Title: To provide individuals with foundational information privacy rights, create strong accountability mechanisms, and establish meaningful enforcement.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the "Information Privacy Act".

(b) Table of Contents.—The table of contents of this Act is as follows:

SEC. 2. LEGISLATIVE FINDINGS AND PURPOSE.

(a) Findings.—The Congress finds the following—

(1) The right to privacy is a personal and fundamental right protected by the Constitution of the United States.

(2) Americans cherish privacy as an essential element of their personal and social lives, and our system of self-government. It serves essential human needs by sheltering zones for individual liberty, autonomy, seclusion, and self-definition, including the exercise of free expression; for family life, intimacy and other relationships; and for physical and moral space and security, among other values.

(3) Privacy also advances societal interests in the protection of marginalized or vulnerable individuals or groups, the safeguarding of foundational values of democracy, and the integrity of democratic institutions and processes including elections.

(4) The United States has protected aspects of privacy since the Nation’s founding. The Constitution protects various privacy interests through the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, and protection of individual privacy helps enable the exercise of these fundamental civil rights and fundamental freedoms of all Americans.

(5) The United States has a history of leadership in privacy rights since that time. It enacted some of the first privacy laws anywhere beginning in the 18th century, it gave birth to the legal concept of a “right to privacy” in the 19th century and, in the 20th century, it adopted one of the first national privacy and data protection laws as well as “fair

information practice principles" that influenced laws and privacy practices worldwide. The United States should continue to be a leader in protecting privacy rights in the 21st century.

(6) The right to privacy is widely recognized in international legal instruments that the United States has endorsed, ratified, or promoted.

(7) Throughout the Nation's history, economic growth, opportunity, and leadership have been propelled by technological innovations. In the 20th century, digital and communications technologies and networks have become integral to economic competitiveness, social and political discourse, and the flow of information, ideas, and innovation in the United States and around the world.

(8) The expansion of computers, Internet connectivity, mobile telephones, and other digital information and communications technology has magnified the risks to individuals' privacy that can occur from collection, processing, storage, or dissemination of personal information.

(9) Digital network connectivity has become essential for full engagement in modern life.

(10) As of 2019, more than 90 percent of Americans possess mobile telephones and approximately 80 percent own smartphones equipped with powerful computers, immense storage capacity, arrays of sensors, and the capacity to transmit information around the globe instantaneously. Many individuals use these devices continuously and store on them a digital record of nearly every aspect of their lives.

(11) An increasing number of individuals have smart consumer devices such as automobiles, televisions, home appliances, and wearable accessories that collect, process, and transmit information linked to these individuals and their activities.

(12) In addition to these personal devices, a growing number of interconnected sensors in public spaces collect, process, and transmit personal information linked or linkable to individuals, often without their knowledge or control. The number of such devices is likely to expand faster with increased deployment of smart public and private infrastructure and systems and advances in network technology.

(13) These ubiquitous and always-connected devices have exploded the volume and variety of personal information collected, stored, and analyzed by a wide variety of entities. Such information is often available not only to service providers with which the individuals affected have some relationship, but also to networks of applications providers, websites, advertisers, data brokers, and additional parties that are able to collect, process, and transmit the information for purposes that may be unexpected and unrelated to the reason for which this information originally was shared or collected.

(14) The aggregation of personal information from many different sources across these networks, coupled with the increasing power of data science, enables a wide variety of entities to make connections, inferences, or predictions regarding individuals with levels of

power and granularity far beyond what individuals linked to this information reasonably know or expect. These include the ability to link information to specific individuals even in the absence of explicit identifying information, and to derive conclusions about individuals that are sensitive to a reasonable person.

(15) Surveys demonstrate that most individuals do not read or understand published privacy policies.

(16) Even if they do, the increased velocity, complexity, and opacity of data collection, aggregation, and use have rendered individual control or consent a futile exercise.

(17) Numerous surveys of consumer attitudes on privacy and security also indicate that a majority of Americans lack confidence in industry to handle personal information and keep it secure, and also believe they lack control and knowledge of information collected about them.

(18) Some use of personal information in advertising and marketing provides benefits to businesses and consumers by disseminating information about products, services, and public issues; supporting the delivery of news and other content; and enabling free services. However, increases in precise targeting of individuals and automated advertising exchanges have enabled sharing of personal information for advertising that can be unwanted, intrusive, manipulative, discriminatory, or unfair.

(19) With the development of artificial intelligence and machine learning, the potential to use personal information in ways that replicate existing societal biases has increased in scale. Algorithms use personal information to guide decisionmaking related to critical issues—such as credit determination, housing advertisements, and hiring processes—and can result in differing accuracy rates among demographic groups. Such outcomes may violate federal and state anti-discrimination laws or result in diminished opportunities for members of some groups. The covered entities that use these algorithms should have the responsibility to show that the algorithms do not cause discriminatory effects.

(20) The majority of Americans have experienced losses of personal information linked to them due to data breaches that have occurred at numerous businesses and institutions. Personal information increasingly is a target of malicious actors, including nation-states and organized criminals anywhere in the world.

(21) The aggregation of increasing volumes of data among many different entities expands the attack surface exposed to malicious actors in cyberspace and the availability of personal information to such actors.

(22) The risks of harm from privacy violations are significant. Unwanted or unexpected disclosure of personal information and loss of privacy can have devastating effects for individuals, including financial fraud and loss, identity theft and the resulting loss of personal time and money, destruction of property, harassment, and even potential physical

injury. Other effects such as reputational or emotional damage can be equally or even more substantial.

(23) Individuals need to feel confident that data that relates to them will not be used or shared in ways that harm themselves, their families, or society.

(24) As with all forms of commerce, trust is an essential element for broad consumer use and acceptance of goods and services offered in the digital economy, and a growing lack of trust in online services harms the interstate and foreign commerce of the United States. Trust is also important to social and political discourse, and a growing lack of trust in online communications impairs American democracy and society.

(25) As enterprises use technology to collect, retain, and process more and more personal information, laws and regulations protecting individual privacy must keep pace to protect users and businesses and sustain the Nation's digital economy and society.

(26) Current laws and regulations governing the use of personal information do not sufficiently protect individual privacy because they do not cover many new and expanding types of information and uses of such information.

(27) In addition, they rely substantially on "notice and choice" for individuals. This places the burden of protecting privacy on individuals instead of on the companies that use and collect data, and permits the companies to set the boundaries for what information they collect and how they use or share it, with little meaningful understanding on the part of the individuals whose data is collected.

(28) Entities that collect, use, process, and share personal information should be subject to meaningful and effective boundaries on such activities. They should be obligated to take reasonable steps to protect the privacy and security of personal information, and to act with loyalty and care toward individuals linked or linkable to such information.

(29) Privacy risk and harms must be mitigated and addressed up front, because in the digital era, data harms are often unforeseen and compounded almost instantaneously. Information leakage usually cannot be undone, and it is often difficult to make victims of privacy harms whole after the fact.

(30) There is a need for a national solution to ensure that entities that collect, process, and transmit personal information do so in ways that respect the privacy interests of individuals linked or linkable to that information and do not cause harm to these individuals or their families and communities.

(31) States have a patchwork of differing laws and jurisprudence relating to the privacy of their citizens. A robust and comprehensive federal privacy law will ensure that all Americans have the benefit of the same privacy protections regardless of where they live and can rely on the entities they deal with to handle personal information consistently regardless of where these entities are located.

(32) The need for consistent federal privacy protection is heightened by the interstate and global nature of the information economy in which few online products and services are targeted toward specific states. Instead, many such services are offered to users anywhere in the United States (and often around the world) who can access the Internet. Consistent federal privacy protection will facilitate entry and competition in interstate commerce for millions of small businesses for which compliance with multiple state laws could present barriers to entry.

(33) Consistent and robust data security practices will enhance the privacy of individuals as well as the collective security of U.S. information and communications networks.

(34) Privacy laws must be backed by strong enforcement agencies and tools. To provide such enforcement, the Federal Trade Commission needs adequate resources and legal authority at least equal to that of other leading privacy regulators, reinforced by authorized state officials.

(35) Individuals should have recourse through the federal courts for privacy harms that have been commonly compensable under existing laws, including anti-discrimination laws, as well as violations of federal privacy law that cause "actual" harm.

(36) Technology will continue to evolve and change. Any new privacy laws therefore must be flexible and technology-neutral, so that the laws' protections may apply not only to the technologies and products of today, but to those of tomorrow.

(37) A comprehensive federal privacy law will enable the United States to take steps toward ensuring that Americans' privacy is appropriately protected internationally, while increasing the flow of information and promoting greater trust in American commerce abroad.

(b) Policy.—The Congress declares the following—

(1) In order to protect the privacy of individuals, it is necessary and proper for Congress to regulate the collection, use, processing, and sharing of personal information.

(2) There is a compelling national interest in providing meaningful and effective boundaries on the collection, use, storage, and sharing of personal information so all individuals linked or linkable to such information have a basis to trust that such information will be handled in ways consistent with their privacy and other interests.

(3) There is a compelling national interest in empowering individuals through meaningful and effective rights with respect to personal information linked to them so that those individuals who want to can ensure this information is used and shared in ways consistent with their privacy and other interests.

(4) It is the policy of the United States to provide a consistent national approach to the collection, processing, storage, and sharing of personal information, but also to preserve the

existing fabric of state and local statutory and common law protecting privacy to the extent it does not interfere with the comprehensive operation of federal law.

(5) It is the policy of the United States to provide individuals with meaningful remedies for privacy harms, whether those harms are financial, physical, reputational, emotional, or other kinds; and to ensure that an exclusive federal remedy for violation of privacy rights vindicates interests that have long been protected by other privacy laws.

(6) It is the policy of the United States to ensure that protections for users' privacy can remain up-to-date, and continue to evolve as technology, innovation, and services—and risks to privacy—evolve.

SEC. 3. DEFINITIONS.

In this Act:

(1) Affirmative express consent.—The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's authorization for certain collection, processing, or transfer practices in response to a specific and unambiguous request that meets the requirements of sections 102(c) and 104.

(2) Algorithmic decision-making.—The term "algorithmic decision-making" means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that uses covered data to make a decision or provide significant support for human decision-making.

(3) Biometric information.—

(A) In general.—The term "biometric information" means any covered data generated from the measurement or specific technological processing of an individual's biological, physical, or physiological characteristics, including—

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina scans;

(iv) facial scans or templates;

(v) deoxyribonucleic acid (DNA) information;

(vi) gait, or any other identifiable physical movement characteristics used for the purpose of identifying an individual; and

(vii) other physical attributes of an individual used to identify the individual.

(B) Exclusions.—Such term does not include writing samples, written signatures, photographs, voice recordings, demographic data, or physical characteristics such as height, weight, hair color, or eye color, provided that such data is not used for the

purpose of identifying an individual's unique biological, physical, or physiological characteristics.

(4) Collect; collection.—The terms "collect" and "collection" mean acquiring covered data by any means, including buying, renting, gathering, obtaining, receiving, accessing, or observing individual behavior.

(5) Common branding.—The term "common branding" means a shared name, servicemark, or trademark between two or more entities.

(6) Control.—The term "control" means, with respect to an entity—

(A) ownership of, or the power to vote, more than 50 percent of the outstanding shares of voting securities of the entity;

(B) control in any manner over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

(C) the power to exercise a controlling influence over the management of the entity.

(7) Commission.—The term "Commission" means the Federal Trade Commission.

(8) Covered data.—

(A) In general.—The term "covered data" means information that identifies, or is linked or reasonably linkable to an individual, household, or device used by in individual or household, including derived data. "Covered data of the individual" means information that is linked or reasonably linkable to a specific individual or a device associated with that individual.

(B) Exclusions.—Such term does not include—

(i) de-identified data;

(ii) employee data; and

(iii) public records;

Provided that such data or records are not aggregated with other covered data.

(9) Covered entity.—

(A) In general.—The term "covered entity" means any entity or person that processes or transfers covered data and—

(i) is subject to the Federal Trade Commission Act (15 U.S.C. § 41 et seq.) as amended from time to time; or

(ii) is identified in Section 301(c) of this Act.

(B) Inclusion of commonly controlled and commonly branded entities.—Such term includes any entity or person that controls, is controlled by, is under common control with, or shares common branding with a covered entity.

(10) Data broker.—The term “data broker” means a covered entity that knowingly collects and processes covered data and transfers such data to third parties for consideration.

(11) De-identified data.—The term “de-identified data” means covered data that is altered, aggregated, or otherwise processed in such a way that it cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household, provided that the entity—

(A) takes reasonable administrative, technical, and legal measures to ensure that the information cannot be reidentified, or associated with, an individual, a household, or a device used by an individual or household; including—

(i) publicly commits in the disclosure required by Section 202—

(I) to process and transfer the information only in a de-identified form; and

(II) not to attempt to re-identify or associate the information with any individual, household, or device used by an individual or household; and

(ii) contractually obligates any person or entity that receives the information from the covered entity to comply with all of the provisions of this subsection.

(12) Delete.—The term “delete” means to remove or destroy data such that it is not maintained in retrievable form and effectively cannot be retrieved for any purpose.

(13) Derived data.—The term “derived data” means covered data that is created by the derivation of information, data, assumptions, inferences, or conclusions from facts, evidence, or another source of information or data about an individual, household, or device used by an individual or household.

(14) Device.—

(A) In general.—The term "device" means an item of hardware or equipment that can be connected directly or indirectly to networking technology and is linked or likable to an individual or a household. This term includes among other things computers, tablets, wireless phones, “smart” devices and appliances, connected automobiles, and data storage and networking equipment commonly found in use by individuals and households.

(B) Exclusion.—Such term does not include hardware or equipment that is used exclusively or predominantly only in commercial contexts, such as backbone networking equipment, industrial machinery, and other industrial equipment connected to the Internet.

(C) Hardware and equipment used by employees and contractors.—To the extent that an entity provides a hardware or equipment for use by an employee or contractor of the entity, the entity shall not be deemed to violate this Act by tracking or monitoring the use of such hardware or equipment so long as the entity discloses the tracking or monitoring to the employee or contractor.

(D) Rulemaking authority.—Upon petition of an interested party, and if the Commission determines that there exists significant confusion as to the applicability of the term "device" to a particular type or class of physical hardware or equipment, the Commission may conduct a rulemaking pursuant to section 553 of title 5, United States Code, to resolve the confusion.

(15) Employee data.—The term “employee data” means covered data that is collected and processed by a covered entity or the covered entity’s service provider—

(A) about an individual in the course of the individual’s employment or application for employment in any capacity (including on a contract or temporary basis) solely for purposes necessary for the individual’s status with the covered entity;

(B) emergency contact information for an individual who is an employee, contractor, or job applicant of the covered entity, provided that such data is retained or processed by the covered entity or the covered entity’s service provider solely for the purpose of having an emergency contact for such individual on file; and

(C) about an individual (or a relative of an individual) necessary for the purpose of administering benefits to which such individual or relative is entitled on the basis of the individual’s employment with the covered entity, provided that such data is retained or processed by the covered entity or the covered entity’s service provider solely for the purpose of administering such benefits.

(16) Individual.—The term “individual” refers to a natural person residing in the United States.

(17) Large data holder.—The term “large data holder” means a covered entity that, in the most recent calendar year—

(A) processed or transferred the covered data of more than 30,000,000 individuals, devices used by individuals or households, or households; or

(B) processed or transferred the sensitive covered data of more than 3,000,000 individuals, devices used by individuals or households, or households.

(18) Material.—In reference to any communication by a covered entity concerning any processing or practice, the term “material” means that such communication or the processing or practice referred to is likely to affect an individual’s decision or conduct regarding to such processing or practice.

(19) Process.—The term "process" means any operation or set of operations performed on covered data including collection, analysis, organization, structuring, retaining, using, deleting, or otherwise handling covered data.

(20) Publicly available information.—

(A) In general.—The term "publicly available information" means—

(i) information that a covered entity has a reasonable basis to believe is lawfully available to the general public from widely distributed media; and

(ii) information that is directly and voluntarily disclosed to the general public by the individual to whom the information relates.

(B) Limitation.—Such term does not include—

(i) information derived from publicly available information;

(ii) biometric information;

(iii) nonpublicly available information that has been combined with publicly available information; or

(iv) a disclosure that is required to be made by an individual under Federal, State, or local law.

(21) Public records.—The term "public records" means information that is lawfully made available from Federal, State, or local government records provided that the covered entity processes and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity.

(22) Sensitive covered data.—The term "sensitive covered data" means the following forms of covered data—

(A) A government-issued identifier, such as a Social Security number, passport number, or driver's license number, that uniquely corresponds to an individual person and that is not routinely made publicly available by the issuing authority.

(B) Any information that describes or reveals the existence or nature of a medical diagnosis, condition, or treatment or the past, present, or future physical health, mental health, or disability of an individual.

(C) A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account.

(D) Account log-in credentials such as a user name, email address or telephone number when combined with a password or similar credential, including a security question and answer, that would permit access to an online account, application, or communications device.

(E) Biometric information.

(F) Precise geolocation information that reveals the past or present actual physical location of an individual or device of an individual or household to within a reasonable degree of specificity.

(G) The content of an individual's private communications and the identity of the parties to such communications, unless the covered entity is an intended party to a communication.

(H) Information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information.

(I) Information revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information.

(J) Information revealing the online activities of an individual, a household, or a device used by an individual or household that relate to a category of sensitive covered data described in another subsection of this section.

(K) Calendar information, address book information, phone or text logs, photos, or videos maintained in an individual's non-public account, whether on an individual's device or otherwise.

(L) Any other covered data processed or transferred for the purpose of identifying the above data types.

(M) Any other covered data that the Commission determines should be included in the term "sensitive covered data" through a rulemaking pursuant to section 553 of title 5, United States Code, based on a finding that such data warrants similar treatment to the categories above in light of developments in technology, industry practices, or public expectations.

(23) Service provider.—

(A) In general.—The term "service provider" means a covered entity that processes or transfers covered data in the course of performing a service or function on behalf of, and at the direction of, another covered entity, but only to the extent that such processing or transfer—

(i) is reasonably necessary and limited to the performance of such service or function; and

(ii) is not performed under common ownership or control or with common branding.

(B) Exclusions.—Such term does not include—

(i) a covered entity that processes or transfers the covered data outside of the direct relationship between the service provider and the covered entity; or

(ii) a data broker to the extent that the broker transfers covered data to a covered entity or processes service provider data based on or in combination with covered data under the control of such data broker.

(24) Service provider data.—The term "service provider data" means covered data that is collected by or has been transferred to a service provider by a covered entity for the purpose of allowing the service provider to perform a service or function on behalf of, and at the direction of, such covered entity.

(25) Small or medium entity.—

(A) Business.—The term "small or medium entity" means, with respect to a for-profit business, an entity that can establish that, with respect to the 3 preceding calendar or fiscal years (or for the period during which the entity has been in existence if, as of such date, such period is less than 3 years) the entity does not—

(i) maintain annual average gross revenue in excess of $25,000,000;

(ii) annually process the covered data of an average of greater than 100,000 or more individuals, households, or devices used by individuals or households; and

(iii) derive 50 percent or more of its annual revenue from transferring individuals' covered data.

(B) Common control; common branding.—For purposes of subsection (A), the annual average gross revenue, data processing volume, and percentage of annual revenue of an entity shall include the revenue and processing activities of any person that controls, is controlled by, is under common control with, or shares common branding with such entity.

(C) Nonprofit entities.—The term "small or medium entity" means, with respect to an organization not organized to carry on business for their own profit or that of their members, an entity that does not annually process covered data of individuals, households, or devices used by individuals or households at more than levels to be established by the Commission pursuant to a rulemaking under section 553 of title 5, United States Code, within one year after the effective date of this Act; provided, however, that such levels shall not encompass entities that annually process the covered data of an average less than 100,000 individuals, households, or devices used by individuals or households.

(26) Third party.—The term "third party"—

(A) means any person or entity that—

(i) processes or transfers data received from a covered entity; and

(ii) is not a service provider with respect to such data; and

(B) does not include a person or entity that collects covered data from another entity if the two entities are related by common ownership or corporate control or share common branding.

(27) Third party data.—The term "third party data" means covered data that is transferred to a third party by a covered entity.

(28) Transfer.—The term "transfer" means to disclose, release, share, disseminate, make available, sell, license, or otherwise communicate covered data by any means to a service provider or third party—

(A) in exchange for consideration; or

(B) for a commercial purpose.

(29) Unique identifier.—The term "unique identifier" means any unique sequence or aggregation of data that is reasonably linkable to an individual, household, or device used by an individual or household, including a unique pseudonym, user alias, user or subject number or key code, telephone numbers, device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad identifier, or similar technology, as well as keystroke patterns, web browser data, device information or other forms of persistent or probabilistic identifiers that can be used to identify a particular individual, household, or device used by an individual or household.

(30) Widely distributed media.—The term "widely distributed media" means information that is available to the general public, including information from a telephone book or online directory, a television, Internet, or radio program, the news media, or an Internet site that is available to the general public on an unrestricted basis.

SEC. 4. EFFECTIVE DATES.

(a) Except as provided in this section, the provisions of this Act shall take effect upon the date of enactment of this Act.

(b) The obligations of covered entities under this Act shall take effect on the date that is 180 days after the date of enactment of this Act, except that the obligations under sections 103 and 105 shall take effect two years after the date of enactment.

(c) The obligations of covered entities under this Act shall not give rise to a cause of action based on this Act or any other law (1) less than six months after the entry into force of the provisions enforced for actions initiated under sections 301(a) and (b), or (2) less than one year after such entry into force for any other actions.

(d) The provisions of section 304 shall take effect two years after the date of enactment, except that subsection 304(f) shall take effect immediately upon the date of enactment of this Act.

TITLE I—INDIVIDUAL INFORMATION PRIVACY RIGHTS

SEC. 101. RIGHT TO LOYALTY AND CARE IN PROCESSING.

(a) Duty of loyalty.—A covered entity shall establish reasonable policies and practices, appropriate to the size and complexity of the covered entity and volume, nature, and intended uses of the covered data processed, so as to process and transfer data in a manner that respects the privacy of individuals linked or linkable to such data.

(1) A covered entity shall process and transfer covered data only to the extent reasonably necessary, proportionate, and in accordance with law—

(A) To provide a product or service specifically requested by an individual;

(B) For purposes otherwise reasonably foreseeable within the context of the relationship between the covered entity and an individual;

(C) To carry out a processing purpose or transfer for which the covered entity has obtained affirmative consent; or

(D) To the extent necessary for any purpose expressly permitted by this Act or other applicable law.

(2) A covered entity shall communicate its policies and practices for processing and transferring covered data in a fair and transparent manner appropriate to the complexity of the processing, the volume and nature of covered data processed, and the context of the relationship between the covered entity and the individual.

(b) Duty of care.—A covered entity shall not process or transfer covered data in a manner that reasonably foreseeably causes—

(1) Financial, physical, or reputational injury to an individual;

(2) Physical or other intrusion upon the solitude, seclusion, or obscurity of an individual or of intimacy and intimate relationships, where such intrusion would be highly offensive and unexpected to a reasonable person;

(3) Discrimination in violation of Federal antidiscrimination laws or antidiscrimination laws of any State or political subdivision thereof applicable to the covered entity; or

(4) Other substantial injury to an individual.

(c) Rule of construction.—The rights and obligations provided in subsequent sections of Titles I and II of this Act shall be construed in light of the duties set out in this section; provided, however, that this subsection shall not be interpreted to alter the applicable standard of liability under Section 303 of this Act.

SEC. 102. RIGHT TO TRANSPARENCY.

(a) A covered entity shall make publicly and prominently available at all times an up-to-date statement of its policies and practices relating to collection, processing, and transferring of covered data for each product or service the covered entity provides. Such a statement is distinct from the comprehensive disclosures provided for in section 202, but may link to specific information in such disclosure or share certain content.

(b) Any statement prescribed in subsection (a) shall be clear and intelligible to persons of ordinary understanding, as well as in all of the languages in which the covered entity provides the relevant products or services, available to vision-impaired persons, and in machine-readable format. It shall include—

(1) the categories of covered data being collected, processed, or transferred;

(2) the purposes for which the covered entity is collecting, processing, or transferring such covered data;

(3) the categories of third parties to which the covered entity transfers such covered data with information available listing such third parties;

(4) how long each category of covered data will be held;

(5) a summary of the rights provided in Title I of this Act, information as to how an individual can exercise such rights, and prominent links to the mechanisms for exercising such rights; and

(6) the identity and contact information of the contact entity, including of individuals responsible for the security and privacy of covered data processing.

(c) In addition to any statement prescribed in subsections (a) and (b), a covered entity shall provide individuals with timely, actionable, and context-specific notification of—

(1) any collection, processing, or transferring of sensitive covered data for which affirmative express consent is required under section 104(b);

(2) any collection, processing, or transferring of covered data that reflects material changes in policies and practices covered by Section 104(c); and

(3) any government request, subpoena, warrant or other process seeking covered data of the individual, unless otherwise required by law.

(4) Such notification shall—

(A) present clear, fair, and affirmative choices of actions to take in response;

(B) identify concretely what covered data is involved, the purpose of the processing, and why the data is needed for such purpose; and

(C) explain the right to withhold as well as grant consent, and the right to opt out where applicable.

(5) Such notification may include links to additional information provided pursuant to subsection (a), but such additional information shall not be essential to comprehension of the notification.

(6) The notification prescribed in this subsection is not required for an in-person transaction where the sensitive covered data will not be used for any purpose inconsistent with context in which such data was collected.

SEC. 103. RIGHT TO CONTROL.

(a) In general.—A covered entity shall establish means by which an individual may exercise the rights described in this section. Subject to subsections (f) and (g), the covered entity shall respond to the exercise of such rights as quickly as possible and in no case later than 45 days after receiving a verified request from the individual.

(b) The right to access.—In response to a verified request, a covered entity shall provide to the requesting individual in an easily-readable format and in language in which such covered entity transacts business with individuals—

(1) the covered data of the individual, including derived data, or an accurate representation of such data, that is processed by the covered entity and any service provider of the covered entity;

(2) if a covered entity transfers covered data, a description of the purpose for which the covered entity transferred the covered data of the individual to a service provider or third party; and

(3) an easily accessible list of names of any third parties and service providers to which the covered entity has transferred the covered data of the individual.

(c) The right to correction.—In response to a verified request, a covered entity shall—

(1) correct material inaccuracies or incomplete information with respect to the covered data of the individual that is processed by the covered entity; and

(2) notify any service provider or third party to which the covered entity transferred such covered data of the corrected information.

(d) The right to deletion.—In response to a verified request, a covered entity shall—

(1) delete or de-identify covered data of the individual that is processed by the covered entity; and

(2) notify any service provider or third party to which the covered entity transferred such covered data of the individual's request.

(e) The right to portability.—In response to a verified request, a covered entity shall, to the extent that is technically feasible, provide covered data of the requesting individual (except for derived data) in a portable, structured, standards-based, interoperable, and machine-readable format that is not subject to licensing restrictions.

(f) Frequency and cost of access.—A covered entity shall provide an individual with—

(1) the opportunity to exercise the rights described in subsections (b) through (e) not less than twice in any 12-month period; and

(2) with respect to the first two times that an individual exercises the rights described in subsections (b) through (e) in any 12-month period, shall allow the individual to exercise such rights free of charge.

(g) Exception for small and medium entities.—The rights and obligations of this section do not apply to a covered entity that is a small or medium entity. A small or medium entity that grows to exceed the definition of that category shall come into compliance with this section within six months after reaching that level.

(h) Regulations.—Not later than 18 months after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, establishing requirements for covered entities with respect to the verification of requests to exercise rights described in subsection (a)(1).

SEC. 104. RIGHT TO CONSENT.

(a) Opt Out of Transfers.—

(1) In general.—A covered entity—

(A) shall not transfer an individual's covered data to a third party if the individual objects to the transfer; and

(B) shall allow an individual to object to the covered entity transferring covered data of the individual to a third party through a process established under the rule issued by the Commission pursuant to subsection (2).

(2) Rulemaking.—

(A) In general.—Not later than 18 months after the date of enactment of this Act, the Commission shall issue a rule under section 553 of title 5, United States Code, establishing one or more acceptable processes for covered entities to follow in allowing individuals to opt out of transfers of covered data.

(B) Requirements.—The processes established by the Commission pursuant to this subsection shall—

(i) be centralized, to the extent feasible, to minimize the number of opt-out designations of a similar type that an individual must make;

(ii) include clear and conspicuous opt-out notices and consumer-friendly mechanisms to allow an individual to opt out of transfers of covered data;

(iii) allow an individual who objects to a transfer of covered data to view the status of such objection;

(iv) allow an individual who objects to a transfer of covered data to withdraw or modify such objection;

(v) be privacy protective;

(vi) permit covered entities to contract with service providers to handle the processing of opt-out requests; and

(vii) be informed by the Commission's experience developing and implementing the National Do Not Call Registry.

(b) Consent to Processing of Sensitive Data.—A covered entity—

(1) shall not process the sensitive covered data of an individual without the individual's prior, affirmative express consent;

(2) shall provide an individual with a consumer-friendly means to withdraw affirmative express consent to process the sensitive covered data of the individual previously given; and

(3) is not required to obtain prior, affirmative express consent to process or transfer publicly available information.

(c) Consent to Processing Involving Minors.—

(1) A covered entity shall not transfer the covered data of an individual under the age of 16 to a third party without affirmative express consent either of the individual or a parent or legal guardian if the covered has actual knowledge that such individual is less than 16 years of age.

(2) A parent or legal guardian may provide affirmative express consent on behalf of an individual who less than 18 years of age, provided that such consent shall be effective only until that individual reaches the age of 18.

(3) Once the minor turns 18 years of age, the affirmative express consent of that individual is required for the continued processing of sensitive covered data of the individual.

(d) Consent to Material Changes.—

(1) Unless it first obtains prior affirmative express consent from affected individuals, a covered entity shall not make a material change to its privacy policies or practices with respect to previously collected covered data that—

(A) would be inconsistent with terms on which an individual gave affirmative express consent to processing or transfer of sensitive collected data; or

(B) would adversely affect the exercise of opt-out rights under subsection (a) of this section.

(2) The covered entity shall provide direct notification regarding such changes to affected individuals where possible, taking into account available technology and the nature of the relationship between the covered entity and affected individuals.

SEC. 105. RIGHT TO RECOURSE.

(a) Covered entities must establish an internal process whereby an individual may—

(1) Seek recourse not otherwise provided for in this title for complaints concerning the practices of a covered entity in processing or transferring covered data under this Act; or

(2) appeal a refusal to act on a request to exercise any of the rights under subsections 103 (b) through (e) within a reasonable period of time after the individual's receipt of the notice sent by the covered entity under subsection (c) of this section.

(b) These internal processes must be as conspicuously available and easy to use as the process for submitting such requests under this section.

(c) A covered entity must inform an individual of any action taken on a request under subsection (a) without undue delay and in any event within forty-five days of receipt of the request. This period may be extended once by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests, provided that the covered entity informs the requesting individual of any such extension and the reasons for the delay within the initial forty-five days.

(d) If within the time periods set out in subsection (c) a covered entity does not take action to address an individual's request in full, it must inform the individual of the reasons for not taking action and instructions for how to appeal the decision with the covered entity as described in subsection (a)(2) of this section.

(e) Within thirty days of receipt of such an appeal under subsection (d), a covered entity must inform the individual of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. This period may be extended by fifteen additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The covered entity must inform the individual of any such extension and the reasons for the delay within thirty days of receipt of the appeal.

(f) In responding to a request or appeal pursuant to this section, a covered entity may make an offer of monetary compensation to an individual. An individual who receives such an offer shall have thirty days from the date of receipt to accept the offer, reject it, or otherwise respond. In the absence of a response within this time, the offer shall be deemed rejected. Payment of an accepted offer shall be made within sixty of receipt of the acceptance.

(g) Exception for small and medium entities.—The rights and obligations of this section do not apply to a covered entity that is a small or medium entity, unless the small or medium entity voluntarily and in a conspicuous manner opts to comply with this section. A small or medium entity that grows to exceed the definition of that category shall come into compliance with this section within six months after reaching that level.

SEC. 106. RIGHT TO DATA SECURITY.

(a) In General.—A covered entity shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data. Such data security practices shall be appropriate to—

(1) the volume and nature of the covered data collected, processed, or transferred by the covered entity;

(2) the potential risks to individuals from any unauthorized access, use, destruction, misappropriation, alteration, or disclosure involving such covered data;

(3) the vulnerabilities of covered data and the covered entity to such risks; and

(4) the size and complexity of the covered entity and the costs and technical feasibility of mitigating vulnerabilities.

(b) Specific Requirements.—Data security practices required under subsection (a) shall include, at a minimum, the following administrative, technical, physical, and legal safeguards—

(1) Assessment of vulnerabilities.—Identifying and assessing any reasonably foreseeable risks to, and vulnerabilities in, each system maintained by the covered entity that processes or transfers covered data.

(2) Preventive and correction action.—Taking preventive and corrective action to mitigate any risks or vulnerabilities to covered data identified by or reported to the covered entity, including appropriate changes to or the architecture, installation, or implementation of network or operating software or data security practices.

(3) Information retention and disposal.—Disposing covered data that is required to be deleted or is no longer necessary for the purpose for which the data was collected. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable for any purpose.

(4) Training.—Training all employees and any contractors with access to covered data on how to safeguard covered data and protect individual privacy and updating that training as necessary.

(c) FTC Guidance.—Not later than one year after the date of enactment of this Act, the Commission, in conjunction with the National Institute of Standards and Technology of the Department of Commerce, shall publish guidance on standards and practices for protecting data security, including—

(1) assessment of vulnerabilities;

(2) administrative, technical, physical, and legal safeguards to mitigate vulnerabilities and risks to covered data;

(3) effective data security and privacy training; and

(4) detecting, responding to, and recovering from attacks, intrusions and other system failures.

SEC. 107. CIVIL RIGHTS.

(a) In General.—A covered entity shall not process or transfer covered data, including derived data, that differentiates an individual or class of individuals with respect to any characteristic, category, or classification protected under the Constitution or laws of the United States as they may be construed or amended from time to time—

(1) for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for an opportunity for housing, employment, credit, or education in a manner that unlawfully discriminates against or otherwise diminishes the opportunity to the individual or class of individuals; or

(2) in a manner that unlawfully segregates, discriminates against, or otherwise reduces the availability to the individual or class of individuals the goods, services, facilities, privileges, advantages, opportunities, or accommodations of any place of public accommodation.

(b) Burden of proof.—If the processing of covered information differentiates an individual or class of individuals with respect to any characteristic, category, or classification protected under the Constitution or laws of the United States, the covered entity shall have the burden of demonstrating that—

(1) such processing of data—

(A) is independent of any protected characteristic, category, or classification; and

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

(2) there is no reasonable method of processing that could serve the interests described in clause (B) of subsection (b)(1) with a less discriminatory effect.

(c) FTC Enforcement Assistance.—

(1) Whenever the Commission obtains information or evidence that any covered entity may have processed or transferred covered in violation of any antidiscrimination law, the Commission shall transmit such information or evidence to, and cooperate with, the appropriate Executive agency with authority to initiate investigation or proceedings on the basis of the information or evidence. The Commission shall endeavor to implement this section by executing cooperative agreements or memoranda of understanding with the Executive agencies charged with enforcing Federal antidiscrimination laws.

(2) If the Commission obtains information or evidence that any covered entity may have processed or transferred covered in violation of the antidiscrimination law of any State or political subdivision thereof, the Commission may transmit such information or evidence to, and cooperate with, the appropriate State or local agency with authority to initiate investigation or proceedings on the basis of the information or evidence.

(3) In its annual reports to Congress pursuant to section 6(f) of the Federal Trade Commission Act (15 U.S.C. § 46 (f)), the Commission shall include a summary of the information transmitted to other Federal departments and agencies pursuant to subsection (b)(1) and an assessment of how processing and transfers of covered data may relate to Federal antidiscrimination laws.

(d) Exception.—Nothing in this section shall limit a covered entity from processing covered data for legitimate internal testing for the purpose of preventing unlawful discrimination or otherwise necessary and proportionate to evaluate the extent or effectiveness of the covered entity's compliance with this Act.

SEC. 108. PROHIBITION ON WAIVER OF RIGHTS.

(a) In General.—A covered entity shall not condition the provision of a service or product to an individual on the individual's agreement to waive privacy rights guaranteed by—

(1) sections 101, 105(a), and 106 through 109 of this Act; and

(2) sections 102 through 104, and 105(b) and (c) of this Act, except in the case where—

(A) there exists a direct relationship between the individual and the covered entity initiated by the individual;

(B) the provision of the service or product requested by the individual requires the processing or transferring of the specific covered data of the individual and the covered data is strictly necessary to provide the service or product; and

(C) an individual provides affirmative express consent to such specific limitations.

SEC. 109. LIMITATIONS AND APPLICABILITY.

(a) Exceptions to Individual Control.—

(1) In general.—A covered entity shall not comply with a request to exercise a right described in section 102 (b) through (e) if—

(A) the covered entity cannot reasonably verify that the individual making the request to exercise the right is—

(i) the individual to whom the covered data that is the subject of the request is linked, or

(ii) an individual or entity authorized to make such a request on such individual's behalf; or

(B) the covered entity reasonably believes that the request is made to interfere with a contract between the covered entity and another individual or entity.

(2) A covered entity may decline to comply with an individual's request to exercise a right described in section 102 (b) through (e) if—

(A) complying with the request would require the covered entity to retain covered data for the sole purpose of fulfilling the request or to re-identify covered data that has been de-identified;

(B) complying with the request would be impossible or demonstrably impracticable, provided that the receipt of a large number of verified requests within a short period shall not be considered to render compliance with a request demonstrably impracticable;

(C) complying with the request would prevent the covered entity from carrying out internal audits, performing accounting functions, processing refunds, or fulfilling warranty claims, provided that the covered data that is the subject of the request is not processed or transferred for any purpose other than these specific activities;

(D) the request is made to correct or delete publicly available information, and then only to the extent the data is publicly available information;

(E) complying with the request would impair the publication of newsworthy information of legitimate public concern to the public by a covered entity;

(F) complying with the request would impair the privacy of another individual or the rights of another to exercise free speech; or

(G) the covered entity processes or will process the data subject to the request for a specific purpose described in subsection (b) of this section and complying with the request would prevent the covered entity from using such data for such specific purpose.

(3) Additional information.—If a covered entity cannot reasonably verify that a request to exercise a right described in sections 102 through 105(a) is made by the individual whose covered data is the subject of the request (or an individual or entity authorized to make such a request on the individual's behalf), the covered entity shall request the provision of additional information necessary for the sole purpose of verifying the identity of the individual and shall not process or transfer such additional information for any other purpose.

(4) Burden minimization.—A covered entity shall minimize the inconvenience to individuals relating to the verification or authentication of requests.

(b) Exceptions to Affirmative Express Consent.—

(1) In general.—A covered entity may process or transfer covered data without the individual's affirmative express consent for any of the following purposes, provided that the processing or transfer is reasonably necessary, proportionate, and limited to the specific purpose—

(A) to complete a transaction or fulfill an order or service specifically requested by an individual, such as billing, shipping, or accounting;

(B) to provide an ephemeral and immediate answer or service in response to a request by an individual or household when the data collected is reasonably necessary to provide such answer or service, and is not recorded or retained beyond the time strictly necessary to provide such immediate answer or service;

(C) to perform system maintenance, diagnostics, debugging, or error repairs to ensure or update the functionality of a product or service provided by the covered entity;

(D) to detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service;

(E) to protect against deception, fraud, or other illegal or malicious activity;

(F) to comply with a legal obligation or the establishment, exercise, or defense of legal claims;

(G) to prevent an individual from suffering harm where the covered entity believes in good faith that there is an immediate risk to the life, safety, or welfare of an individual;

(H) to effectuate a product recall pursuant to Federal or State law; or

(I) to conduct scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or a similar oversight entity that meets standards promulgated by the Commission pursuant to section 553 of title 5, United

States Code, in consultation with the Departments of Commerce and Health and Human Services and the National Institutes of Health.

(2) The Commission shall have the authority pursuant to section 553 of Title 5, United States Code, to promulgate a regulation or regulations establishing additional specific exceptions to affirmative express consent in circumstances where the purposes of collection, processing, or transfer of sensitive covered data proposed offer significant benefits to the public interest or the individuals affected and the collection, processing, or transfer is reasonably necessary and proportionate for such purposes.

(3) Biometric information.—Not later than one year after the date of enactment of this Act, the Commission shall promulgate regulations pursuant to section 553 of title 5, United States Code, identifying privacy protective requirements for the processing of biometric information for a purpose described in clauses (C) or (D) of subsection (1). Such regulations shall include—

(A) data processing limitations, including a prohibition on the processing of biometric information unless the covered entity has a reasonable suspicion, after a specific criminal incident involving the covered entity, that the individual may engage in criminal activity;

(B) strict data transfer limitations, including a prohibition on the transfer of biometric information to a third party other than to comply with a legal obligation or to establish, exercise, or defend a legal claim; and

(C) strict transparency obligations, including requiring disclosures in a conspicuous and readily accessible manner regarding specific data processing and transfer activities.

(c) Bankruptcy.—In the event that a covered entity enters into a bankruptcy proceeding that could lead to the disclosure of covered data to a third party, the covered entity shall, within a reasonable time prior to any such disclosure—

(1) provide notice to all affected individuals of the proposed disclosure of covered data, identify the third party, and provide material information on the third party's policies and practices with respect to the covered data and the terms on which such data would be disclosed; and

(2) provide each affected individual with the opportunity to withdraw any previously-granted affirmative express consent with respect to covered data of the individual or to request that such data be deleted or de-identified.

(d) Journalism Exception.—Nothing in this title shall apply to the publication of newsworthy information of legitimate public concern to the public by a covered entity, or to the processing or transfer of information by a covered entity for that purpose.

TITLE II—RESPONSIBILITY AND OVERSIGHT OF COVERED ENTITIES

SEC. 201. ORGANIZATIONAL ACCOUNTABILITY.

(a) Risk assessment.—A covered entity shall consider the benefits of its covered data collection, processing, and transfer practices; the potential adverse consequences of such practices to individuals and their privacy; and measures to mitigate any such adverse consequences. Such risk assessments shall be reasonable and appropriate in scope and frequency given—

(1) the nature of the covered data collected, processed, or transferred by the covered entity;

(2) the volume and uses of the covered data collected, processed, or transferred by the covered entity;

(3) the potential risks to individuals from the collection, processing, and transfer of covered data by the covered entity; and

(4) the size and complexity of the covered entity.

(b) Privacy and data security officer.—A covered entity other than a small or medium entity shall designate—

(1) one or more qualified employees as privacy officers; and

(2) one or more qualified employees as data security officers, in addition to any employee designated under subsection (1).

(3) Such privacy and security officers shall develop and implement comprehensive written information privacy programs and data security programs to comply with this Act and to safeguard the privacy and security of covered data throughout the life cycle of development and operational practices of the covered entity's products or services.

(c) Risk assessments by large data holders.—A covered entity that is a large data holder shall document the privacy risk assessments required by subsection (a) in written form and maintain the record of such assessments for at least five years after it ceases to be applicable.

(1) Such a risk assessment shall be completed not later than one year after the date of enactment of this Act (or one year after the covered entity meets the definition of a large data holder in this Act), and in any event at least once every two years after the assessment required by subsection (1).

(2) Such risk assessments shall take into account the impact of data processing under common branding or control of the large data holder.

(3) The large data holder shall conduct and document in writing additional such assessments whenever a change in the factors enumerated in subsection (a) may increase the potential adverse consequences to individuals and their privacy. Such additional risk assessments shall include—

(A) the extent to which the actual policies and practices of the covered entity are consistent with any statement or disclosure required by sections 102 and 202 and representations to individuals, including specifically whether the processing and transferring of covered data are consistent with such statements;

(B) whether individual privacy settings available in connection with a service product offered by the covered entity are adequately accessible to individuals, consistent with reasonable expectations of individuals, and calibrated to provide control in accordance with these expectations;

(C) the extent to which the adverse consequences to individuals or groups of individuals vary from previous assessments of risks; and

(D) additional technical and operational measures that could enhance the protection of privacy and security and mitigate risks.

(4) The written record of any risk assessment required by this subsection shall be available upon request to the Commission. A covered entity may redact and segregate trade secrets, as defined by section 1839 of title 18 of the United States Code, from public disclosure.

SEC. 202. DISCLOSURE OF PRIVACY POLICIES AND PRACTICES.

(a) Comprehensive Disclosure.—A covered entity shall make publicly and persistently available, in a conspicuous and readily accessible manner, a detailed, complete, and accurate disclosure of the entity's data processing and data transfer activities and policies and practices to protect individual privacy and data security and to comply with this Act. Such disclosure shall include, at a minimum—

(1) each category of covered data the covered entity collects from individuals and information collected about individuals from third parties, publicly available information, and public records;

(2) the methods by which such covered data is collected from individuals and otherwise;

(3) for each such category, an explanation of the processing purposes for which the data is collected;

(4) a summary of the ways in which any covered data is used to customize products, services, marketing, or pricing to individuals or for algorithmic decision-making that may have a significant impact on individuals;

(5) whether the covered entity transfers covered data and, if so—

(A) each category of service provider and third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such categories;

(B) an accessible list, which shall be updated at least annually, that identifies each such third party to which the covered entity transfers data and specifies the purposes for which such data is transferred to each third party, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such transfer; and

(C) the identity of any affiliate of the covered entity to which covered data may be transferred by the covered entity and the purposes for which such transfer is made;

(6) how long each kind of covered data processed by the covered entity will be retained by the covered entity and a description of the covered entity's policies to minimize the collection and processing of data and mitigate risks to individuals;

(7) how individuals can exercise the individual rights enumerated in Title I of this Act;

(6) a summary of the covered entity's data security policies and identification of any data breaches reported under applicable law during at least the preceding three years;

(7) how individuals and organizations can request to receive notification of changes in the covered entity's processing and transferring of covered data and privacy and data security policies and practices;

(8) the identity and the contact information of the covered entity, including the contact information for the covered entity's representative for privacy and data security inquiries; and

(9) the effective date or dates of the privacy and security policies and practices described.

(b) Languages.—A covered entity shall make the disclosure required under this section available to the public in all of the languages in which the covered entity provides a product or service or carries out any other activities to which the disclosure relates, as well as available to vision-impaired persons and in machine-readable format.

(c) Changes to Disclosure.—A covered entity shall keep its disclosure reasonably current to reflect changes in its processing or transferring of covered data or the policies and practices to protect privacy and data, and shall announce material changes publicly through widely distributed media and through a distribution list for individuals and organizations that request such information, as well provide individual notice to the extent required by section 104(c).

(d) Large data holders.—Beginning one year after the date of enactment of this Act, the chief executive officer of a covered entity that is a large data holder (or, if the entity does not have a chief executive officer, the highest ranking officer of the entity) and each privacy officer and data security officer of such entity shall annually certify to the Commission, in a manner specified by the Commission, that the information provided in the entity's disclosure is accurate and timely and that the entity maintains adequate—

(1) internal controls to comply with this Act; and

(2) reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this Act.

(e) Requirements.—A certification submitted under subsection (a) shall be based on a review of the effectiveness of a covered entity's internal controls and reporting structures that is conducted by the certifying officers no more than 90 days before the submission of the certification.

SEC. 203. ALGORITHMIC DECISION-MAKING.

(a) Algorithmic decision-making risk assessment.—A covered entity that is a large data holder and uses or is considering using algorithmic decision-making that may have a significant effect on individuals shall include in the risk assessment required under section 201(c)—

(1) a description of the algorithmic decision-making processes including the design, logic, and training data used to develop the algorithmic decision-making;

(2) an evaluation of the accuracy and fairness, and risk of error, bias or discrimination in the algorithmic decision-making process; and

(3) an assessment of the relative benefits and costs of the algorithmic decision-making system in light of the nature of the covered data used, the accuracy and fairness, the relative risks of error, bias or discrimination, and the impact on individuals and other affected interests.

(b) Impact assessment.—On an annual basis after the risk assessment described in subsection (a) and notwithstanding any other provision of law, a covered entity that is a large data holder and engaged in, or providing services to others engaged in, algorithmic decision-making, directly or indirectly through a service provider, or is providing service to others for purposes of such decision-making, shall conduct an impact assessment of such algorithmic decision-making that—

(1) assesses whether the algorithmic decision-making system produces discriminatory results on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability; and

(2) identifies whether any such discriminatory results occur in the context of opportunities or eligibility for housing, education, employment, credit, or determining access to, or restrictions on the use of, any place of public accommodation or any other form of discrimination that may be covered by Federal law from time to time.

(3) The written record of any impact assessment required by this subsection shall be available upon request to the Commission. A covered entity may redact and segregate trade secrets, as defined by section 1839 of title 18 of the United States Code, from public disclosure.

(4) Study.—Within three years after the date of enactment of this Act, the Commission shall publish a report containing the results of a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. § 46(b)), examining the use of algorithms and benefits, costs, and impacts described in this section. Not later than three years after the publication of the initial report, and as necessary thereafter, the Commission shall publish a new and updated version of such report.

SEC. 204. SERVICE PROVIDERS AND THIRD PARTIES.

(a) General Obligations of Covered Entities.—

(1) A covered entity shall exercise reasonable due diligence in selecting a service provider and deciding to transfer covered data to a third party.

(2) A covered entity shall conduct reasonable oversight of its service providers and of third parties to ensure compliance with the applicable requirements of this section.

(3) The level of due diligence and oversight shall be appropriate to the size and complexity of the covered entity; the volume, nature, and uses of the covered data subject to transfer; and the risk of harm to individuals that may result from the disclosure of such covered data.

(b) Contractual Requirements.—A covered entity shall disclose covered data to a service provider only pursuant to a contract that is binding on both parties and meets the following requirements—

(1) the contract shall specify the service provider data that is the subject of the contract and require the service provider to collect or process only the data authorized by the covered entity;

(2) the contract shall specify the purposes for which the service provider is to collect and process such service provider data and the policies and practices that the service provider must apply to collecting and processing such data; and

(3) the contract shall incorporate a reasonable representation by the service provider that it has established appropriate procedures and controls to comply with this Act, including section 106, and specify what additional information or representations the service provider

must provide to the covered entity to demonstrate performance of its obligations under the contract and this section.

(4) No such contract shall relieve either the covered entity or the service provider of any requirement or obligation directly imposed on it under this Act.

(c) Service Providers Obligations.—A service provider—

(1) shall not process service provider data for any purpose other than the one performed on behalf of, and at the direction of, a covered entity; as specifically provided in this Act; or pursuant to the contract required by subsection (b);

(2) shall not transfer service provider data to a third party without the affirmative express consent, obtained by or on behalf of the covered entity, of the individual to whom such service provider data is linked or reasonably linkable.

(3) Notification.—A service provider shall give notifications to the covered entity as follows—

(A) a service provider shall give reasonable notice to the covered entity of amendments to policies and practices relating to collection, processing, or transfer of service provider data that may affect compliance with this Act or the contract with the covered entity required by subsection (b);

(B) in the event that a service provider is required to process service provider data to comply with a legal obligation, including a subpoena of other legal process or the establishment, exercise, or defense of legal claims, the service provider shall inform the covered entity of such requirement for service provider data prior to processing, unless the service is prohibited by law from doing so; and

(C) a service provider shall give the covered entity sufficient notice of an intention to employ a subcontractor to carry out or assist in the collection or processing of the service provider data sufficiently in advance of such employment to enable the covered entity to object; any such objection shall not be interposed arbitrarily, provided

(i) use of a subcontractor is not prohibited by the contract between the service provider and the covered entity;

(ii) the service provider is able to represent it has conducted due diligence consistent with subsection (a); and

(iii) the subcontractor is subject to a binding contract with the service provider that incorporates all relevant obligations of the contract required by subsection (b)(4). Except as otherwise required by law, the service provider shall delete or de-identify all service provider data after the completion of services as soon as possible after the completion of the services subject to a contract described in subsection (b).

(4) As applied to service provider data, a service provider is exempt from the requirements of sections 101 through 105, but shall, to the extent practicable—

(A) provide the covered entity with appropriate technical and administrative support in fulfilling requests made by individuals under sections 103 and 105 with respect to any service provider data;

(B) shall respond as promptly as possible to requests from a covered entity for deletion, de-identification, correction, or portability (as applicable), any service provider data received from that covered entity that such covered entity has identified as subject to a verified request from an individual described in section 103; and

(C) shall inform the covered entity if is unable to carry out the response called in subsection (B) because the service does not hold such data, cannot reasonably access such data, or is unable to comply because of a legal requirement on the service provider.

(d) Third Parties.—A third party—

(1) shall not process third party data for a purpose that is—

(A) inconsistent with the terms of an individual's consent to the transfer of sensitive covered data;

(B) otherwise inconsistent with the practices or policies disclosed pursuant to sections 102(b) or 202(a) by the covered entity from which the third party data was obtained;

(C) inconsistent with an individual's exercise of opt-out rights under section 104(a);

(D) not reasonably foreseeable in the context in which the third party data was collected or processed prior to transfer; or

(E) otherwise in violation of this Act or applicable law;

(2) may reasonably rely on representations made by the covered entity that transferred third party data regarding the expectation of a reasonable individual, provided the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) upon receipt of any third party data, is exempt from the requirements of section 101(a) with respect to such data, but shall have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(4) Guidance.—Not later than one year after the date of enactment of this Act, the Commission shall issue guidance for covered entities regarding compliance with this subsection.

(e) With regard to obligations of a covered entity under this Act to list or otherwise identify service providers, if a service provider (termed a "contracting service provider" for purposes of this subsection) contracts with one or more individuals who act as independent contractors to provide a benefit (such as transportation, delivery, short term housing, or other immediate benefit) directly to an end customer (termed an "end service provider" for purposes of this subsection), the covered entity must list or otherwise identify the contracting service provider, but need not list or identify any end service providers.

(f) In General.—The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations necessary to carry out the provisions of this section.

SEC. 205. DATA BROKERS.

(a) In General.—Each covered entity that has acted as a data broker shall register or reregister with the Commission pursuant to the requirements of this section—

(1) for a covered entity that acted as a data broker in the 90 days prior to the enactment of this Act, not later than 180 days after the date of enactment of this Act; and

(2) for a covered entity that commences or resumes acting as a data broker following enactment of this Act, not later than 90 days after the date such activity commences or resumes.

(3) Each covered entity registered as a data broker shall renew its registration annually on or before the anniversary of its initial registration.

(b) Registration Requirements.—In initially registering or annually registering with the Commission as required under subsection (a), a covered entity required to register or register under subsection (a) shall do the following—

(1) pay to the Commission a registration fee of $100 for every 100,000 individuals linked to covered data it processes;

(2) provide the Commission with the following information—

(A) the name and primary physical, email, and Internet addresses of the covered entity;

(B) a copy of its current disclosure pursuant to section 202(a) of this Act;

(C) a link to its website through which an individual may exercise the rights provided under Sections 103 through 105 of this Act;

(D) a description of the categories of information in processes linked or reasonably linkable to individuals; and

(E) any additional information or explanation the covered entity chooses to provide concerning its data collection and processing practices.

(c) Penalties.—A covered entity that fails to register as required under subsection (a) of this section shall be liable for—

(1) a civil penalty of $100 for each day it fails to register; and

(2) an amount equal to the fees due under this section for each year that it failed to register as required under subsection (a).

(d) Publication and Oversight of Registration Information.—

(1) The Commission shall establish forms and online mechanisms for registration and payment of fees pursuant to this section, and shall publish on the website of the Commission the registration information provided by covered entities under this section.

(2) The Commission is authorized to apply the proceeds of fees or penalties paid pursuant to this section to the development of an applications program interface or other mechanism by which individuals may exercise their rights under sections 103 through 105 of this Act through a single transaction.

(3) In its annual reports to Congress pursuant to section 6(f) of the Federal Trade Commission Act (15 U.S.C. § 46 (f)), the Commission shall report on the number of covered entities registered under this section, the amount of fees collected, the number of individuals affected as inferred from fee receipts, and an assessment of other information obtained regarding data brokers and the operation of this section.

SEC. 206. WHISTLEBLOWER PROTECTIONS.

(a) In General.—A covered entity shall not, directly or indirectly, discharge, demote, suspend, threaten, harass, or in any other manner discriminate against a covered individual of the covered entity because—

(1) the covered individual, or anyone perceived as assisting the covered individual, takes (or the covered entity 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 testify) in an investigation or judicial or administrative proceeding concerning such a violation; or

(4) the covered individual assists or participates (or the covered entity expects that the covered individual will assist or participate) in such an investigation or judicial or administrative proceeding, or the covered individual takes any other action to assist in carrying out the purposes of this Act.

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

(1) Temporary relief while the case is pending;

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

(3) Three times the amount of back pay otherwise owed to the individual, with interest; and

(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) Covered Individual Defined.—In this section, the term "covered individual" means an applicant, current or former employee, contractor, subcontractor, grantee, or agent of an employer.

TITLE III—MISCELLANEOUS

SEC. 301. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) Treatment as violation of rule.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice

prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. § 57a(a)(1)(B)).

(b) Powers of commission.—

(1) In general.—Except as provided in subsection (c), the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. § 41 et seq.) were incorporated into and made a part of this Act.

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

(3) Independent litigation authority.—The Commission may commence, defend, or intervene in, and supervise the litigation of any civil action under this subsection (including an action to collect a civil penalty) and any appeal of such action in its own name by any of its attorneys designated by it for such purpose. The Commission shall notify the Attorney General of any such action and may consult with the Attorney General with respect to any such action or request the Attorney General on behalf of the Commission to commence, defend, or intervene in any such action.

(4) Civil penalties.—

(A) A covered entity found in violation of this Act shall be subject to a civil penalty calculated by multiplying the number of individuals affected by an amount not to exceed $43,280.

(B) In assessing such a penalty, the Commission shall consider—

(i) the gravity of the violation, including the degree of harm to the privacy and security of individuals and impact on their reasonable expectations; and

(ii) the conduct of the covered entity, including its size, sophistication, and resources, its actions to comply with this Act, and any prior conduct and remedial actions taken.

(C) Beginning on the date the Consumer Price Index is published by the Bureau of Labor Statistics (or any successor agency) three years after the date of enactment of this Act, the amount in subsection (4)(A) shall be adjusted annually by the amounts of change in the Consumer Price Index in the intervening year or years.

(c) Common carriers and nonprofit organizations.—Notwithstanding section 4, 5(a), or 6 of the Federal Trade Commission Act (15 U.S.C. §§ 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner provided in this section, with respect to—

(1) common carriers subject to the Communications Act of 1934 (47 USC 151 *et seq*.) and all Acts amendatory thereto and supplementary thereof; and

(2) organizations not organized to carry on business for their own profit or that of their members.

(d) Information privacy and security relief fund.—

(1) Establishment of relief fund.—There is established in the Treasury of the United States a separate fund to be known as the "Information Privacy and Security Relief Fund" (referred to in this subsection as the "Relief Fund").

(2) Deposits.—

(A) Deposits from the commission.—The Commission shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act.

(B) Deposits from the attorney general.—The Attorney General of the United States shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.

(3) Use of fund amounts.—Notwithstanding section 3302 of title 31, United States Code, amounts in the Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been obtained under this Act. To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of consumer or business education relating to information privacy and data security or for the purpose of engaging in technological research that the Commission considers necessary to enforce this Act.

(4) Amounts not subject to apportionment.—Notwithstanding any other provision of law, amounts in the Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.

(e) New bureau.—

(1) In general.—The Commission shall establish a new Bureau within the Commission comparable in structure, size, organization, and authority to the existing Bureaus with the Commission related to consumer protection and competition.

(2) Mission.—The mission of the Bureau established under this subsection shall be to assist the Commission in exercising the Commission's authority under this Act and under other Federal laws addressing privacy, data security, and related issues.

(3) Appointments.—The Chair of the Commission shall appoint a Director of the Bureau. The Bureau Director in turn shall appoint not less than 500 professional staff without regard to civil service laws, which staff shall include but not be limited to lawyers, people trained in information technologies, and economists.

(4) Timeline.—Such Bureau shall be established, staffed, and fully operational within 2 years of enactment of this Act.

SEC. 302. ENFORCEMENT BY STATES.

(a) Civil action.—In any case in which the attorney general of a State or other officer duly authorized by State law has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State or other officer authorized by State law, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(1) enjoin that act or practice;

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

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

(4) obtain such other relief as the court may consider to be appropriate.

(b) Notice to the Commission and rights of the Commission.—Except where not feasible, the State officer bringing an action pursuant to subsection (a) shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. If prior notice is not feasible, the State shall provide a copy of the complaint to the Commission immediately upon instituting the action. Upon receiving such notice, the Commission may elect to—

(1) to assume responsibility for the prosecution of the action and either bring its own action instead (and dismiss the action brought by the State) or intervene as of right in the action brought by the State and prosecute the action;

(2) intervene as of right in such action and, upon intervening be heard on all matters arising in such action (including the filing of petitions for appeal of a decision in such action); or

(3) allow the action brought by the State to proceed without Commission involvement.

(c) Preservation of state powers.—No provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or other authorized officer of a State to—

(1) bring an action or other regulatory proceeding arising solely under the law in effect in that State; or

(2) exercise the powers conferred on the attorney general or other officer of a State by the laws of the State, including the ability to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(d) Venue; service of process.—

(1) Venue.—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code. In the event actions are brought by officers of more than one State involving common questions of law or fact warranting consolidation of cases, they shall be consolidated and transferred in accordance with section 1407 of title 28, United States Code.

(2) Service of process.—In an action brought under subsection (1), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

SEC. 303. ENFORCEMENT BY INDIVIDUALS.

(a) Any individual who has been injured by a violation of this Act or a regulation promulgated under this Act may bring a civil action in any State or Federal court of competent jurisdiction as provided in this section.

(b) Prior to bringing such an action against a covered entity—

(1) that is covered by or has opted into section 105, such individual shall seek recourse as provided in section 105 of this Act and shall file with the complaint an affidavit describing the recourse sought and the manner in which the covered entity has failed to provide such recourse; or

(2) that is a small to medium entity that has not opted into section 105, such individual shall at least thirty days prior to the filing of any such action mail or delivery to the covered entity a written demand for relief, identifying the claimant and reasonably describing the violation of this Act and the injury suffered. The covered entity may, within thirty days of the mailing or delivery of the demand for relief, make a written tender of settlement. If the tender is rejected by the claimant, the coverer entity may, in any subsequent action, file the

written tender and an affidavit concerning its rejection and thereby limit any recovery to the relief tendered if the court finds that the relief tendered was reasonable in relation to the injury actually suffered by the claimant.

(3) In the event of an immediate threat of physical injury or other irreparable harm as a result of the violation alleged that makes recourse or prior notice unfeasible, such individual may forgo compliance with subparagraphs (1) or (2) and shall in that event file with the complaint an affidavit describing the immediate threat or other irreparable harm.

(c) The complaint shall allege with reasonable particularity–

(1) the violation of the duty of care as provided in Section 101(d);

(2) the knowing or reckless disregard of the privacy or security of individuals in violation of other provisions of this Act, except as otherwise provided in this Act; or

(3) the willful or repeated violation of sections 103, 105, 201, or 202.

(d) In a civil action in which the plaintiff prevails, the court may award—

(1) actual damages for the injuries by the violations found;

(2) statutory damages in an amount not less than $100 nor greater than $1,000 per violation per day for willful or repeated violations; for the purpose of this provision, a violation shall not be considered repeated solely by virtue of the fact that it affects a large number of individuals at one time;

(3) reasonable attorney's fees and litigation costs, provided that if the final amount of a judgment for actual damages is not more favorable than an offer made to the plaintiff pursuant to section 105(f) or section 303(b)(2), the plaintiff must pay costs; and

(4) any additional relief, including equitable or declaratory relief, that the court determines appropriate.

(e) A civil action under this section shall be the exclusive judicial remedy for the individual injuries at issue.

(f) Class Actions.—

(1) This subsection shall apply in each private civil action arising under this Act that is brought as a class action. The Federal courts shall have exclusive jurisdiction over any civil action under this section brought as a class action.

(2) Certification filed with complaint.—

(A) Each plaintiff seeking to serve as a representative party on behalf of a class shall provide a sworn certification, which shall be personally signed by such plaintiff and filed with the complaint, that—

(i) states that the plaintiff has reviewed the complaint and authorized its filing;

(ii) states that the plaintiff is willing to serve as a representative party on behalf of a class, including providing testimony at deposition and trial, if necessary;

(iii) sets forth all of the matters required by subsections (b) and (c) above during the class period specified in the complaint; and

(iv) states that the plaintiff will not accept any payment for serving as a representative party on behalf of a class beyond the plaintiff's pro rata share of any recovery, except as ordered or approved by the court in accordance with subsection (6)(D).

(B) The certification filed pursuant to subsection (f)(2) shall not be construed to be a waiver of the attorney-client privilege.

(3) Appointment of lead plaintiff.—

(A) Not later than 20 days after the date on which the complaint is filed, the plaintiff or plaintiffs shall cause to be published, in a widely circulated national publication or wire service, and a widely used online information service, a notice advising members of the purported plaintiff class—

(i) of the pendency of the action, the claims asserted therein, and the purported class period; and

(ii) that, not later than 60 days after the date on which the notice is published, any member of the purported class may move the court to serve as lead plaintiff of the purported class.

(B) If more than one action on behalf of a class asserting substantially the same claim or claims arising under this chapter is filed, only the plaintiff or plaintiffs in the first filed action shall be required to cause notice to be published in accordance with clause (A).

(C) Notice required under clause (A) shall be in addition to any notice required pursuant to the Federal Rules of Civil Procedure.

(D) Not later than 90 days after the date on which a notice is published under clause (A), the court shall consider any motion made by a purported class member in response to the notice, including any motion by a class member who is not individually named as a plaintiff in the complaint or complaints, and shall appoint as lead plaintiff the member or members of the purported plaintiff class that the court determines to be most capable of adequately representing the interests of class members (hereafter in this subsection referred to as the "most adequate plaintiff") in accordance with this clause.

(E) If more than one action on behalf of a class asserting substantially the same claim or claims arising under this chapter has been filed, and any party has sought to

consolidate those actions for pretrial purposes or for trial, the court shall not make the determination required by clause (D) until after the decision on the motion to consolidate is rendered. As soon as practicable after such decision is rendered, the appropriate court or courts shall appoint the most adequate plaintiff as lead plaintiff for the consolidated actions in accordance with this subsection. The most adequate plaintiff shall, subject to the approval of the court, select and retain counsel to represent the class.

(F) For purposes of this subsection, discovery relating to whether a member or members of the purported plaintiff class is the most adequate plaintiff may be conducted by a plaintiff only if the plaintiff first demonstrates a reasonable basis for a finding that the presumptively most adequate plaintiff is incapable of adequately representing the class.

(4) The share of any final judgment or of any settlement that is awarded to a representative party serving on behalf of a class shall be equal, on a per rata basis, to the portion of the final judgment or settlement awarded to all other members of the class. Nothing in this subsection shall be construed to limit the award of reasonable costs and expenses (including lost wages) directly relating to the representation of the class to any representative party serving on behalf of a class.

(5) The terms and provisions of any settlement agreement of a class action shall not be filed under seal, except that on motion of any party to the settlement, the court may order filing under seal for those portions of a settlement agreement as to which good cause is shown for such filing under seal. For purposes of this subsection, good cause shall exist only if publication of a term or provision of a settlement agreement would cause direct and substantial harm to any party.

(6) Total attorneys' fees and expenses awarded by the court to counsel for the plaintiff class shall not exceed a reasonable percentage of the amount of any damages and prejudgment interest actually paid to the class.

(7) Any proposed or final settlement agreement that is published or otherwise disseminated to the class shall include each of the following disclosures to class members, along with a cover page summarizing the information contained in such statements—

(A) The amount of the settlement proposed to be distributed to the parties to the action, determined in the aggregate and on an average per person basis;

(B) A brief statement explaining the reasons why the parties are proposing the settlement and of the potential outcomes of the case.

(i) If the settling parties agree on the average amount of damages per person that would be recoverable if the plaintiff prevailed on each claim alleged under

this chapter, a statement concerning the average amount of such potential damages per person.

(ii) If the settling parties do not agree on the average amount of damages per person that would be recoverable if the plaintiff prevailed on each claim alleged under this chapter, a statement from each settling party concerning the issue or issues on which the parties disagree.

(iii) A statement made in accordance with subclauses (i) or (ii) concerning the amount of damages shall not be admissible in any Federal or State judicial action or administrative proceeding, other than an action or proceeding arising out of such statement.

(C) If any of the settling parties or their counsel intend to apply to the court for an award of attorneys' fees or costs from any fund established as part of the settlement, a statement on the cover page of any notice to a party of any proposed or final settlement agreement indicating—

(i) which parties or counsel intend to make such an application;

(ii) the amount of fees and costs that will be sought (including the amount of such fees and costs determined on an average per person basis), and a brief explanation supporting the fees and costs sought; and

(iii) contact information of one or more representatives of counsel for the plaintiff class who will be reasonably available to answer questions from class members concerning any matter contained in any notice of settlement published or otherwise disseminated to the class.

(D) Such other information as may be required by the court.

(9) In any private action arising under this chapter that is certified as a class action pursuant to the Federal Rules of Civil Procedure, the court may require an undertaking from the attorneys for the plaintiff class, the plaintiff class, or both, or from the attorneys for the defendant, the defendant, or both, in such proportions and at such times as the court determines are just and equitable, for the payment of fees and expenses that may be awarded under this subsection.

(10) Sanctions for abusive litigation.—

(A) In any private action arising under this chapter, upon final adjudication of the action, the court shall include in the record specific findings regarding compliance by each party and each attorney representing any party with each requirement of Rule 11(b) of the Federal Rules of Civil Procedure as to any complaint, responsive pleading, or dispositive motion.

(B) If the court makes a finding under clause (A) that a party or attorney violated any requirement of Rule 11(b) of the Federal Rules of Civil Procedure as to any complaint, responsive pleading, or dispositive motion, the court shall impose sanctions on such party or attorney in accordance with Rule 11 of the Federal Rules of Civil Procedure. Prior to making a finding that any party or attorney has violated Rule 11 of the Federal Rules of Civil Procedure, the court shall give such party or attorney notice and an opportunity to respond.

(C) If the party or attorney against whom sanctions are to be imposed meets its burden under subsection (B), the court shall award the sanctions that the court deems appropriate pursuant to Rule 11 of the Federal Rules of Civil Procedure.

(g) Statute of limitations.—Any civil action under this subsection may be brought in any appropriate State or Federal court without regard to the amount in controversy, within three years from the date on which the violation occurs or the date on which the plaintiff discovered or reasonably should have discovered such violation, whichever is later.

(h) Invalidity of Pre-dispute Arbitration Agreements and Pre-dispute Joint Action Waivers.—

(1) 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 privacy or data security dispute arising under this Act.

(2) Applicability.—Any determination as to whether or how this subsection applies to any privacy or data security dispute shall be made by a court, rather than an arbitrator, without regard to whether such agreement purports to delegate such determination to an arbitrator.

(3) Definitions.—For purposes of this subsection—

(A) 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.

(B) 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.

(C) The term “privacy or data security dispute” means any claim relating to an alleged violation of this Act, or a regulation promulgated under this Act, and between an individual and a covered entity.

SEC. 304. INDUSTRY-SPECIFIC COMPLIANCE PROGRAMS.

(a) In General.—The Commission may approve compliance programs designed to provide guidance to covered entities on how to comply with requirements and obligations of this Act in the context of specific subsectors, technologies, or applications, and to establish compliance systems to ensure that covered entities meet commitments to follow the guidance. Such industry-specific compliance programs shall be developed by one or more covered entities or organizations representing categories of covered entities to create standards or codes of conduct regarding compliance with one or more provisions in this Act, and may be submitted to the Commission for consideration no earlier than two years after the date of enactment of this Act.

(b) Requirements.—To be eligible for approval by the Commission, a compliance program shall—

(1) specify clear and enforceable requirements for covered entities participating in the program that provide an overall level of privacy, or data security protection, or other compliance with this Act, that is equivalent to or greater than that provided in the relevant provisions in this Act (which provisions shall be specifically identified in any application for a program);

(2) require each participating covered entity to post in a prominent place a clear and conspicuous public attestation of compliance and a link to the website described in subsection (4);

(3) require a process for the independent assessment of a participating covered entity's compliance with the program prior to attestation and on an annual basis;

(4) create a website describing the program's goals and requirements, listing participating covered entities, and providing a method for individuals and organizations representing individuals to ask questions and file complaints about the program or any participating covered entity;

(5) take meaningful action for non-compliance with the compliance program or with relevant provisions of this Act by any participating covered entity, which shall depend on the severity of the non-compliance and may include—

(A) removing the covered entity from the program;

(B) referring the covered entity to the Commission for enforcement;

(C) publicly reporting the disciplinary action taken with respect to the covered entity;

(D) providing redress to individuals harmed by the non-compliance;

(E) making voluntary payments to the United States Treasury; and

(F) taking any other action or actions to ensure the compliance of the covered entity with respect to the relevant provisions of this Act and deter future non-compliance; and

(6) issue annual reports to the Commission and to the public detailing the activities of the program and its effectiveness during the preceding year in ensuring compliance with the relevant provisions of this Act by participating covered entities.

(c) Consideration and Approval by the Commission.—The Commission shall consider and respond to the application as follows, and pursuant to regulations issued pursuant to this section—

(1) The application for approval shall set forth how the program meets the requirements of subsection (b); list to the extent possible the covered entities known or expected to participate; identify the entity or entities that will conduct the independent assessment required by subsection (b)(3); and identify organizations or individuals consulted regarding the requirements of the program that the applicant wishes to bring to the attention of the Commission.

(2) Public Comment and Requests for Information.—The Commission shall provide an opportunity for public comment on the application, and may issue requests for information to the applying party or other entities.

(3) Time for Approval.—Unless an application is withdrawn, the Commission shall issue a decision regarding the approval or non-approval of a certification program not later than 270 days after an application for approval is submitted, except that the Commission may extend this deadline based on the number of applications simultaneously pending before it.

(4) Standard for Approval.—The Commission shall approve an application only if the applicant demonstrates that the program provides an overall level of privacy, or data security protection, or other compliance with this Act that is equivalent to or greater than that provided in the relevant provisions in this Act. In evaluating the proposed compliance program, the Commission shall consider whether and how much the proposal reflects consultation and/or consensus with academic, civil society, and other experts and stakeholders knowledgeable about the matters covered by the proposal.

(5) Explanation of Decision.—The Commission shall publicly explain in writing the reasons for approving or denying each application that it reviews pursuant to this section.

(6) Duration of an Approval.—Any approval of a program by the Commission shall be for an initial duration of not more than four years. No later than 270 days before the end of an approval period, the applicant may seek a renewal of the approval pursuant to the procedures in this section. In such application for renewal, the applicant shall provide the full information required for an initial application, and shall highlight for the Commission and public review all alterations and improvements, if any, in the program as compared to

the previously approved program. If the Commission approves of the requested renewal, such renewal shall be of a duration of not more than seven years.

(d) Effect of Approval.—A covered entity that complies with a compliance program approved by the Commission shall be deemed to be in compliance with the provisions of this Act addressed by such program.

(e) Effect of Non-compliance.—

(1) In general.—A covered entity that has certified compliance with an approved program and is found not to be in compliance with such program by the Commission shall be considered to be in violation of the section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) prohibition on unfair or deceptive acts or practices.

(2) Effect of decision by program on FTC authority.—A determination by an approved compliance program with respect to the compliance or noncompliance with such program of a covered entity shall not affect the authority of the Commission to make a different determination with respect to such compliance.

(f) Rulemaking.—The Commission may promulgate regulations under section 553 of title 5, United States Code, to establish the process by which the Commission will determine whether to approve or renew a compliance program under this section. Such process shall include—

(1) requirements for the form and content of requests for approval, including a requirement that the requesting entity provide details about the process used to develop the proposed compliance program, including whether and how much the proposal reflects consultation and/or consensus with academic, civil society, and other experts and stakeholders knowledgeable about the matters covered by the proposal;

(2) timing and form for notice and opportunity for public comment about a request for approval; and

(3) equitable approaches to the scheduling of consideration of applications for approval of compliance programs and managing the resources of the Commission needed to review applications for and compliance with such programs.

SEC. 305. RELATIONSHIP TO FEDERAL AND STATE LAWS.

(a) Federal Law Preservation.—Nothing in this Act or a regulation promulgated under this Act shall be construed to limit—

(1) the authority of the Commission, or any other Executive agency, under any other provision of law; or

(2) any other provision of Federal law unless as specifically authorized by this Act.

(b) Applicability of Other Information Privacy Requirements.—A covered entity that is required to comply with the provisions of a federal law listed in this subsection and is in compliance with the information privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this title, except for section 107, with respect to data subject to the requirements of such regulations, part, title, or Act—

(1) Title V of the Financial Services Modernization Act of 1999 (15 U.S.C. § 6801 et seq.);

(2) The Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17931 et seq.);

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

(4) The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

(5) Section 444 of the General Education Provisions Act (20 U.S.C. § 1232g) (commonly referred to as the "Family Educational Rights and Privacy Act");

(6) Regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d–2 note);

(7) The Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.);

(8) The Fair Debt Collection Practices Act (15 U.S.C. § 692 et seq.);

(9) The Controlling Assault and Non-Solicited Pornography and Marketing Act (15 U.S.C. chapter 103);

(10) The Restore Online Shoppers' Confidence Act (15 U.S.C. § 8403);

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

(12) The Telephone Consumer Protection Act (47 U.S.C. § 227);

(13) The Genetic Information Nondiscrimination Act (42 U.S.C. § 2000ff);

(14) Section 222 of the Communications Act of 1934, as amended, insofar as it relates to use of information necessary to provide emergency services or to address anticompetitive behavior based on customer usage of existing services (47 U.S.C. § 222);

(15) The Electronic Communications Privacy Act (18 U.S.C. § 2510 et seq.);

(16) The Driver's Privacy Protection Act (18 U.S.C. § 2721 et seq.); and

(17) The Federal Aviation Act of 1958 (49 U.S.C. § 1301 et seq.).

(c) Applicability of Other Data Security Requirements.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17931 et seq.), part

C of title XI of the Social Security Act (42 U.S.C. § 1320d et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d–2 note), and is in compliance with the information security requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the requirements of section 107 with respect to data subject to the requirements of such regulations, part, title, or Act.

(d) Not later than one year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of subsections (b) and (c), in consultation with the Department of Health and Human Services, the Department of Education, the Federal Communications Commission, and Consumer Financial Protection Board and, with respect to subsection (c), the Department of Commerce and the Department of Homeland Security.

(e) Except as provided in subsection (b)(14), any provision of the Communications Act of 1934 as amended (47 U.S.C. § 151 et seq.) relating to privacy policies and practices and any other matters covered by this Act or of any rules or regulations promulgated thereunder shall have no force or effect.

(f) State Law Preservation.—Except to the extent specifically provided in subsection (g), nothing in this Act shall be construed to preempt, displace, or supplant the following laws, rules, regulations, or requirements of any State or political subdivision thereof—

(1) Consumer protection laws of general applicability;

(2) Laws prohibiting unfair and deceptive or unconscionable practices;

(3) Laws protecting civil rights or freedom from discrimination based on race, sex, national origin, or other classification protected under State law;

(4) Laws that govern the privacy rights or other protections of employees, employee information, students or student information, or library users or library usage information;

(5) Laws that address notification requirements in the event of a data breach;

(6) Statutory and common law rights and remedies for individuals under contract, property, or tort law, including existing causes of action based personal injury, property damage, invasion of privacy, trespass, or other damage;

(7) Criminal laws governing fraud, theft, unauthorized access to information or communications or unauthorized use of information, malicious behavior, and similar provisions, and laws of criminal procedure;

(8) Laws addressing collection and use of social security numbers, motor or vehicle license information, or other public records governed by State law;

(9) Public safety or sector-specific laws unrelated to privacy or security; and

(10) State constitutional law.

(g) Preemption of Inconsistent State Laws.—

(1) This Act shall preempt and supersede any State law regulating the collection, processing, transferring, and security of covered data to the extent such law is inconsistent with the provisions of this Act or a standard, rule, or regulation promulgated under this Act.

(2) Upon petition of any interest party or its own motion, if the Commission determines, after notice and the opportunity to comment, that the law of any State or subdivision thereof (including law enacted consistent with subsection (c)(2)) is inconsistent with the operation of this Act or any standard, rule, or regulation promulgated thereunder, it shall preempt to the extent necessary to prevent such conflict.

(3) Upon petition of any interested party or its own motion, if the Commission determines, after notice and the opportunity to comment, that the laws of any two or more States or subdivisions thereof (including laws enacted consistent with subsection (g)(4)) conflict with each other in a manner that harms the goals or operation of this Act or any standard, rule or regulation promulgated thereunder, and that creates a burden on interstate Commerce, it may preempt one or more of such laws to the extent necessary to prevent such conflict, harm, or burden.

(4) Except as may be provided by a further Act of Congress, subsection (g)(1) shall not preempt or supersede any provision of State law (including any provision of a State constitution) that—

(A) is enacted eight (8) years after the enactment of this Act;

(B) states explicitly that the provision is intended to supplement this Act; and

(C) gives greater protection to individuals than is provided under this Act.

(5) Subsection (g)(1) shall not preempt or supersede any provision of—

(A) any State law that establishes additional obligations to regulate covered entities as defined in the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191), the Family Educational Rights and Privacy Act (Pub. L. 93-380), the Fair Credit Reporting Act of 1974 (Pub. L. 91-508), or the Financial Services Modernization Act of 1999 (Pub. L. 106-102); or

(B) any law of a State or political subdivision thereof that regulates the use of biometric covered data for surveillance of individuals in public spaces within the jurisdiction of such State or political subdivision.

(h) Commission on Harmonization of Federal Privacy Laws.—As of the date five years after the enactment of this Act, there is hereby established a Bipartisan Privacy Harmonization Commission (in this Act referred to as the “Harmonization Commission”), which not later than 24 months following its initial meeting shall issue a report to Congress that (1) analyzes and compares the operation and effectiveness of this Act with other Federal laws that protect privacy

and data security, and (2) considers recommendations to Congress about how Federal laws addressing privacy and data security may be harmonized.

SEC. 306. DIGITAL CONTENT FORGERIES.

(a) Reports.—Not later than one year after the date of enactment of this Act, and annually thereafter, the Director of the National Institute of Standards and Technology shall publish a report regarding digital content forgeries.

(b) Requirements.—Each report under subsection (a) shall include the following—

(1) A definition of digital content forgeries along with accompanying explanatory materials. The definition developed pursuant to this section shall not supersede any other provision of law or be construed to limit the authority of any executive agency related to digital content forgeries;

(2) A description of the common sources in the United States of digital content forgeries and commercial sources of digital content forgery technologies;

(3) An assessment of the uses, applications, and harms of digital content forgeries;

(4) An analysis of the methods and standards available to identify digital content forgeries as well as a description of the commercial technological counter-measures that are, or could be, used to address concerns with digital content forgeries, which may include the provision of warnings to viewers of suspect content;

(5) A description of the types of digital content forgeries, including those used to commit fraud, cause harm or violate any provision of law; and

(6) Any other information determined appropriate by the Director.

SEC. 307. SEVERABILITY.

If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the remainder of this Act and the application of such provision to other persons not similarly situated or to other circumstances shall not be affected by the invalidation.

SEC. 308. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission such sums as may be necessary to carry out this Act.

Information Privacy Act (released June 3, 2020; updated December 7, 2020)

This document was drafted by Cameron F. Kerry and John B. Morris, Jr., in consultation with experts from academia, government, civil society, and industry. Cameron Kerry is the Ann R. and Andrew H. Tisch Distinguished Visiting Fellow in Governance Studies at The Brookings Institution, and John Morris is a Nonresident Senior Fellow at Brookings. For further information about the provisions in this document, please see the following two reports: "Bridging the gaps: A path forward to federal privacy legislation" and "Framing a privacy right: Legislative findings for federal privacy legislation."