protection Civil Penalty Fund'' (referred to in this section as the ''Civil Penalty Fund''). The Civil Penalty Fund shall be maintained and established at a Federal reserve bank, in accordance with such requirements as the Board of Governors may impose. If the Agency obtains a civil penalty against any person in any judicial or administrative action under Federal laws, the Agency shall deposit into the Civil Penalty Fund, the amount of the penalty collected.

(B) PAYMENT TO VICTIMS.—Amounts in the Civil Penalty Fund shall be available to the Agency, without fiscal year limitation, for payments to the victims of activities for which civil penalties have been imposed under this Act and for other violations of other Federal privacy laws. If individual victims can be identified through reasonable effort, and the distributions

are sufficiently large to make individual distributions economically viable, penalties should be distributed directly to individual victims. To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable or economically viable, the Agency may—

(i) use such funds for the purpose of consumer or business education relating to data protection or for the purpose of engaging in technological research that the Agency considers necessary to enforce this Act and Federal privacy laws; and

(ii) utilize a cy-pres approach to distribute funds in order to advance data protection and privacy in the United States. The Agency may identify recipients, including charitable and civil society organizations, whose interests reasonable approximate those of the victims of the activities for which civil penalties have been imposed and distribute funds from the Civil Penalty Fund to those recipients.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Agency such sums as may be necessary to carry out this Act.

TITLE II—PRIVACY PROTECTIONS

SEC. 201. PROHIBITED ACTS.

It shall be unlawful for—

(1) any data aggregator or service provider to commit any act or omission in violation of this Act, Federal privacy law, or any rule or order issued by the Agency under this Act;

(2) any data aggregator or service provider to commit any unlawful, unfair, deceptive, abusive, or discriminatory acts or practices in connection with the collection, processing, or sharing of personal data;

(3) any data aggregator or service provider to fail or refuse as required by this Act or Federal privacy law, or any rule or order issued by the Agency thereunder—

(A) to permit access to or copying of records;

(B) to establish or maintain records; or

(C) to make reports or provide information to the Agency;

(4) any person to knowingly or recklessly provide substantial assistance to a data aggregator or service provider in violation of this Act or Federal privacy law, or any rule or order issued thereunder, and notwithstanding any provision of this Act, the provider of such substantial assistance shall be deemed to be in violation of this Act or Federal privacy law to the same extent as the person to whom substantial assistance is provided; or

(5) any person, data aggregator, or service provider to re-identify, or attempt to re-identify, an individual, household, or device from anonymized data, unless such person, data aggregator, or service provider is conducting authorized testing to prove personal data has been anonymized.

SEC. 202. SUPERVISION OF DATA AGGREGATORS.

(a) IN GENERAL.—A large data aggregator is a data aggregator that satisfies one or more of the following thresholds:

(1) The data aggregator has annual gross revenues that exceed $25,000,000.

(2) The data aggregator annually collects, uses, or shares, alone or in combination, the personal data of 50,000 or more individuals, households, or devices.

(b) SUPERVISION.—The Agency may require reports and conduct examinations on a periodic basis of large data aggregators described in subsection (a) for purposes of—

(1) assessing compliance with the requirements of this Act, rules and orders issued by the Agency, or other Federal privacy laws;

(2) obtaining information about the activities subject to such laws and the associated compliance systems or procedures of such entities;

(3) detecting and assessing associated risks to individuals and groups of individuals; and

(4) requiring and overseeing high-risk data practice risk impact assessments and high-risk data practice impact evaluations to advance fair and just data practices.

(c) PUBLICLY ACCESSIBLE LIST.—

(1) IN GENERAL.—The Agency shall maintain a publicly accessible list of data aggregators that collect, process, or share personal data of more than 10,000 persons or households, and the permissible purposes for which the data aggregators purport to collect personal data.

(2) CONTRACTING AUTHORITY.—The Agency may contract with a State to procure a list (or technological system for managing and accessing such a

list) of data aggregators similar to the list described in paragraph (1).

(d) MERGER REVIEW.—The Agency shall conduct a review and submit to the Federal Trade Commission and Department of Justice a report on the privacy and data protection implications of—

(1) any merger involving a data aggregator described in subsection (a); or

(2) any merger that proposes the transfer of personal data of 50,000 or more individuals.

TITLE III—MISCELLANEOUS

SEC. 301. INITIAL REGULATIONS.

The Agency shall issue such regulations, after notice and comment in accordance with section 553 of title 5, United States Code, as may be necessary to carry out this Act. The Agency shall prescribe rules applicable to a data aggregator or service provider identifying—

(1) high-risk data practices in connection with the collection, processing, or sharing of personal data, which may include requirements for—

(A) the purpose of auditing, preventing, or restricting such acts or practices;

(B) limiting the collection, processing, and sharing of personal data to what is reasonably necessary to provide or maintain the specific

product or service requested by the individual or for other permissible purposes as prescribed by the Agency; and

(C) heightened protections for sensitive personal data, as defined by the Agency;

(2) acts or practices in connection with the collection, processing, or sharing of personal data that causes or are likely to cause privacy harm to individuals or groups of individuals, which may include requirements for—

(A) the limited purpose of preventing or restricting such acts or practices; and

(B) minimizing—

(i) the collection of personal data to not more than is reasonably necessary to provide a product or service that an individual or other end user has requested;

(ii) the processing or sharing of personal data to not more than is reasonably necessary to meet the purposes for which the personal data was collected; and

(iii) the retention of personal data to not longer than is necessary to meet the purposes for which the personal data was collected;

(3) unlawful, unfair, deceptive, abusive, or discriminatory acts or practices in connection with the collection, processing, or sharing of personal data, which may include requirements for the purpose of preventing or restricting such acts or practices, for the purpose of preventing disparate impacts on the basis of protected class, or for the purpose of affirmatively furthering equal opportunity;

(4) rights that data aggregators must provide to individuals, including the right to access and correct, limit the processing of, and request deletion of the individual's personal data; and

(5) obligations on data aggregators, including transparency about business practices, data collection limitations, processing and disclosure limitations, purpose specification and legal basis for processing requirements, accountability requirements, confidentiality and security requirements, and data accuracy requirements.

SEC. 302. SEVERABILITY.

If any provision of this Act, an amendment made by this Act, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this Act, the amendments made by this Act, and the application of the provisions of such

to any person or circumstance shall not be affected thereby.

SEC. 303. RELATION TO FEDERAL AND STATE LAW.

(a) RELATION TO STATE LAW.—

(1) RULE OF CONSTRUCTION.—This Act may not be construed as annulling, altering, or affecting, or exempting any person subject to the provisions of this Act from complying with, the statutes, regulations, orders, or interpretations in effect in any State, except to the extent that any such provision of law is inconsistent with the provisions of this Act, and then only to the extent of the inconsistency.

(2) GREATER PROTECTION UNDER STATE LAW.—For purposes of this paragraph, a statute, regulation, order, or interpretation in effect in any State is not inconsistent with the provisions of this Act if the protection that such statute, regulation, order, or interpretation affords to individuals is greater than the protection provided under this Act. A determination regarding whether a statute, regulation, order, or interpretation in effect in any State is inconsistent with the provisions of this Act may be made by the Agency on its own motion or in response to a nonfrivolous petition initiated by any interested person.

(b) RELATION TO OTHER PROVISIONS OF FEDERAL PRIVACY LAWS THAT RELATE TO STATE LAW.—No provision of this Act shall be construed as modifying, limiting, or superseding the operation of any provision of a Federal privacy law that relates to the application of a law in effect in any State with respect to such Federal law.

(c) PRESERVATION OF ENFORCEMENT POWERS OF STATES.—The attorney general (or the equivalent thereof) of any State may bring a civil action in the name of such State in any district court of the United States in that State or in State court that is located in that State and that has jurisdiction over the defendant, to enforce provisions of this Act or rules or orders issued under this Act, and to secure remedies under provisions of this Act or remedies otherwise provided under other law. A State regulator may bring a civil action or other appropriate proceeding to enforce the provisions of this Act or rules or orders issued under this Act with respect to any entity that is State-chartered, incorporated, licensed, or otherwise authorized to do business under State law (except as provided in paragraph (2)), and to secure remedies under provisions of this Act or remedies otherwise provided under other provisions of law with respect to such an entity.

(d) PRESERVATION OF STATE AUTHORITY.—

(1) STATE CLAIMS.—No provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or any other regulatory or enforcement agency or authority to bring an action or other regulatory proceeding arising solely under the law in effect in that State.

(2) STATE CONSUMER PROTECTION, PRIVACY, AND DATA REGULATORS.—No provision of this Act shall be construed as altering, limiting, or affecting the authority of a State consumer protection, data protection, or privacy agency (or any agency or office performing like functions) under State law to adopt rules, initiate enforcement proceedings, or take any other action with respect to a person regulated by such commission or authority.