To provide for data accountability and transparency.

IN THE SENATE OF THE UNITED STATES

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

A BILL

To provide for data accountability and transparency.

Be it enacted by the Senate and House of Represe-
tatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Data Accountability and Transparency Act of 2020”.

SEC. 2. FINDINGS.

Congress finds that—

(1) privacy is a fundamental individual right protected by the Constitution of the United States;

(2) the right of privacy is widely recognized in international legal instruments that the United States has endorsed, ratified, or promoted;
(3) the right to privacy protects the individual against intrusions into seclusion, protects individual autonomy, safeguards fair use of data that pertains to the individual, advances the just use of data, and contributes to respect for civil rights and fundamental freedoms;

(4) privacy protections not only protect and benefit the individual, but also advance other societal interests, including—

(A) the protection of marginalized and vulnerable groups of individuals; and

(B) the safeguarding of—

(i) other foundational values of the democracy of the United States, such as freedom of information, freedom of speech, justice, and human ingenuity and dignity; and

(ii) the integrity of democratic institutions, including fair and open elections;

(5) in order to protect the privacy of individuals, groups of individuals, and support society, it is necessary and proper for Congress to regulate the collection, maintenance, use, processing, storage, and dissemination of information; and
(6) this Act protects these rights and concrete interests and is intended to prevent harm to individuals that would otherwise be caused by the unrestricted collection, use, or sharing of personal data.

SEC. 3. DEFINITIONS.

In this Act:

(1) AFFILIATE.—The term “affiliate” means any person that controls, is controlled by, or is under common control with another person.

(2) AGENCY.—The term “Agency” means the Data Accountability and Transparency Agency established under section 301.

(3) ANONYMIZED DATA.—The term “anonymized data” means information that has been proven to not identify, relate to, describe, reference, be capable of being associated with, or be linked or reasonably linkable to a particular individual or device.

(4) 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 makes a decision, or facilitates human decisionmaking.
(5) AUTOMATED DECISION SYSTEM IMPACT EVALUATION.—The term “automated decision system impact evaluation” means a study conducted after deployment of an automated decision system that includes, at a minimum—

(A) an evaluation of an automated decision system’s accuracy, bias on the basis of protected class, and impact on privacy on individuals or groups of individuals;

(B) an evaluation of the effectiveness of measures taken to minimize risks as outlined in any prior automated decision system risk assessments; and

(C) recommended measures to further minimize risks to accuracy, bias on the basis of protected class, and privacy on individuals or groups of individuals.

(6) AUTOMATED DECISION SYSTEM RISK ASSESSMENT.—The term “automated decision system risk assessment” means a study evaluating an automated decision system and the automated decision system’s development process, including the design and training data of the automated decision system, for potential risks to accuracy, bias, discrimination,
and privacy on individuals or groups of individuals that includes, at a minimum—

(A) a detailed description of the automated decision system, including—

(i) its design and methodologies;

(ii) training data characteristics;

(iii) data; and

(iv) purpose;

(B) an assessment of the automated decision system governance in light of its purpose, potential unintended consequences, and taking into account relevant factors, including—

(i) the duration and methods for which personal data and the results of the automated decision system are stored;

(ii) what information about the automated decision system (including inputs, features, and results) is available to individuals; and

(iii) the recipients of the results of the automated decision system;

(C) an assessment of the risks posed by the automated decision system—

(i) poses to individuals or groups of individuals of privacy harm; and
(ii) may result in or contribute to inaccurate, biased, or discriminatory decisions impacting individuals or groups of individuals;

(D) the measures a data aggregator will employ to minimize the risks described in subparagraph (C), including technological and physical safeguards.

(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 observing the behavior of an individual.

(8) DATA AGGREGATOR.—The term “data aggregator”—

(A) means any person that collects, uses, or shares an amount of personal data that is not de minimis; and
(B) does not include an individual who collects, uses, or shares personal data solely for personal reasons.

(9) 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.

(10) DIRECTOR.—The term “Director” means the Director of the Data Accountability and Transparency Agency.

(11) 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.

(12) FACIAL RECOGNITION TECHNOLOGY.—The term “facial recognition technology” means an automated or semiautomated process that assists in identifying or verifying an individual based on the characteristics of the face of an individual.

(13) 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 by such laws):

(A) Title V of the Gramm-Leach-Bliley Act (Public Law 106–102; 113 Stat. 1338).

(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.).


(L) Section 552a of title 5, United States Code.


(Q) Sections 1028A, 1030, 1801, 2710, and 2721 and chapter 119, of title 18, United States Code.

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

(T) The Census Confidentiality Statute of 1954. [Note: Unclear what this is meant to reference -- I can’t find a match for this short title. Please clarify.]


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

(14) INDIVIDUAL.—The term “individual” means a natural person.

(15) INTENTIONAL INTERACTION.—The term “intentional interaction” means an interaction in which an individual engages in 1 or more actions to demonstrate that the individual intends to interact with a data aggregator.

(16) JOURNALISM.—The term “journalism”—
(A) means the gathering, preparing, collecting, photographing, recording, writing, editing, reporting, or publishing of news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public; and

(B) includes the collection or use of personal data about a public individual or official, or that otherwise concerns matters of public interest, for dissemination to the public.

(17) **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.

(18) **PERSONAL DATA.**—The term “personal data” means electronic data that, alone or in combination with other data—

(A) could be linked or reasonably linkable to an individual, household, or device; or

(B) could be used to determine that an individual or household is part of a protected class.
12

(19) 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, or potentially caused, in whole or in part, by the collection, use, 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 or the otherwise unfair or unethical differential treatment with respect to an individual, including in a manner that is prohibited under section 104;

(F) the interference with, or the surveillance of, activities that are protected by the First Amendment to the Constitution of the United States;

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

(H) the impairment of the autonomy of an individual or society generally; and

(I) any harm fairly traceable to an invasion of privacy tort; and

(J) any other adverse consequence, or potential adverse consequence, consistent with the provisions of this Act, as determined by the Director.

(20) PROTECTED CLASS.—The term “protected class” means the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender
identity, sexual orientation, familial status, biometric
information, lawful source of income, or disability of
an individual or a group of individuals.

(21) Public accommodation.—The term
“public accommodation” means any type of business
considered a place of public accommodation pursuant
to section 201(b) of the Civil Rights Act of 1964
(42 U.S.C. 2000a(b)) or section 301(7) of the Amer-
icans with Disabilities Act of 1990 (42 U.S.C.
12181(7)) or a business that offers goods or services
through the internet to the general public.

(22) Service provider.—The term “service
provider” means a data aggregator that collects,
uses, or shares personal data only on behalf of an-
other data aggregator in order to carry out a per-
missible purpose.

(23) Share.—The term “share” means dis-
seminating, making available, transferring, or other-
wise communicating orally, in writing, or by elec-
tronic or other means, personal data, except for as
required under section 201 of this Act.

(24) Use.—The term “use” means to perform
an operation or a set of operations on personal data,
either manually or by automated means, after the
collection of the data, including—
(A) the analysis, organization, storage, re-
tention, or maintenance of the data; and

(B) the derivation or inference of informa-
tion from the personal data.

(25) VERIFIABLE REQUEST.—The term
“verifiable request” means a request that a data
aggregator can reasonably verify is made—

(A) by an individual;

(B) by an individual on behalf of the indi-
vidual’s minor child; or

(C) by a person registered with the Sec-
retary of State authorized by the individual to
act on the individual’s behalf.

SEC. 4. SEVERABILITY.

If any provision of this Act, an amendment made by
this Act, or the application of such provision or amend-
ment to any person or circumstance is held to be unconsti-
tutional, the remainder of this Act, the amendments made
by this Act, and the application of the provisions of such
to any person or circumstances shall not be affected there-
by.
TITLE I—REQUIREMENTS FOR DATA AGGREGATORS

SEC. 101. BAN ON DATA PRACTICES WITHOUT A PERMISSIBLE PURPOSE.

A data aggregator shall not collect, use, or share, or cause to be collected, used, or shared any personal data, unless the data aggregator can demonstrate that such personal data is strictly necessary to carry out a permissible purpose under section 102.

SEC. 102. PERMISSIBLE PURPOSES.

(a) Permissible Purposes.—A data aggregator may not collect, use, or share personal data unless strictly necessary to carry out one or more of the following permissible purposes:

(1) To provide a good, service, or specific feature requested by an individual in an intentional interaction.

(2) To engage in journalism, provided that the data aggregator has reasonable safeguards and processes that prevent the collection, use, or sharing of personal data for commercial purposes other than journalism.

(3) To conduct public or peer-reviewed scientific, historical, or statistical research in the public
interest, but only to the extent such research is not possible using anonymized data.

(4) To employ an individual, including for administration of wages and benefits, except that a data aggregator may not invasively collect, use, or share the employee’s personal data in carrying out this paragraph.

(5) Where mandated to comply with Federal, State, or local law.

(6) Consistent with due process, direct compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons.

(7) To bring or defend legal claims, provided that the parties or potential parties take all necessary measures, including, as applicable, obtaining a protective order, to protect against unnecessary public disclosure of personal data.

(8) To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.

(9) Free expression by individuals on a social network or media platform.

(10) In exigent circumstances, if first responders or medical personnel, in good faith, believe dan-
ger of death or serious physical injury to an individual, or danger of serious and unlawful injury to property, requires collection, use, or sharing of personal data relating to the exigent circumstances.

(11) The development and delivery of advertisements—

(A) based on the content of the website, online service, or application to which the individual or device is connected; and

(B) excludes advertising based on the use of any personal data collected or stored from previous interactions with the individual or device, a profile of the individual or device, or the previous online or offline behavior of the individual or device.

(12) To offer discounted or free goods or services to an individual if—

(A) the offering is in connection with the voluntary participation by the individual in a program that rewards individuals for patronage; and

(B) personal data is only collected to track purchases for loyalty rewards under the program described in subparagraph (A).
(b) Restrictions on Permissible Purposes.—Except where strictly necessary to carry out a permissible purpose, a data aggregator shall not—

(1) share personal data with affiliated entities, service providers, or third parties;

(2) use personal data for any purpose other than to carry out a permissible purpose;

(3) retain personal data for any time longer than strictly necessary to carry out a permissible purpose; or

(4) derive or infer data from any element or set of personal data.

(c) Rule of Construction.—Collecting, using, or sharing personal data to generate advertising revenue to support or carry out a permissible purpose is not a permissible purpose.

SEC. 103. UNLAWFUL DATA PRACTICES.

(a) In General.—It is unlawful for a person to engage or cause to be engaged in the following practices:

(1) Charge an extra fee or raise the price for a good, service, or feature when a person exercises the rights of the person under this Act.

(2) Terminate, refuse to provide, degrade goods or services to, or otherwise retaliate against, a per-
son that exercises the rights of the person under this Act.

(3) Re-identify, or attempt to re-identify, an individual, household, or device from anonymized data (unless conducting authorized testing to prove personal data has been anonymized).

(4) Commingle personal data from multiple applications, services, affiliates, or independent business lines.

(b) FACIAL RECOGNITION TECHNOLOGY.—It is unlawful for any data aggregator to—

   (1) use facial recognition technology; or

   (2) collect, use, or share any personal data obtained from facial recognition technology.

(c) RULE OF CONSTRUCTION.—A person is prohibited from engaging in the unlawful data practices in subsection (a) regardless of whether such person has a permissible purpose for collecting, using, or sharing personal data.

(d) DAMAGES.—In addition to the relief available under section 401(c), a data aggregator shall be subject to treble damages for a violation of this section.
SEC. 104. PROHIBITION ON DISCRIMINATORY USE OF PERSONAL DATA.

(a) Prohibition on Discrimination in Economic Opportunities.—It is unlawful for a data aggregator to collect, use, or share personal data for advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, or insurance in a manner that discriminates against or otherwise makes the opportunity unavailable or offered on different terms on the basis of a protected class or otherwise materially contributes to unlawful discrimination.

(b) Prohibition on Discrimination in Public Accommodations.—

(1) In General.—It is unlawful for a data aggregator to collect, use, or share personal data in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a protected class.

(2) Burden of Proof.—The burden of proof for disparate impact cases set forth in subsection (a)(2) applies to cases with respect to this subsection.
(3) INTERFERENCE WITH RIGHTS AND PRIVILEGES.—It is unlawful for a data aggregator to—

(A) withhold, deny, deprive, or attempt to withhold, deny, or deprive any individual of any right or privilege secured by this subsection;

(B) intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any individual with the purpose of interfering with any right or privilege secured by this subsection; or

(C) punish or attempt to punish any individual for exercising or attempting to exercise any right or privilege secured by this subsection.

(c) PROHIBITION ON USE OF PERSONAL DATA FOR VOTER SUPPRESSION.—It is unlawful for a person to use personal data in a manner that deprives, defrauds, or attempts to deprive or defraud an individual of the free and fair exercise of the right to vote in a Federal, State, or local election. Intentionally depriving, defrauding, or attempting to deprive or defraud includes—

(1) deception as to—

(A) the times, places, or methods of voting;

(B) eligibility to vote;

(C) counting of ballots;
(D) adjudication of elections;

(E) explicit endorsements by any person of a candidate; or

(F) other material information pertaining to the procedures or requirements for voting or registering to vote in a Federal, state, or local election; or

(2) using deception, threats, intimidation, or coercion to prevent, interfere with, retaliate against, deter, or attempt to prevent, interfere with, retaliate against, or deter—

(A) voting or registering to vote in a Federal, State, or local election; or

(B) giving support or advocacy in a legal manner toward a candidate in a Federal, State, or local election.

(d) DISCRIMINATION AGAINST AN INDIVIDUAL FOR EXERCISE OF RIGHTS.—

(1) IN GENERAL.—It is unlawful for any data aggregator to discriminate against an individual because the individual exercised any of their rights under this title, or did not agree to the use of their personal data for a separate product or service, including by—

(A) denying goods or services;
(B) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(C) providing a different level or quality of goods or services; and

(D) suggesting that an individual will receive a different price or rate for goods or services or a different level or quality of goods or services.

(e) Burden of Proof for Disparate Impact.—If the use of personal data causes a disparate impact on the basis of a protected class under subsection (a) or (b), the data aggregator has the burden of demonstrating that such use of personal data—

(1) is not intentionally discriminatory;

(2) is strictly necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; and

(3) there is no reasonable alternative policy or practice that could serve the interest described in paragraph (2) with a less discriminatory effect.
SEC. 105. ALGORITHMIC ACCOUNTABILITY.

(a) IN GENERAL.—If a data aggregator utilizes automated decision systems, the data aggregator shall perform—

(1) continuous and automated testing for bias on the basis of a protected class; and

(2) continuous and automated testing for disparate impact on the basis of a protected class as required by the Agency.

(b) REQUIREMENT FOR SIMILAR METHODOLOGY.—When evaluating an automated decision system against other less discriminatory alternatives, similar methodology shall be used to create the alternatives.

(c) REPORTING REQUIREMENTS.—For any automated decision system, a data aggregator shall provide the Agency—

(1) an automated decision system risk assessment—

(A) within 90 days for any automated decision system currently in use;

(B) prior to the deployment of any new automated decision system; or

(C) as determined by the Director.

(2) an automated decision system impact evaluation on a periodic basis as determined by the Director, but no less than annually.
(d) Publicly Available.—The Agency shall make automated decision system impact evaluations publicly available.

TITLE II—INDIVIDUAL RIGHTS

SEC. 201. RIGHT TO ACCESS AND PORTABILITY.

Upon receipt of a verifiable request, a data aggregator shall provide the—

(1) specific pieces of personal data that the data aggregator has collected, used, or shared about the individual;

(2) permissible purposes for such collection, use, or sharing of an individual’s personal data at the time of its collection, use, or sharing;

(3) service providers or third parties with which it has shared the personal data; and

(4) individual’s personal data in an electronic, portable, machine-readable, and readily useable format or formats to the individual, or to another person of the individual’s choice.

SEC. 202. RIGHT TO TRANSPARENCY.

A data aggregator shall disclose the following information, including in its online privacy policy:

(1) A description of an individual’s rights under this Act and designated methods for submitting verifiable requests.
(2) A description of the personal data that the data aggregator collects, uses, or shares.

(3) The specific sources from which personal data is collected.

(4) A description of the sources from which personal data is collected.

(5) The permissible purposes for which personal data is collected, used, or shared.

(6) The affiliates, service providers, or third parties with which the data aggregator shares personal data, and the permissible purpose for such sharing.

(7) A description of the length of time for which personal data is retained.

(8) If personal data is collected and retained as anonymized data, a description of the techniques and methods used to create the anonymized data.

SEC. 203. RIGHT TO ACCURACY AND CORRECTION.

(a) IN GENERAL.—A data aggregator shall maintain reasonable policies and procedures to ensure that any personal data that it collects, uses, or shares is accurate.

(b) REQUEST BY INDIVIDUAL.—An individual has the right to require that a data aggregator that retains the individual’s personal data correct any inaccurate or incomplete personal data.
(c) Correction by Data Aggregator.—Upon receipt of a verifiable request, a data aggregator shall correct any inaccurate or incomplete personal data, as directed by that individual, and direct any service provider to correct the individual’s personal data in its records.

SEC. 204. RIGHT TO DELETION.

(a) Request by Individual.—An individual has the right to request that a data aggregator delete any personal data that the data aggregator has collected about the individual.

(b) Deletion by Data Aggregator.—Unless strictly necessary to carry out a permissible purpose under section 102, upon receipt of a verifiable request, a data aggregator shall delete the personal data of such individual, and direct any service providers to delete such individual’s personal data from its records.

SEC. 205. RIGHT TO OBJECT TO CLAIMED PERMISSIBLE PURPOSE.

(a) Request by an Individual.—An individual has the right to object to the claimed permissible purpose for any personal data that a data aggregator has collected, used, or shared of such individual.

(b) Response by Data Aggregator.—Upon receipt of an individual’s verifiable request that objects to the data aggregator’s claimed permissible purpose for col-
lecting, using, or sharing such individual’s personal data, a data aggregator shall produce evidence supporting the data aggregator’s claim that the collection, use, or sharing of such individual’s personal data—

(1) was strictly necessary to carry out a permissible purpose;

(2) was not used or shared for any other purpose; and

(3) has not been retained for any time longer than strictly necessary to carry out a permissible purpose.

SEC. 206. RIGHT TO HUMAN REVIEW OF AUTOMATED DECISIONS.

For any material decision by a data aggregator based on automated processing of personal data of an individual, a data aggregator shall—

(1) inform the individual of the specific personal data that was used for such a decision;

(2) make available an easily available mechanism by which the individual may request human review of such decisions; and

(3) upon receipt of a verifiable request for a human review of a material decision, conduct such a review within 15 days of the date of the request.
SEC. 207. DUTY OF CARE.

(a) IN GENERAL.—A data aggregator shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the personal data and the purposes for which the personal data will be collected, used, or shared, to ensure that personal data—

(1) is only collected, used, or shared where strictly necessary to carry out a permissible purpose under section 102;

(2) is not retained for any time longer than strictly necessary to carry out a permissible purpose under section 102; and

(3) is protected from unauthorized collection, use, sharing, or disclosure.

(b) DUTY OVER SERVICE PROVIDERS.—A data aggregator—

(1) shall ensure that the service providers of the data aggregator comply with the requirements of this Act; and

(2) is liable for any violation of this Act by its service providers.
SEC. 208. DUTIES OF DATA AGGREGATOR UPON RECEIPT OF VERIFIABLE REQUEST.

(a) No Charge.—A data aggregator is prohibited from charging any fee to carry out a verifiable request under this title.

(b) Timing.—A data aggregator shall carry out a verifiable request within 30 days of receiving the verifiable request.

(c) Frivolous or Irrelevant Request.—The requirements of this title shall not apply if the data aggregator receiving a verifiable request determines that the verifiable request is frivolous or irrelevant, including by reason of—

(1) the failure of the individual to provide sufficient information to carry out the verifiable request; or

(2) the verifiable request is substantially the same as a verifiable request previously submitted by the individual, with respect to which the person has already performed the data aggregator’s duties under this title.
TITLE III—DATA ACCOUNTABILITY AND TRANSPARENCY AGENCY

SEC. 301. ESTABLISHMENT OF THE DATA ACCOUNTABILITY AND TRANSPARENCY AGENCY.

(a) AGENCY ESTABLISHED.—There is established in the Executive branch an independent agency to be known as the “Data Accountability and Transparency Agency”, which shall regulate the collection, use, and sharing of personal data.

(b) DIRECTOR AND DEPUTY DIRECTOR.—

(1) IN GENERAL.—There is established a position of the Director of the Data Accountability and Transparency Agency (referred to in this Act as the “Director”), who shall serve as the head of the Agency.

(2) APPOINTMENT.—Subject to paragraph (3), the Director shall be appointed by the President, by and with the advice and consent of the Senate.

(3) 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—

(A) technology;
(B) protection of personal data;
(C) civil rights and liberties;
(D) law;
(E) social sciences; and
(F) business.

(4) COMPENSATION.—

(A) 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.

(B) 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 Accountability and Transparency Agency.”.

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

(A) be appointed by the Director; and

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

(c) TERM.—

(1) IN GENERAL.—The Director shall serve for a term of 5 years.
(2) 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.

(3) Removal for Cause.—The President may remove the Director for inefficiency, neglect of duty, or malfeasance in office.

(d) 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.

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

(f) 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.

SEC. 302. EXECUTIVE AND ADMINISTRATIVE POWERS.

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

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

(3) 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;

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

(5) to adopt and use a seal;

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

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

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

(9) the use and expenditure of funds;

(10) implementing this Act through rules, orders, guidance, interpretations, statements of policy, examinations, and enforcement actions; and

(11) performing such other functions as may be authorized or required by law.
(b) **Delegation of Authority.**—The Director may delegate to any duly authorized employee, representative, or agent any power vested in the Agency by law.

(c) **Office Responsibilities.**—Notwithstanding subsections (a) and (b), section 303(a), and any other provision of law, with respect to the specific functional units and offices described in section 303(b), the Director—

1. shall ensure that such functional units and offices perform the functions, duties, and coordination assigned to them under the applicable provision of section 303; and

2. may not reorganize or rename such units or offices in a manner not provided for under the applicable provisions of section 303.

(d) **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.

SEC. 303. ADMINISTRATION.

(a) PERSONNEL.—

(1) APPOINTMENT.—

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

(B) EMPLOYEES OF THE AGENCY.—The
Director may employ attorneys, compliance ex-
aminers, compliance supervision analysts,
economists, statisticians, and other employees
as may be deemed necessary to conduct the
business of the Agency. Unless otherwise pro-
vided expressly by law, any individual appointed
under this section shall be an employee, as de-
fined in section 2105 of title 5, United States
Code, and subject to the provisions of such title
and other laws generally applicable to the em-
ployees of an Executive agency.

(C) WAIVER AUTHORITY.—

(i) IN GENERAL.—In making any ap-
pointment 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—

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

(II) fair and open competition and equitable treatment in the consideration and selection of individuals to positions; and

(III) 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’ pref-
ference 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.

(D) Duty to provide adequate staffing.—The Director shall ensure that the specific functional units and offices established under section 303, 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.

(E) 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 subpara-
graph, the term "political appointee" means an employee who holds—

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

(II) 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

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

(2) 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:

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

(C) 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)).

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

(b) SPECIFIC FUNCTIONAL UNITS.—

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

(A) providing oversight and enforcement of this Act to ensure that the collection, use, and sharing of personal data is fair, equitable, and nondiscriminatory;
(B) 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;

(C) working with civil rights, privacy organizations, and industry on the promotion of compliance with the civil rights compliance under this Act;

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

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

(2) RESEARCH.—The Director shall establish a unit whose functions shall include researching, analyzing, and reporting relating to the collection and use of personal data, including use of automated decision systems.

(3) COLLECTING AND TRACKING COMPLAINTS.—

(A) IN GENERAL.—

(i) ESTABLISHMENT OF UNIT.—The Director shall establish a unit, the functions of which shall include 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, use, and sharing of personal data.

(ii) **Website Requirements.**—The Director shall ensure that—

(I) 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

(II) 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 lan-
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.

(B) Public availability of information.—

(i) In general.—The Director shall—

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

(II) 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

(III) 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.

SEC. 304. COORDINATION.

The Agency shall coordinate with the Consumer Financial Protection Bureau, the Federal Trade Commission, the Department of Health and Human Services, the Department of Education, and other Federal agencies and State regulators, as appropriate, to promote consistent regulatory treatment of personal data.

SEC. 305. APPEARANCES BEFORE AND REPORTS TO CONGRESS.

(a) APPEARANCES BEFORE CONGRESS.—The Director of the Agency shall appear before the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives at semi-annual hearings regarding the reports required under subsection (b).

(b) REPORTS REQUIRED.—The Agency shall, concurrent with each semi-annual hearing referred to in subsection (a), prepare and submit to the President and to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives, a report, beginning with the session following the designated transfer date.
(c) CONTENTS.—The reports required by subsection (b) shall include—

(1) a discussion of the significant problems faced by individuals in exercising their rights under this Act;

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

(3) 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;

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

(5) 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;

(6) the actions taken regarding rules, orders, and supervisory actions with respect to data aggregators;
(7) an assessment of significant actions by State attorneys general or State regulators relating to this Act or other Federal privacy laws;

(8) an analysis of the efforts of the Agency to fulfill the civil rights in data mission of the Agency; and

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

SEC. 306. FUNDING; PENALTIES AND FINES.

(a) Funding.—

(1) Assessments, fees, charges.—

(A) 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.

(B) 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.
(2) 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).

(b) Data Accountability and Transparency Agency Fund.—

(1) Separate fund in Federal Reserve established.—There is established in the Federal Reserve a separate fund, to be known as the “Data Accountability and Transparency 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.

(2) Fund receipts.—All amounts transferred to the Agency under subsection (a) shall be deposited into the Agency Fund.

(3) Investment authority.—

(A) 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.

(B) ELIGIBLE INVESTMENTS.—Invest-
ments authorized by this paragraph shall be
made in obligations of the United States or ob-
ligations that are guaranteed as to principal
and interest by the United States, with matur-
ities suitable to the needs of the Agency Fund,
as determined by the Agency.

(C) INTEREST AND PROCEEDS CRED-
ITED.—The interest on, and the proceeds from
the sale or redemption of, any obligations held
in the Agency Fund shall be credited to the
Agency Fund.

(c) USE OF FUNDS.—

(1) IN GENERAL.—Funds obtained by, trans-
ferred 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 com-
pensation 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.
(2) 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.

(3) 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.

(d) Penalties and fines.—

(1) 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.
(2) 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.

SEC. 307. PURPOSE, OBJECTIVES, AND FUNCTIONS.

(a) Purpose.—The Agency shall seek to protect individuals’ privacy and enforce this Act’s limitations on the collection, use, and sharing of personal data and other Federal privacy law, and is authorized to exercise its authorities under this Act for such purposes.

(b) Objectives.—The Agency is authorized to exercise its authorities under this Act for the following purposes:

(1) Protect individuals from violations of this Act or other Federal privacy laws or unfair, deceptive, abusive, or discriminatory data practices.

(2) Ensure that Federal privacy law is enforced consistently and in order to protect individuals and ensure fair competition.

(c) Functions.—The primary functions of the Agency are—

(1) 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;

(2) 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, data protection rights and standards, and fair information practices and principles;

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

(4) requiring and overseeing ex-ante impact assessments and ex-post outcomes audits of high-risk data practices by covered entities to advance fair and just data practices;

(5) examining the social, ethical, economic, and civil rights impacts of high-risk data practices and propose remedies;
(6) ensuring that data privacy practices are fair, just, and nondiscriminatory, and comply with fair information practices;
(7) collecting, researching, and responding to complaints;
(8) developing model privacy, data protection, and fair information practices, standards, guidelines, policies, and routine uses for use by the private sector;
(9) issuing rules, orders, and guidance implementing this Act; and
(10) enforcing other privacy statutes and rules as authorized by Congress.

SEC. 308. RULEMAKING AUTHORITY.

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

(b) RULEMAKING, ORDERS, AND GUIDANCE. —

(1) 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 to prevent evasions of this Act.
(2) REGULATIONS.—The Agency may 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.

(3) STANDARDS FOR RULEMAKING.—In prescribing a rule under this Act—

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

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

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

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

(5) 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 reasonable or permissible interpretation of this Act.
(c) MONITORING.—In order to support its rule-making and other functions, the Agency shall monitor for risks to individuals or groups of individuals in the collection, use, or sharing of personal data.

SEC. 309. SUPERVISION OF DATA AGGREGATORS.

(a) IN GENERAL.—This section shall apply to any 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 data aggregators described in paragraph (1) for purposes of—

(1) assessing compliance with the requirements of this Act 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
requiring and overseeing ex-ante impact assessments and ex-post outcome audits of automated decision systems to advance fair and just data practices.

SEC. 310. SPECIFIC AGENCY AUTHORITIES.

(a) Prohibiting Unfair, Deceptive, or Abusive Acts and Practices.—

(1) In General.—The Agency may take any action authorized under this Act to prevent a data aggregator or service provider from committing or engaging in any unfair, deceptive, or abusive act or practice in connection with the collection, use, or sharing of personal data.

(2) Rulemaking.—The Agency may prescribe rules applicable to a data aggregator identifying unlawful, unfair, deceptive, or abusive acts or practices in connection with the collection, use, or sharing of personal data, which may include requirements for the purpose of preventing such acts or practices. Rules under this section shall not limit, or be interpreted to limit, the scope of unlawful, deceptive, or abusive acts or practices in connection with the collection, use, or sharing of personal data.

(3) Unfairness.—
(A) IN GENERAL.—The Agency may declare an act or practice in connection with the collection, use, or sharing of personal data to be unlawful on the grounds that such act or practice is unfair if the Agency has a reasonable basis to conclude that—

(i) the act or practice causes or is likely to cause privacy harm or other substantial injury to individuals which is not reasonably avoidable by individuals; and

(ii) such privacy harm or substantial injury is not outweighed by countervailing benefits to individuals or to competition.

(B) CONSIDERATION OF PUBLIC POLICIES.—In determining whether an act or practice is unfair, the Agency may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

(4) ABUSIVE.—The Agency may declare an act or practice abusive in connection with the collection, use, or sharing of personal data if the act or practice—
(A) materially interferes with the ability of an individual to understand a term of condition of a good or service; or

(B) takes unreasonable advantage of—

(i) a lack of understanding on the part of the individual of the material risks, costs, or conditions of the product or service;

(ii) the inability of the individual to protect their interests in selecting or using a product or service; or

(iii) the reasonable reliance by the individual on a data aggregator or service provider to act in the interests of the individual.

(b) DATABASE.—The Agency shall create and maintain a publicly available database through which—

(1) data aggregators report the types of personal data that those data aggregators collect, use, or share; and

(2) an individual may exercise rights, including rights under title II, with respect to the personal data of the individual.

(c) PUBLICLY ACCESSIBLE LIST.—The Agency shall maintain a publicly accessible list of data aggregators that
collect, use, 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.

(d) LIMITATION ON LINES OF BUSINESS.—The Agency shall—

(1) limit or require the divestment of any lines of business in which any data aggregator participates based on antitrust or competition concerns; and

(2) have the authority to review and approve any merger between a data aggregator and any other company.

SEC. 311. PROHIBITED ACTS.

It shall be unlawful for—

(1) any data aggregator or service provider—

(A) to commit any act or omission in violation of this Act or Federal privacy law; or

(B) to engage in any unfair, deceptive, or abusive act or practice relating to personal data;

(2) 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; or

(3) 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.

SEC. 312. ENFORCEMENT POWERS.

(a) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

(1) 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 this section.

(2) 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 any
other Federal privacy law.

(3) Custodian.—The term “custodian” means
the custodian or any deputy custodian designated by
the Agency.

(4) Documentary Material.—The term
“documentary material” includes the original or any
copy of any book, document, record, report, memo-
randum, paper, communication, tabulation, chart,
logs, electronic files, or other data or data compil-
ations stored in any medium.

(5) Violation.—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.

(b) Investigations and Administrative Dis-
covery.—

(1) Joint Investigations.—

(A) In General.—The Agency or, where
appropriate, an Agency investigator, may en-
gage in joint investigations and requests for in-
formation, as authorized under this Act.

(B) 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.

(2) _Subpoenas._—

(A) **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.

(B) **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 appear
and give testimony or to appear and produce
documents or other material.

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

(3) DEMANDS.—

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

(i) produce such documentary mate-
rial for inspection and copying or repro-
duction 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.

(B) REQUIREMENTS.—Each civil investiga-
tive demand shall state the nature of the con-
duct constituting the alleged violation which is
under investigation and the provision of law ap-
plicable to such violation.

(C) 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 de-
manded may be assembled and made avail-
able for inspection and copying or repro-
duction; and

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

(E) 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.
(F) 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.

(G) 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—

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

(II) 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.

(H) 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.

(I) 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.

(J) 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 hav-
ing 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.

(K) 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.

(L) 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.

(M) TESTIMONY.—

(i) IN GENERAL.—

(I) 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.

(II) TRANSCRIPTION.—The testi-
mony shall be taken stenographically
and transcribed.

(III) TRANSMISSION TO CUSTO-
dian.—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 cus-
todian.

(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 representative
of an agency with which the Agency is en-
gaged in a joint investigation, and any ste-
nographer 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.—

(I) 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.

(II) AUTHORITY.—The attorney may advise a person described in sub-clause (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.
(III) 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.

(IV) 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—

(I) after the testimony of any
witness is fully transcribed, the Agen-
cy investigator shall afford the witness
(who may be accompanied by an at-
torney) a reasonable opportunity to
examine the transcript;

(II) the transcript shall be read
to or by the witness, unless such ex-
amination and reading are waived by
the witness;

(III) any changes in form or sub-
stance which the witness desires to
make shall be entered and identified
upon the transcript by the Agency in-
vestigator, with a statement of the
reasons given by the witness for mak-
ing such changes;

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

(V) if the transcript is not signed
by the witness during the 30-day pe-
riod 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, to-
gether 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 in-
vestigator 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.

(4) CONFIDENTIAL TREATMENT OF DEMAND MATERIAL.—

(A) 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.
(B) 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.

(5) Petition for Enforcement.—

(A) 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.

(B) 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.

(6) Petition for order modifying or setting aside demand.—

(A) 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.

(B) 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.

(C) 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.

(7) 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.

(8) JURISDICTION OF COURT.—

(A) 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.

(B) 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.

(c) Hearings and Adjudicatory Proceedings.—

(1) 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—

(A) the provisions of this Act, including any rules prescribed by the Agency under this Act; and

(B) any other Federal privacy law that the Agency is authorized to enforce, and any regulations 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.
(2) Special rules for cease-and-desist proceedings.—

(A) 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.

(B) 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.

(C) 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 sub-
section. Unless a petition for review is timely
filed in a court of appeals of the United States,
as provided in subparagraph (D), and there-
after 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.

(D) APPEAL TO COURT OF APPEALS.—Any
party to any proceeding under this subsection
may obtain a review of any order served pursu-
ant to this subparagraph (other than an order
issued with the consent of the person con-
cerned) 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 there-
upon 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.

(E) NO STAY.—The commencement of pro-
ceedings 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.

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

(B) 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.

(C) 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—

(I) 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

(II) 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)—

(I) shall become effective upon service; and
(II) 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.

(4) Special rules for enforcement of orders.—

(A) 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 jurisdic-
tion and power to order and require compliance herewith.

(B) 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.

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

(d) LITIGATION AUTHORITY.—

(1) IN GENERAL.—If any person violates this Act, 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.

(2) 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.
(3) COMPROMISE OF ACTIONS.—The Agency may compromise or settle any action if such compromise is approved by the court.

(4) NOTICE TO THE ATTORNEY GENERAL.—

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

(B) NOTICE AND COORDINATION.—

(i) NOTICE OF OTHER ACTIONS.—In addition to any notice required under subparagraph (A), the Agency shall notify the Attorney General 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 provi-
sions to ensure that parallel investigations and proceedings involving the Federal pri-
vacy laws are conducted in a manner that avoids conflicts and does not impede the ability of the Attorney General to prose-
ceute 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 inter-
pret Federal privacy law.

(5) 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 certio-
rari, and the Attorney General concurs with such re-
quest or fails to take action within 60 days of the request of the Agency.

(6) Forum.—Any civil action brought under this Act 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 re-
quire compliance with any Federal privacy law.

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

(e) RELIEF AVAILABLE.—

(1) ADMINISTRATIVE PROCEEDINGS OR COURT
ACTIONS.—

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

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

(i) rescission or reformation of con-
tracts;
(ii) refund of moneys or return of real
property;

(iii) restitution;

(iv) disgorgement or compensation for
unjust enrichment;

(v) payment of damages or other mon-
etary relief;

(vi) public notification regarding the
violation, including the costs of notifica-
tion;

(vii) limits on the activities or func-
tions of the person; and

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

(C) NO EXEMPLARY OR PUNITIVE DAM-
AGES.—Nothing in this subparagraph shall be
construed as authorizing the imposition of ex-
emplary or punitive damages in an action
brought by the Agency.

(2) RECOVERY OF COSTS.—In any action
brought by the Agency, a State attorney general, or
any State regulator to enforce this Act or any Fed-
eral privacy law, the Agency, the State attorney gen-
eral, or the State regulator may recover its costs in
connection with prosecuting such action if the Agen-
cy, the State attorney general, or the State regulator is the prevailing party in the action.

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

(A) **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.

(B) **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 $5,000 for each day during which such violation or failure to pay continues.

(ii) **SECOND TIER.**—Notwithstanding clause (i), for any person that recklessly engages in a violation of a this Act or any Federal privacy law, a civil penalty may not exceed $25,000 for each day during which such violation continues.

(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 $1,000,000 for each day during which such violation continues.

(C) 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).

(D) 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 the individual;

(iv) the history of previous violations;

and

(v) such other matters as justice may require.

(E) AUTHORITY TO MODIFY OR REMIT PENALTY.—The Agency may compromise, modi-
ify, or remit any penalty which may be assessed
or had already been assessed under subpara-
graph (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.

(F) NOTICE AND HEARING.—No civil pen-
alty 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 op-
portunity for a hearing to the person ac-
cused of the violation; or

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

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

**TITLE IV—CIVIL LIABILITY**

**SEC. 401. PRIVATE RIGHT OF ACTION.**

(a) **IN GENERAL.**—Any person may commence a civil action—

(1) against any person, including the United States or any other governmental instrumentality or agency to the extent permitted by the Eleventh Amendment to the Constitution of the United States, that is alleged to have violated this Act; or

(2) against the Agency if the Agency is alleged to have—

(A) adopted a rule in violation of—

(i) any provision of chapter 5 of title 5, United States Code; or

(ii) any provision of this title; or

(B) failed to promulgate a rule required under this title, in order compel the issuance of such rule.

(b) **JURISDICTION.**—The district courts of the United States shall have jurisdiction, without regard to the amount in controversy or the citizenship of the parties.
(c) RELIEF.—In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award—

(1) an amount not less than $100 and not greater than $1,000 per violation per day or actual damages, whichever is greater;

(2) punitive damages;

(3) reasonable attorney’s fees and litigation costs; and

(4) any other relief, including a temporary or permanent injunction, equitable, or declaratory relief, that the court determines appropriate.

(d) INJURY IN FACT.—A violation of this Act or a regulation promulgated under this Act with respect to the personal data of an individual is presumed to cause privacy harm and constitutes a concrete and particularized injury in fact to that individual.

(e) TIME FOR BRINGING AN ACTION.—Except as otherwise permitted by law or equity, no individual may bring an action under this Act more than 5 years after the date of discovery of the violation to which an action relates.
SEC. 402. INVALIDITY OF PRE-DISPUTE ARBITRATION AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIVERS.

(a) In General.—Notwithstanding any other provision of law, no pre-dispute arbitration agreement or pre-dispute joint action waiver shall be valid or enforceable with respect to a dispute regarding a violation of this Act or regulations promulgated by the Agency.

(b) Applicability.—Any determination as to whether or how this subsection applies to any dispute regarding a violation of this Act or regulations promulgated by the Agency shall be made by a court, rather than an arbitrator, without regard to whether such agreement purports to delegate such determination to an arbitrator.

(c) Definitions.—For purposes of this section:

(1) The term “pre-dispute arbitration agreement” means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

(2) The term “pre-dispute joint-action waiver” means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit, or waive the right of, one of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other
forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.

SEC. 403. PROHIBITION ON WAIVER.

No provisions of this Act may be waived and any agreement to waive compliance with or modify any provision of the Act shall be void as contrary to public policy.

TITLE V—CORPORATE ACCOUNTABILITY

SEC. 501. REPORTING AND CERTIFICATION.

(a) IN GENERAL.—Each data aggregator shall establish comprehensive privacy and data security policies, procedures, and practices to ensure compliance with this Act.

(b) ANNUAL REPORT.—Each data aggregator shall submit to the Agency an annual report—

(1) describing its collection, use, or sharing of personal data, and the permissible purposes for such collection, use, or sharing of personal data;

(2) identifying each service provider with which the data aggregator shares personal data, the permissible purposes for sharing personal data with each such service provider, and a description of the oversight and supervision conducted by the data aggregator to ensure that each such service provider complies with the requirements of this Act;
(3) internal controls that the data aggregator has put in place to ensure compliance with the requirements of this Act; and

(4) a description of the testing, and results of such testing, to ensure compliance with the requirements of this Act.

(c) EXECUTIVE CERTIFICATION.—The chief executive officer or, if the data aggregator does not have a chief executive officer, the highest ranking officer of the data aggregator, shall annually certify to the Agency that it has complied with this Act, including—

(1) conducted oversight sufficient to demonstrate all service providers are complying with this Act;

(2) maintains adequate internal controls sufficient to demonstrate compliance with this Act;

(3) conducted testing sufficient to demonstrate compliance with this Act; and

(4) maintains reporting structures to ensure that the chief executive officer (or, if the data aggregator does not have a chief executive officer, the highest ranking officer of the data aggregator) is involved in, and responsible for, decisions to ensure compliance with this Act.
(d) CRIMINAL AND CIVIL PENALTIES FOR CEO AND BOARD OF DIRECTORS.—

(1) CRIMINAL PENALTY.—

(A) IN GENERAL.—Whoever knowingly and intentionally violates, or knowingly and intentionally attempts to violate, this section shall be fined in accordance with title 18, United States Code, or imprisoned for not more than 5 years, or both.

(B) ENHANCED PENALTY FOR AGGRAVATED CASES.—Whoever violates, or attempts to violate, this section while violating another law of the United States or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period shall be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of title 18, United States Code, imprisoned for not more than 10 years, or both.

(2) CIVIL FINE.—Whoever violates this section shall be liable to the United States for a civil fine of not more than $10,000,000.

SEC. 502. WHISTLEBLOWER PROTECTIONS.

(a) IN GENERAL.—A data aggregator may not, directly or indirectly, discharge, threaten, harass, suspend,
demote, terminate, or in any other manner discriminate against a covered individual because—

(1) the covered individual, or anyone perceived as assisting the covered individual, takes (or the data aggregator suspects that the covered individual has taken or will take) a lawful action in providing to the Federal Government or the attorney general of a State information relating to any act or omission that the covered individual reasonably believes to be a violation of this Act or any regulation promulgated under this Act;

(2) the covered individual provides information that the covered individual reasonably believes evidences such a violation to—

(A) a person with supervisory authority over the covered individual at the covered entity; or

(B) another individual working for the covered entity who the covered individual reasonably believes has the authority to investigate, discover, or terminate the violation or to take any other action to address the violation;

(3) the covered individual testifies (or the covered entity expects that the covered individual will
(105)

1. testify) in an investigation or judicial or administrative proceeding concerning such a violation;

2. (4) the covered individual assists or participates
3. (or the covered entity expects that the covered individual will assist or participate) in such an investigation or judicial or administrative proceeding; or

4. (5) takes any other action to assist in carrying
5. out the purposes of this section.

(b) ENFORCEMENT.—An individual who alleges discharge or other discrimination in violation of subsection
6. (a) may bring an action governed by the rules, procedures,
7. statute of limitations, and legal burdens of proof in section
8. 42121(b) of title 49, United States Code. If the individual
9. has not received a decision within 180 days and there is
10. no showing that such delay is due to the bad faith of the
11. claimant, the individual may bring an action for a jury
12. trial, governed by the burden of proof in section 42121(b)
13. of title 49, United States Code, in the appropriate district
14. court of the United States for the following relief:

15. (1) Temporary relief while the case is pending.

16. (2) Reinstatement with the same seniority status that the individual would have had, but for the
17. discharge or discrimination.

18. (3) Three times the amount of back pay otherwise owed to the individual, with interest.
(4) Consequential and compensatory damages, and compensation for litigation costs, expert witness fees, and reasonable attorneys’ fees.

c) Waiver of Rights and Remedies.—The rights and remedies provided for in this section shall not be waived by any policy form or condition of employment, including by a predispute arbitration agreement.

d) Predispute Arbitration Agreements.—No predispute arbitration agreement shall be valid or enforceable if the agreement requires arbitration of a dispute arising under this section.

e) Definition.—In this section, the term “covered individual” means an applicant, current or former employee, contractor, subcontractor, grantee, or agent of a data aggregator or service provider.

TITLE VI—RELATION TO FEDERAL AND STATE LAW

SEC. 601. RELATION TO FEDERAL LAW.

The Agency shall have concurrent enforcement authority with other Federal agencies to enforce Federal privacy laws.

SEC. 602. RELATION TO STATE LAW.

(a) In General.—Nothing in this Act, nor any amendment, standard, rule, requirement, or standard of performance, shall be construed to preempt, displace, or
supplant any State or Federal common law or statute, except to the extent that any such provision of law specifically and directly conflicts with the provisions of this Act, and then only to the extent of the specific and direct conflict.

(b) GREATER PROTECTION UNDER STATE LAW.—For purposes of this subsection, a statute, regulation, order, or interpretation in effect in any State is not in specific and direct conflict with the provisions of this Act if the protection that such statute, regulation, order, or interpretation affords to persons is greater than the protection provided under this Act.

(e) STATE REGULATION WHEN ACT IS SILENT.—Nothing in this Act shall be construed or interpreted as limiting the right of any State to regulate any person, personal data, right, or obligation covered by this Act or any rule, regulation or standard under this Act if any such State regulation is not covered by or is exempted from this Act, or any final agency regulation issued under this Act.

(d) REMEDIES PRESERVED.—Notwithstanding any other provision of this Act, nothing in this Act, nor any nor any amendment, standard, rule, requirement, assessment, shall preempt, displace, or supplant any Federal or State common law or statutory rights and remedies, in-
excluding any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any State law, Federal common law, or statutory law.

SEC. 603. PRESERVATION OF ENFORCEMENT POWERS OF STATES.

(a) IN GENERAL.—

(1) ACTION BY STATE.—

(A) STATE ATTORNEY GENERAL.—Except as provided in paragraph (2), 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 regulations issued under this Act, and to secure remedies under provisions of this Act or remedies otherwise provided under other law.

(B) STATE REGULATOR.—A State regulator may bring a civil action or other appro-
appropriate proceeding to enforce the provisions of
this Act or regulations issued under this Act
with respect to any entity that is State-char-
tered, incorporated, licensed, or otherwise au-
thorized to do business under State law (except
as provided in paragraph (2)), and to secure
remedies under provisions of this Act or rem-
edies otherwise provided under other provisions
of law with respect to such an entity.

(2) Rule of Construction.—No provision of
this Act may be construed as modifying, limiting, or
superseding the operation of any provision of a Fed-
eral privacy law that relates to the authority of a
State attorney general or State regulator to enforce
that Federal privacy law.

(b) Consultation Required.—

(1) Notice.—

(A) In general.—Before initiating any
action in a court, or any other administrative or
regulatory proceeding, against a data
aggregator or service provider, as authorized
under subsection (a), to enforce any provision
of this Act, including any regulation prescribed
by the Agency under this Act, a State attorney
general or State regulator shall timely provide
to the Agency a copy of the complete complaint
to be filed and written notice describing the ac-
tion or proceeding.

(B) Emergency Action.—If providing
the notice required under subparagraph (A) is
not practicable, the State attorney general or
State regulator, as applicable, shall provide to
the Agency immediately upon instituting the ac-
tion or proceeding.

(C) Contents of Notice.—The notifica-
tion required under this paragraph shall, at a
minimum, describe—

(i) the identity of the parties;

(ii) the alleged facts underlying the
proceeding; and

(iii) whether there may be a need to
coordinate the prosecution of the pro-
ceeding so as not to interfere with any ac-
tion, including any rulemaking, undertaken
by the Agency.

(2) Agency Response.—In any action de-
scribed in paragraph (1), the Agency may—

(A) intervene in the action as a party;

(B) upon intervening—
(i) remove the action to the appropriate United States district court, if the action was not originally brought there; and

(ii) be heard on all matters arising in the action; and

(C) appeal any order or judgment, to the same extent as any other party in the proceeding may.

(c) REGULATIONS.—The Agency shall prescribe regulations to implement the requirements of this section and, from time to time, provide guidance in order to further coordinate actions with the State attorneys general and other regulators.

(d) PRESERVATION OF STATE AUTHORITY.—No provision of this section may 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.

SEC. 604. SAVINGS.

Nothing in this Act may be construed to prohibit compliance with otherwise valid and constitutional legal process.