[STATE] DATA PRIVACY AND PROTECTION ACT

SECTION 1. Short Title.

This Act may be cited as the "[State] Data Privacy and Protection Act".

SEC. 2. Definitions.

(a) In this Act:

(1) "**Affirmative express consent**" means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity, provided:

(A) The request is provided to the individual in a clear and conspicuous standalone disclosure made through the primary medium used to offer the covered entity's product or service, or only if the product or service is not offered in a medium that permits the making of the request under this paragraph, another medium regularly used in conjunction with the covered entity's product or service.

(B) The request includes a description of the processing purpose for which the individual's consent is sought and—

(i) clearly states the specific categories of covered data that the covered entity shall collect, process, and transfer necessary to effectuate the processing purpose; and

(ii) includes a prominent heading and is written in easy-to-understand language that would enable a reasonable individual to identify and understand the processing purpose for which consent is sought and the covered data to be collected, processed, or transferred by the covered entity for such processing purpose.

(C) The request clearly explains the individual's applicable rights related to consent.

(D) The request is made in a manner reasonably accessible to and usable by individuals with disabilities.

(E) The request is made available to the individual in each covered language in which the covered entity provides a product or service for which authorization is sought.

(F) The option to refuse consent shall be at least as prominent as the option to accept, and the option to refuse consent shall take the same number of steps or fewer as the option to accept.

(G) Processing or transferring any covered data collected pursuant to affirmative express consent for a different processing purpose than that for which affirmative express consent was obtained shall require affirmative express consent for the subsequent processing purpose.

(H) affirmative express consent to an act or practice is not inferred from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(I) Affirmative express consent is not obtained or attempted to be obtained through—

(i) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(ii) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data.

(2) **"Authentication"** means the process of verifying an individual or entity for security purposes.

(3) **"Biometric information"** means any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual. including, but is not limited to fingerprints; voice prints; iris or retina scans; facial or hand mapping, geometry, or templates; or gait or other unique body movements; provided, however, that "biometric information" does not include a digital or physical photograph; an audio or video recording; or data generated from a digital or physical photograph, or an audio or video recording, that cannot be used, alone or in combination with other information, to identify an individual.

(4) **"Collect"** and **"collection"** mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.

(5) **"Control"** means, with respect to an entity—

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

(B) control 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.

(6) **"Covered algorithm"** means a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision-making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual.

(7) **"Covered data"** means information, including derived data and unique identifiers, that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual; provided, however, that "covered data" does not include—

(A) de-identified data;

(B) employee data; or

(C) publicly available information.

(8) **"Covered entity"** means any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data. "Covered entity" includes any entity or person that controls, is controlled by, or is under common control with the covered entity. An entity shall not be considered to be a covered entity for purposes of this Act in so far as the entity is acting as a service provider. The term "covered entity" does not include—

(A) a Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district, agency, or political subdivision of the Federal Government or a State, Tribal, territorial, or local government;

(B) a person or an entity that is collecting, processing, or transferring covered data on behalf of a Federal, State, Tribal, territorial, or local government entity, in so far as such person or entity is acting as a service provider to the government entity; or

(C) an entity that serves as a congressionally designated nonprofit, national resource center, and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(9) **"Covered high-impact social media company"** means a covered entity that provides any internet-accessible platform where—

(A) such covered entity generates $3,000,000,000 or more in annual revenue;

(B) such platform has 300,000,000 or more monthly active users for not fewer than 3 of the preceding 12 months on the online product or service of such covered entity; and

(C) such platform constitutes an online product or service that is primarily used by users to access or share, user-generated content.

(10) **"Covered language"** means the ten languages with the most speakers in the United States, according to the most recent United States Census.

(11) **"Covered minor"** means an individual under the age of 17.

(12) **"Data broker"** means a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data; and does not include a covered entity insofar as such entity processes employee data collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third party providing benefits to the employee. An entity may not be considered to be a data broker for purposes of this Act if the entity is acting as a service provider.

(A) For purposes of this paragraph, the term "principal source of revenue" means, for the prior 12-month period, either—

(i) more than 50 percent of all revenue of the covered entity; or

(ii) obtaining revenue from processing or transferring the covered data of more than 5,000,000 individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data.

(13) "**De-identified data"** means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider—

(A) takes technical measures that ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;

(B) publicly commits in a clear and conspicuous manner—

(i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and

(ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and

(C) contractually obligates any person or entity that receives the information from the covered entity or service provider—

(i) to comply with all of the provisions of this paragraph with respect to the information; and

(ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.

(14) **"Derived data"** means covered data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about an individual or an individual's device.

(15) **"Device"** means any electronic equipment capable of collecting, processing, or transferring covered data that is used by one or more individuals.

(16) **"Employee"** means an individual who is an employee, director, officer, staff member, individual working as an independent contractor that is not a service provider, trainee, volunteer, or intern of an employer, regardless of whether such individual is paid, unpaid, or employed on a temporary basis.

(17) **"Employee data"** means—

(A) information relating to a job applicant collected by a covered entity acting as a prospective employer of such job applicant in the course of the application, or hiring process, if such information is collected, processed,

or transferred by the prospective employer solely for purposes related to the employee's status as a current or former job applicant of such employer;

(B) information processed by an employer relating to an employee who is acting in a professional capacity for the employer, provided that such information is collected, processed, or transferred solely for purposes related to such employee's professional activities on behalf of the employer;

(C) the business contact information of an employee, including the employee's name, position or title, business telephone number, business address, or business email address that is provided to an employee by an employer who is acting in a professional capacity, if such information is collected, processed, or transferred solely for purposes related to such employee's professional activities on behalf of the employer;

(D) emergency contact information collected by an employer that relates to an employee of that employer, if such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the employee and for processing or transferring such information in case of an emergency; or

(E) information relating to an employee (or a spouse, dependent, other covered family member, or beneficiary of such employee) that is necessary for the employer to collect, process, or transfer solely for the purpose of administering benefits to which such employee (or spouse, dependent, other covered family member, or beneficiary of such employee) is entitled on the basis of the employee's position with that employer.

(18) **"First party advertising or marketing"** means advertising or marketing conducted by a covered entity that collected covered data from the individual linked or reasonably linkable to that data through either direct communications with the individual such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by or on behalf of such covered entity, or on a web site or app operated by or on behalf of such covered entity.

(19) **"Genetic information"** means any covered data, regardless of its format, that concerns an individual's genetic characteristics, including—

(A) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid (DNA) of an individual; or

(B) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph (A).

(20) **"Individual"** means a natural person who is a [INSERT STATE] resident or present in [INSERT STATE].

(21) **"Knowledge"** means—

(A) with respect to a covered entity that is a covered high-impact social media company, the entity knew or should have known the individual was a covered minor;

(B) with respect to a covered entity or service provider that is a large data holder, and otherwise is not a covered high-impact social media company, that the covered entity knew or acted in willful disregard of the fact that the individual was a covered minor; and

(C) with respect to a covered entity or service provider that does not meet the requirements of clause (i) or (ii), actual knowledge.

(22) **"Large data holder"** means a covered entity or service provider that, in the most recent calendar year—

(A) had annual gross revenues of $250,000,000 or more; and

(B) collected, processed, or transferred the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; and the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals.

(C) "Large data holder" does not include any instance in which the covered entity or service provider would qualify as a large data holder solely on the basis of collecting or processing personal email addresses, personal telephone numbers, or log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity or service provider.

(23) **"Market research"** means the collection, processing, or transfer of covered data as reasonably necessary and proportionate to investigate the market for or marketing of products, services, or ideas, where the covered data is not integrated

into any product or service, otherwise used to contact any individual or individual's device, or used to advertise or market to any individual or individual's device.

(24) **"Material"** means, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to individuals) involving the collection, processing, or transfer of covered data, that such act, practice, or representation is likely to affect a reasonable individual's decision, conduct, or expectations regarding a product or service or processing of personal data.

(25) **"Precise geolocation information"** means information that is derived from a device or technology that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, with sufficient precision to identify street level location information of an individual or device or the location of an individual or device within a range of 1,850 feet or less; provided, however, that "precise geolocation information" does not include geolocation information identifiable or derived solely from the visual content of a legally obtained image, including the location of the device that captured such image.

(26) **"Process"** means to conduct or direct any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, storing, using, or otherwise handling covered data.

(27) **"Processing purpose"** means a reason for which a covered entity or service provider collects, processes, or transfers covered data that is specific and granular enough for a reasonable individual to understand the material facts of how and why the covered entity or service provider collects, processes, or transfers the covered data.

(28) **"Publicly available information"** means any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from Federal, State, or local government records, if the covered entity collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity; widely distributed media; a website or online service made available to all members of the public, for free or for a fee, including where all members of the public, for free or for a fee, can log in to the website or online service; a disclosure that has been made to the general public as required by Federal, State, or local law; or the visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession; provided, however, that for purposes of this paragraph,

information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience. "Publicly available information" does not include any obscene visual depiction (as defined in section 1460 of title 18, United States Code); any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual; biometric information; publicly available information that has been combined with covered data; genetic information, unless otherwise made available by the individual to whom the information pertains; or intimate images known to have been created or shared without consent.

(29) **"Revenue"**, with respect to any covered entity or service provider that is not organized to carry on business for its own profit or that of its members means the gross receipts the covered entity or service provider received, in whatever form, from all sources, without subtracting any costs or expenses; and includes contributions, gifts, grants, dues or other assessments, income from investments, and proceeds from the sale of real or personal property.

(30) **"Sensitive covered data"** means the following types of covered data:

(A) A government-issued identifier, such as a Social Security number, passport number, or driver's license number, that is not required by law to be displayed in public.

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

(C) A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual, except that the last four digits of a debit or credit card number shall not be deemed sensitive covered data.

(D) Biometric information.

(E) Genetic information.

(F) Precise geolocation information.

(G) An individual's private communications such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains to the transmission of such communications,

including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call, unless the covered entity or a service provider acting on behalf of the covered entity is the sender or an intended recipient of the communication. Communications are not private for purposes of this clause if such communications are made from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that such employer may access such communications.

(H) Account or device log-in credentials, or security or access codes for an account or device.

(I) Information identifying the sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of such information.

(J) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of whether such information is stored on the individual's device or is accessible from that device and is backed up in a separate location. Such information is not sensitive for purposes of this paragraph if such information is sent from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that it may access such information.

(K) A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.

(L) Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service described in 4(4). This clause does not include covered data used solely for transfers for independent video measurement.

(M) Information about an individual when the covered entity or service provider has knowledge that the individual is a covered minor.

(N) An individual's race, color, ethnicity, religion, or union membership.

(O) Information identifying an individual's online activities over time and across third party websites or online services.

(P) Any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data listed in clauses (i) through (xv).

(31) **"Service provider"** means a person or entity that collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity; and receives covered data from or on behalf of a covered entity or a Federal, State, Tribal, territorial, or local government entity. A service provider that receives service provider data from another service provider as permitted under this Act shall be treated as a service provider under this Act with respect to such data.

(32) **"Service provider data"** means covered data that is collected or processed by or has been transferred to a service provider by or on behalf of a covered entity, a Federal, State, Tribal, territorial, or local government entity, or another service provider for the purpose of allowing the service provider to whom such covered data is transferred to perform a service or function on behalf of, and at the direction of, such covered entity or Federal, State, Tribal, territorial, or local government entity.

(33) **"Small business"** means a covered entity or a service provider that meets the following criteria for the period of the 3 preceding calendar years (or for the period during which the covered entity or service provider has been in existence if such period is less than 3 years):

(A) The covered entity or service provider's average annual gross revenues during the period did not exceed $41,000,000;

(B) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy; and

(C) is not a data broker.

(34) **"Substantial privacy risk"** means the collection, processing, or transfer of covered data in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex, or disability.

(35) **"Targeted advertising"** means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device

identified by a unique identifier; provided, however that "targeted advertising" does not include: advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback; contextual advertising, which is when an advertisement is displayed based on the content or nature of the website or service in which the advertisement appears and does not vary based on who is viewing the advertisement; or processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.

(36) **"Third party"** means—

(A) any person or entity, including a covered entity, that—

(i) collects, processes, or transfers covered data and is not a consumer-facing business with which the individual linked or reasonably linkable to such covered data expects and intends to interact; and

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

(B) does not include a person or entity that collects covered data from another entity if the 2 entities are related by common ownership or corporate control, but only if a reasonable consumer's reasonable expectation would be that such entities share information.

(37) **"Third party data"** means covered data that has been transferred to a third party.

(38) **"Transfer"** means to disclose, release, disseminate, make available, license, rent, or share covered data orally, in writing, electronically, or by any other means.

(39) **"Unique identifier"** means an identifier to the extent that such identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, including a device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias, telephone number, or other form of persistent or probabilistic identifier that is linked or reasonably linkable to an individual or device; provided, however, that "unique identifier" does not include an identifier assigned by a covered entity for the specific and exclusive purpose of giving effect to an individual's exercise of affirmative express consent or opt-outs of the collection, processing, and transfer of covered data pursuant to this Act or otherwise limiting the collection, processing, or transfer of such information.

(40) **"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, but does not include an obscene visual depiction (as defined in section 1460 of title 18, United States Code).

Section 3. Data Minimization.

(a) A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to—

(1) provide or maintain a specific product or service requested by the individual to whom the data pertains; or

(2) effect a purpose permitted under subsection (b).

(b) A covered entity may collect, process, or transfer covered data for any of the following purposes if the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to such purpose:

(1) To initiate, manage, or complete a transaction or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account-servicing activity such as billing, shipping, delivery, storage, and accounting.

(2) With respect to covered data previously collected in accordance with this Act, notwithstanding this exception—

(A) to process such data as necessary to perform system maintenance or diagnostics;

(B) to develop, maintain, repair, or enhance a product or service for which such data was collected;

(C) to conduct internal research or analytics to improve a product or service for which such data was collected;

(D) to perform inventory management or reasonable network management;

(E) to protect against spam; or

(F) to debug or repair errors that impair the functionality of a service or product for which such data was collected.

(3) To authenticate users of a product or service.

(4) To fulfill a product or service warranty.

(5) To prevent, detect, protect against, or respond to a security incident. For purposes of this paragraph, security is defined as network security and physical security and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security.

(6) To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services. For purposes of this paragraph, the term "illegal activity" means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm.

(7) To comply with a legal obligation imposed by Federal, Tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider.

(8) To prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk.

(9) To effectuate a product recall pursuant to Federal or State law.

(10) To conduct a public or peer-reviewed scientific, historical, or statistical research project that—

(A) is in the public interest; and

(B) adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board.

(11) To deliver a communication that is not an advertisement to an individual, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity.

(12) To deliver a communication at the direction of an individual between such individual and one or more individuals or entities.

(13) To transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction when the third party assumes control, in whole or in part, of the covered entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides each affected individual with—

(A) a notice describing such transfer, including the name of the entity or entities receiving the individual's covered data and their privacy policies as described in section 7; and

(B) a reasonable opportunity to withdraw any previously given consents in accordance with the requirements of affirmative express consent under this Act related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data, as described in section 8.

(14) To ensure the data security and integrity of covered data, as described in section 13.

(15) to support or promote participation by individuals in civic engagement activities and democratic governance, including voting, petitioning, engaging with government proceedings, providing indigent legal aid services, and unionizing.

(16) With respect to covered data previously collected in accordance with this Act, to process such data as necessary to provide first party advertising or marketing of products or services provided by the covered entity for individuals who are not-covered minors.

(17) With respect to covered data previously collected in accordance with this Act, provided such collection, processing, and transferring complies with section 9(c), to provide targeted advertising.

(c) A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

(d) Nothing in this Act shall be construed to limit or diminish First Amendment freedoms guaranteed under the Constitution.

Section 4. Loyalty Duties.

Notwithstanding section 3 and unless an exception applies, with respect to covered data, a covered entity or service provider may not—

(a) collect, process, or transfer a Social Security number, except when necessary to facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by Federal, State, or local law;

(b) collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the

individual to whom the covered data pertains, or is strictly necessary to effect a purpose enumerated in paragraphs (1) through (12) and (14) through (15) of section 3(b);

(c) transfer an individual's sensitive covered data to a third party, unless—

(1) the transfer is made pursuant to the affirmative express consent of the individual;

(2) the transfer is necessary to comply with a legal obligation imposed by Federal, State, Tribal, or local law, or to establish, exercise, or defend legal claims;

(3) the transfer is necessary to prevent an individual from imminent injury where the covered entity believes in good faith that the individual is at risk of death, serious physical injury, or serious health risk;

(4) in the case of the transfer of a password, the transfer is necessary to use a designated password manager or is to a covered entity for the exclusive purpose of identifying passwords that are being re-used across sites or accounts;

(5) in the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an individual, or to conduct medical research in accordance with conditions of section 3(b)(10); or

(6) to transfer assets in the manner described in paragraph (13) of section 3(b); or

(d) in the case of a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming service described in section 713(h)(2) of the Communications Act of 1934 (47 U.S.C. 613(h)(2)), transfer to an unaffiliated third party covered data that reveals the video content or services requested or selected by an individual from such service, except with the affirmative express consent of the individual or pursuant to one of the permissible purposes enumerated in paragraphs (1) through (15) of section 3(b).

Section 5. Privacy By Design.

(a) A covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data and that—

(1) consider applicable Federal and state laws, rules, or regulations related to covered data the covered entity or service provider collects, processes, or transfers;

(2) identify, assess, and mitigate privacy risks related to covered minors to result in reasonably necessary and proportionate residual risk to covered minors;

(3) mitigate privacy risks, including substantial privacy risks, related to the products and services of the covered entity or the service provider, including in the design, development, and implementation of such products and services, taking into account the role of the covered entity or service provider and the information available to it; and

(4) implement reasonable training and safeguards within the covered entity and service provider to promote compliance with all privacy laws applicable to covered data the covered entity collects, processes, or transfers or covered data the service provider collects, processes, or transfers on behalf of the covered entity and mitigate privacy risks, including substantial privacy risks, taking into account the role of the covered entity or service provider and the information available to it.

(b) The policies, practices, and procedures established by a covered entity and a service provider under subsection (a), shall correspond with, as applicable—

(1) the size of the covered entity or the service provider and the nature, scope, and complexity of the activities engaged in by the covered entity or service provider, including whether the covered entity or service provider is a large data holder, nonprofit organization, small business, third party, or data broker, taking into account the role of the covered entity or service provider and the information available to it;

(2) the sensitivity of the covered data collected, processed, or transferred by the covered entity or service provider;

(3) the volume of covered data collected, processed, or transferred by the covered entity or service provider;

(4) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity or service provider relates; and

(5) the cost of implementing such policies, practices, and procedures in relation to the risks and nature of the covered data.

Section 6. Prohibition on Retaliation Against an Individual for Exercise of Rights.

(a) A covered entity may not retaliate against an individual for exercising any of the rights guaranteed by the Act, or any regulations promulgated under this Act, or for refusing to agree to collection or processing of covered data for a separate product or service, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

(b) Nothing in subsection (a) may be construed to—

(1) prohibit the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and processed only for the purpose of initiating, rendering, billing for, or collecting payment for a service or product requested by the individual;

(2) prohibit a covered entity from offering a different price, rate, level, quality or selection of goods or services to an individual, including offering goods or services for no fee, if the offering is in connection with an individual's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program, provided that the covered entity may not transfer covered data to a third-party as part of such a program unless:

(A) The transfer is reasonably necessary to enable the third party to provide a benefit to which the individual is entitled;

(B) the transfer of covered data to third parties is clearly disclosed in the terms of the program; and

(C) the third party uses the covered data only for purposes of facilitating such a benefit to which the individual is entitled and does not retain or otherwise use or disclose the covered data for any other purpose.

(3) require a covered entity to provide a bona fide loyalty program that would require the covered entity to collect, process, or transfer covered data that the covered entity otherwise would not collect, process, or transfer;

(4) prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in market research;

(5) prohibit a covered entity from offering different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a right under section 8(a)(3); or

(6) prohibit a covered entity from declining to provide a product or service insofar as the collection and processing of covered data is strictly necessary for such product or service.

(c) Notwithstanding the provisions in this subsection, no covered entity may offer different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

Section 7. Transparency.

(a) Each covered entity and service provider shall make publicly available, in a clear, conspicuous, not misleading, and easy-to-read and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity. The policy must be provided in a manner that is reasonably accessible to and usable by individuals with disabilities. The policy shall be made available to the public in each covered language in which the covered entity or service provider provides a product or service that is subject to the privacy policy; or carries out activities related to such product or service. The policy must include, at a minimum, the following:

(1) The identity and the contact information of—

(A) the covered entity or service provider to which the privacy policy applies (including the covered entity's or service provider's points of contact and generic electronic mail addresses, as applicable for privacy and data security inquiries); and

(B) any other entity within the same corporate structure as the covered entity or service provider to which covered data is transferred by the covered entity.

(2) The categories of covered data the covered entity or service provider collects or processes.

(3) The processing purposes for each category of covered data the covered entity or service provider collects or processes.

(4) Whether the covered entity or service provider transfers covered data and, if so, each category of service provider and third party to which the covered entity or service provider transfers covered data, the name of each data broker to which the covered entity or service provider transfers covered data, and the purposes for which such data is transferred to such categories of service providers and third parties or third-party collecting entities, except for a transfer to a governmental entity pursuant to a court order or law that prohibits the covered entity or service provider from disclosing such transfer.

(5) The length of time the covered entity or service provider intends to retain each category of covered data, including sensitive covered data, or, if it is not possible to identify that timeframe, the criteria used to determine the length of time the covered entity or service provider intends to retain categories of covered data.

(6) A prominent description of how an individual can exercise the rights described in this Act.

(7) A general description of the covered entity's or service provider's data security practices.

(8) The effective date of the privacy policy.

(b) If a covered entity makes a material change to its privacy policy or practices, the covered entity shall notify each individual affected by such material change before implementing the material change with respect to any prospectively collected covered data and, except as provided in paragraphs (1) through (15) of section 3(b), provide a reasonable opportunity for each individual to withdraw consent to any further materially different collection, processing, or transfer of previously collected covered data under the changed policy. The covered entity shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy policy to each affected individual, in each covered language in which the privacy policy is made available, and taking into account available technology and the nature of the relationship. Nothing in this section may be construed to affect the requirements for covered entities under section 4 or 6.

(c) Each large data holder shall retain copies of previous versions of its privacy policy for at least 10 years beginning after the date of enactment of this Act and publish them on its website. Such large data holder shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of each material change to its privacy policy over the past 10 years. The descriptions shall be sufficient for a reasonable individual to understand the material effect of each material change. The obligations in this paragraph shall not apply to any previous versions of a large data holder's privacy policy, or any material changes to such policy, that precede the date of enactment of this Act.

(d) In addition to the privacy policy required under subsection (a), a large data holder that is a covered entity shall provide a short-form notice of its covered data practices in a manner that is—

(1) concise, clear, conspicuous, and not misleading;

(2) readily accessible to the individual, based on what is reasonably anticipated within the context of the relationship between the individual and the large data holder;

(3) inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data; and

(4) no more than 500 words in length.

Section 8. Individual Data Rights.

(a) In accordance with subsections (b) and (c), a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to—

(1) access—

(A) in a human-readable format that a reasonable individual can understand and download from the internet, the covered data (except covered data in a back-up or archival system) of the individual making the request that is collected, processed, or transferred by the covered entity or any service provider of the covered entity within the 24 months preceding the request;

(B) the categories of any third party, if applicable, and an option for consumers to obtain the names of any such third party as well as and the categories of any service providers to whom the covered entity has transferred for consideration the covered data of the individual, as well as the categories of sources from which the covered data was collected; and

(C) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;

(2) correct any verifiable substantial inaccuracy or substantially incomplete information with respect to the covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the corrected information;

(3) delete covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the individual's deletion request; and

(4) to the extent technically feasible, export to the individual or directly to another entity the covered data of the individual that is processed by the covered entity, including inferences linked or reasonably linkable to the individual but not including other derived data, without licensing restrictions that limit such transfers in—

(A) a human-readable format that a reasonable individual can understand and download from the internet; and

(B) a portable, structured, interoperable, and machine-readable format.

(b) A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in subsection (a) through—

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise such right.

(c) Subject to subsections (d) and (e), each request under subsection (a) shall be completed by any—

(1) large data holder within 45 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual;

(2) covered entity that is not a large data holder within 60 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual; or

(3) a response period set forth in this subsection may be extended once by 45 additional days when reasonably necessary, considering the complexity and number of the individual's requests, so long as the covered entity informs the individual of any such extension within the initial 45-day response period, together with the reason for the extension.

(d) A covered entity shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and with respect to the first 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a reasonable fee for each request.

(e) A covered entity may not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity—

(1) cannot reasonably verify that the individual making the request to exercise the right is the individual whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf;

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

(3) determines that the exercise of the right would require access to or correction of another individual's sensitive covered data;

(4) reasonably believes that the exercise of the right would require the covered entity to engage in an unfair or deceptive practice under section 5 of the Federal Trade Commission Act (15 U.S.C. 45) [or specific applicable state law]; or

(5) reasonably believes that the request is made to further fraud, support criminal activity, or the exercise of the right presents a data security threat.

(f) If a covered entity cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity—

(1) may request that the individual making the request to exercise the right provide any additional information necessary for the sole purpose of verifying the identity of the individual; and

(2) may not process or transfer such additional information for any other purpose.

(g) A covered entity may decline, with adequate explanation to the individual, to comply with a request to exercise a right described in subsection (a), in whole or in part, that would—

(1) require the covered entity to retain any covered data collected for a single, one-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction;

(2) be demonstrably impracticable or prohibitively costly to comply with, and the covered entity shall provide a description to the requestor detailing the inability to comply with the request;

(3) require the covered entity to attempt to re-identify de-identified data;

(4) require the covered entity to maintain covered data in an identifiable form or collect, retain, or access any data in order to be capable of associating a verified individual request with covered data of such individual;

(5) result in the release of trade secrets or other privileged or confidential business information;

(6) require the covered entity to correct any covered data that cannot be reasonably verified as being inaccurate or incomplete;

(7) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, prevent, or investigate fraudulent, malicious, or unlawful activity, or enforce valid contracts;

(8) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States;

(9) prevent a covered entity from being able to maintain a confidential record of deletion requests, maintained solely for the purpose of preventing covered data of an individual from being recollected after the individual submitted a deletion request and requested that the covered entity no longer collect, process, or transfer such data;

(10) fall within an exception enumerated in the regulations promulgated under this Act; or

(11) with respect to requests for deletion—

(A) unreasonably interfere with the provision of products or services by the covered entity to another person it currently serves;

(B) delete covered data that relates to a public figure and for which the requesting individual has no reasonable expectation of privacy;

(C) delete covered data reasonably necessary to perform a contract between the covered entity and the individual;

(D) delete covered data that the covered entity needs to retain in order to comply with professional ethical obligations;

(E) delete covered data that the covered entity reasonably believes may be evidence of unlawful activity or an abuse of the covered entity's products or services; or

(F) for private elementary and secondary schools as defined by State law and private institutions of higher education as defined by title I of the Higher Education Act of 1965, delete covered data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(h) In a circumstance that would allow a denial, a covered entity shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so.

(i) For purposes of subsection (g)(ii), the receipt of a large number of verified requests, on its own, may not be considered to render compliance with a request demonstrably impracticable.

(j) LARGE DATA HOLDER METRICS REPORTING.—A large data holder that is a covered entity shall, for each calendar year in which it was a large data holder, do the following:

(1) Compile the following metrics for the prior calendar year:

(A) The number of verified access requests under subsection (a)(1).

(B) The number of verified deletion requests under subsection (a)(3).

(C) The number of requests to opt-out of covered data transfers under section 204(b).

(D) The number of requests to opt-out of targeted advertising under section 204(c).

(E) The number of requests in each of subparagraphs (A) through (D) that such large data holder (i) complied with in whole or in part and (ii) denied.

(F) The median or mean number of days within which such large data holder substantively responded to the requests in each of subparagraphs (A) through (D).

(2) Disclose by July 1 of each applicable calendar year the information compiled in paragraph (1) within such large data holder's privacy policy required under section 202 or on the publicly accessible website of such large data holder that is accessible from a hyperlink included in the privacy policy.

(k) A covered entity shall facilitate the ability of individuals to make requests under this section in any covered language in which the covered entity provides a product or service. The mechanisms by which a covered entity enables individuals to make requests under this section shall be readily accessible and usable by individuals with disabilities.

Section 9. Right to Consent, Object, and Opt Out.

(a) A covered entity shall provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided by the individual that is as easy to execute by a reasonable individual as the means to provide consent, with respect to the processing or transfer of the covered data of the individual.

(b) A covered entity may not transfer or direct the transfer of the covered data of an individual to a third party if the individual objects to the transfer; and shall allow an individual to object to such a transfer through an optout mechanism.

(1) A covered entity need not allow an individual to opt out of the collection, processing, or transfer of covered data made pursuant to the exceptions in paragraphs (1) through (15) of section 3(b).

(c) A covered entity or service provider that directly delivers a targeted advertisement shall prior to engaging in targeted advertising to an individual or device and at all times thereafter, provide such individual with a clear and conspicuous means to opt out of targeted advertising; abide by any opt-out designation by an individual with respect to targeted advertising and notify the covered entity that directed the service provider to deliver the targeted advertisement of the opt-out decision; and allow an individual to make an opt-out designation with respect to targeted advertising through an opt-out mechanism.

(1) A covered entity or service provider that receives an opt-out notification pursuant to this section shall abide by such opt-out designations by an individual and notify any other person that directed the covered entity or service provider to serve, deliver, or otherwise handle the advertisement of the opt-out decision.

(d) A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this section through—

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise any such right.

Section 10. Data Protections for Children and Minors.

(a) A covered entity may not engage in targeted advertising to any individual if the covered entity has knowledge that the individual is a covered minor.

(b) A covered entity may not transfer or direct the transfer of the covered data of a covered minor to a third party if the covered entity has knowledge that the individual is a covered minor; and has not obtained affirmative express consent from the covered minor or the covered minor's parent or guardian; provided, however, that a covered entity or service provider may collect, process, or transfer covered data of an individual the covered entity or service provider knows is under the age of 18 solely in order to submit information relating to child victimization to law enforcement or to the nonprofit, national resource center and clearinghouse congressionally designated to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

Section 11. Data Brokers.

(a) Each data broker shall place a clear, conspicuous, not misleading, and readily accessible notice on the website or mobile application of the data broker (if the data broker maintains such a website or mobile application) that notifies individuals that the entity is a data broker and includes a link to the website established under this section.

(b) Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker and processed covered data pertaining to more than 5,000 individuals or devices that identify or are linked or reasonably linkable to an individual, such covered entity shall register with the Attorney General in accordance with this subsection. In registering with the Attorney General, a data broker shall do the following:

(1) Pay to the Attorney General a registration fee of $100.

(2) Provide the Attorney General with the following information:

(A) The legal name and primary physical, email, and internet addresses of the data broker.

(B) A description of the categories of covered data the data broker processes and transfers.

(C) The contact information of the data broker, including a contact person, a telephone number, an e-mail address, a website, and a physical mailing address.

(D) A link to a website through which an individual may easily exercise the rights provided under this Act.

(i) The Attorney General shall establish and maintain on a website a searchable, publicly available, central registry of data brokers that are registered with the Attorney General.

(c) A data broker that fails to register or provide the notice as required under this section shall be liable for—

(1) a civil penalty of $100 for each day the data broker fails to register or provide notice as required under this section, not to exceed a total of $10,000 for any year; and

(2) an amount equal to the registration fees due under this section for each year that the data broker failed to register as required pursuant to this section.

Section 12. Civil Rights and Algorithms.

(a) A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability. This does not apply to:

(1) the collection, processing, or transfer of covered data for the purpose of—

(A) a covered entity's or a service provider's self-testing to prevent or mitigate unlawful discrimination; or

(B) diversifying an applicant, participant, or customer pool; or

(2) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).

(b) Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, and annually thereafter, a covered entity that is not a small business and that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group of individuals, and uses such covered algorithm solely or in part, to collect, process, or transfer covered data shall conduct an impact assessment of such algorithm. The impact assessment shall provide the following information:

(1) A detailed description of the design process and methodologies of the covered algorithm.

(2) A statement of the purpose and reasonably foreseeable uses of the covered algorithm.

(3) The types of data used by the covered algorithm, including the specific categories and sources of data that will be processed as input and any data used to train the model that the covered algorithm relies on, if applicable.

(4) A description of the outputs produced by the covered algorithm.

(5) An assessment of the necessity and proportionality of the covered algorithm in relation to its stated purpose.

(6) A detailed description of steps the covered entity has taken or will take to mitigate potential harms from the covered algorithm to an individual or group of individuals, including related to—

(A) covered minors;

(B) making or facilitating advertising for, or determining access to, or restrictions on the use of housing, education, employment, healthcare, insurance, or credit opportunities;

(C) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of individuals, including race, color, religion, national origin, sex, or disability;

(D) disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability status; or

(E) disparate impact on the basis of individuals' political party registration status.

(F) Any other information as required by regulations issued by the Attorney General.

(c) Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, a covered entity or service provider that knowingly develops a covered algorithm that is designed, solely or in part, to collect, process, or transfer covered data in furtherance of a consequential decision shall prior to deploying the covered algorithm perform an algorithmic design evaluation to evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under this section.

(d) In complying with this section, a covered entity and a service provider may focus the impact assessment or evaluation on any covered algorithm, or portions of a covered algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms identified under this section.

(e) A covered entity and a service provider shall, not later than 30 days after completing an impact assessment or evaluation, submit the impact assessment or evaluation conducted under paragraph (1) or (2) to the Attorney General; and shall make a summary of such impact assessment and evaluation publicly available in a place that is easily accessible to individuals. Covered entities and service providers may redact and segregate any trade secret (as defined in section 1839 of title 18, United States Code) or other confidential or proprietary information from public disclosure under this subparagraph.

Section 13. Data Security and Protection of Covered Data.

(a) A covered entity or service provider shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and

secure covered data against unauthorized access and acquisition. The practices shall be appropriate to—

(1) the size and complexity of the covered entity or service provider;

(2) the nature and scope of the covered entity or the service provider's collecting, processing, or transferring of covered data;

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

(4) the sensitivity of the covered data collected, processed, or transferred;

(5) the current state of the art (and limitations thereof) in administrative, technical, and physical safeguards for protecting such covered data; and

(6) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such covered data in relation to the risks and nature of the covered data.

(b) The data security practices of the covered entity and of the service provider required under subsection (a) shall include, for each respective entity's own system or systems, at a minimum, the following practices:

(1) Identifying and assessing any material internal and external risk to, and vulnerability in, the security of each system maintained by the covered entity that collects, processes, or transfers covered data, or service provider that collects, processes, or transfers covered data on behalf of the covered entity, including unauthorized access to or risks to such covered data, human vulnerabilities, access rights, and the use of service providers.

With respect to large data holders, such activities shall include a plan to receive and reasonably respond to unsolicited reports of vulnerabilities by any entity or individual and by performing a reasonable investigation of such reports.

(2) Taking preventive and corrective action designed to mitigate reasonably foreseeable risks or vulnerabilities to covered data identified by the covered entity or service provider, consistent with the nature of such risk or vulnerability and the entity's role in collecting, processing, or transferring the data. Such action may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software, among other actions.

(3) Disposing of covered data in accordance with a retention schedule that shall require the deletion of covered data when such data is required to be deleted by

law or is no longer necessary for the purpose for which the data was collected, processed, or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section. Service providers shall establish practices to delete or return covered data to a covered entity as requested at the end of the provision of services unless retention of the covered data is required by law, consistent with this Act.

(4) Training each employee with access to covered data on how to safeguard covered data and updating such training as necessary.

(5) Designating an officer, employee, or employees to maintain and implement such practices.

(6) Implementing procedures to detect, respond to, or recover from security incidents, including breaches.

Section 14. Small Business Protections.

(a) Any small business shall—

(1) be exempt from compliance with section 8(a)(4) and paragraphs (1) through (2) and (4) through (6) of section 13(b); and

(2) at the small business' sole discretion, have the option of complying with section 8(a)(2) by, after receiving a verified request from an individual to correct covered data of the individual under such section, deleting such covered data in its entirety instead of making the requested correction.

Section 15. Executive Responsibility.

(a) Beginning 1 year after the date of enactment of this Act, an executive officer of a large data holder shall annually certify, in good faith, to the Attorney General that the entity maintains—

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

(2) internal reporting structures to ensure that such certifying executive officer is involved in and responsible for the decisions that impact the compliance by the large data holder with this Act.

(b) A certification submitted under subsection (a) shall be based on a review of the effectiveness of the internal controls and reporting structures of the large data holder that is conducted by the certifying executive officer not more than 90 days before the submission

of the certification. A certification submitted under subsection (a) is made in good faith if the certifying officer had, after a reasonable investigation, reasonable ground to believe and did believe, at the time that certification was submitted, that the statements therein were true and that there was no omission to state a material fact required to be stated therein or necessary to make the statements therein not misleading.

(c) A covered entity or service provider that is not a small business shall designate 1 or more qualified employees as privacy officers; and 1 or more qualified employees as data security officers.

(1) An employee who is designated by a covered entity or a service provider as a privacy officer or a data security officer shall, at a minimum—

(A) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this Act; and

(B) facilitate the covered entity or service provider's ongoing compliance with this Act.

(2) A large data holder shall designate at least 1 of the officers described in subsection (c) to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the requirements in subparagraph (1), either directly or through a supervised designee or designees—

(A) establish processes to periodically review and update the privacy and security policies, practices, and procedures of the large data holder, as necessary;

(B) conduct biennial and comprehensive audits to ensure the policies, practices, and procedures of the large data holder ensure the large data holder is in compliance with this Act and ensure such audits are accessible to the Attorney General upon request;

(C) develop a program to educate and train employees about compliance requirements of this Act;

(D) maintain updated, accurate, clear, and understandable records of all material privacy and data security practices undertaken by the large data holder; and

(E) serve as the point of contact between the large data holder and enforcement authorities.

(d) Not later than 1 year after the date of enactment of this Act and biennially thereafter, each covered entity that is not a small business shall conduct a privacy impact assessment. Such assessment shall weigh the benefits of the covered entity's covered data collecting, processing, and transfer practices that may cause a substantial privacy risk against the potential material adverse consequences of such practices to individual privacy. The covered entity shall make a summary of such privacy impact assessment publicly available in a place that is easily accessible to individuals. The privacy impact assessment shall —

(1) be reasonable and appropriate in scope given—

(A) the nature of the covered data collected, processed, and transferred by the covered entity;

(B) the volume of the covered data collected, processed, and transferred by the covered entity; and

(C) the potential risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the covered entity;

(2) be documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under paragraph (1);

(3) include additional information required by regulations issued by the Attorney General;

(4) upon request, make such impact assessments available to the Attorney General; and

(5) if the covered entity is a large data holder, be approved by the privacy protection officer designated in this section, as applicable.

Section 16. Service Providers and Third Parties.

(a) A service provider—

(1) shall adhere to the instructions of a covered entity and only collect, process, and transfer service provider data to the extent necessary and proportionate to provide a service requested by the covered entity, as set out in the contract required by subsection (b), and this paragraph does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

(2) may not collect, process, or transfer service provider data if the service provider has actual knowledge that a covered entity violated this Act with respect to such data;

(3) shall assist a covered entity in responding to a request made by an individual under section 8 or 9, by either—

(A) providing appropriate technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the service provider, for the covered entity to comply with such request for service provider data; or

(B) fulfilling a request by a covered entity to execute an individual rights request that the covered entity has determined should be complied with, by either—

(i) complying with the request pursuant to the covered entity's instructions; or

(ii) providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception to section 8 or 9;

(4) may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing that covered entity with notice and pursuant to a written contract that requires such other service provider to satisfy the obligations of the service provider with respect to such service provider data, including that the other service provider be treated as a service provider under this Act;

(5) shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the compliance of the service provider with the requirements of this Act, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the service provider and the covered entity, providing information necessary to enable the covered entity to conduct and document a privacy impact assessments required this Act, and making available the algorithmic design evaluation required under section 12(b)(2);

(6) shall, at the covered entity's direction, delete or return all covered data to the covered entity as requested at the end of the provision of services, unless retention of the covered data is required by law;

(7) shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and confidentiality of covered data the service provider processes consistent with section 13; and

(8) shall allow and cooperate with, reasonable assessments by the covered entity or the covered entity's designated assessor; alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the service provider's policies and technical and organizational measures in support of the obligations under this Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The service provider shall provide a report of such assessment to the covered entity upon request.

(b) A person or entity may only act as a service provider pursuant to a written contract between the covered entity and the service provider, or a written contract between one service provider and a second service provider as described under subsection (a)(4), if the contract—

(1) sets forth the data processing procedures of the service provider with respect to collection, processing, or transfer performed on behalf of the covered entity or service provider;

(2) clearly sets forth—

(A) instructions for collecting, processing, or transferring data;

(B) the nature and purpose of collecting, processing, or transferring;

(C) the type of data subject to collecting, processing, or transferring;

(D) the duration of processing; and

(E) the rights and obligations of both parties, including a method by which the service provider shall notify the covered entity of material changes to its privacy practices;

(3) does not relieve a covered entity or a service provider of any requirement or liability imposed on such covered entity or service provider under this Act; and

(4) prohibits—

(A) collecting, processing, or transferring covered data in contravention to subsection (a); and

(B) combining service provider data with covered data which the service provider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, provided that such combining is not necessary to effectuate a purpose

described in paragraphs (1) through (15) of section 3(b) and is otherwise permitted under the contract required by this subsection.

(5) Each service provider shall retain copies of previous contracts entered into in compliance with this section with each covered entity to which it provides requested products or services.

(c) Relationship between covered entities and service providers.—

(1) Determining whether a person is acting as a covered entity or service provider with respect to a specific processing of covered data is a fact-based determination that depends upon the context in which such data is processed.

(2) A person that is not limited in its processing of covered data pursuant to the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and not a service provider with respect to a specific processing of covered data. A service provider that continues to adhere to the instructions of a covered entity with respect to a specific processing of covered data remains a service provider. If a service provider begins, alone or jointly with others, determining the purposes and means of the processing of covered data, it is a covered entity and not a service provider with respect to the processing of such data.

(3) A covered entity that transfers covered data to a service provider or a service provider that transfers covered data to a covered entity or another service provider, in compliance with the requirements of this Act, is not liable for a violation of this Act by the service provider or covered entity to whom such covered data was transferred, if at the time of transferring such covered data, the covered entity or service provider did not have actual knowledge that the service provider or covered entity would violate this Act.

(4) A covered entity or service provider that receives covered data in compliance with the requirements of this Act is not in violation of this Act as a result of a violation by a covered entity or service provider from which such data was received.

(d) A third party—

(1) shall not process third party data for a processing purpose other than, in the case of sensitive covered data, the processing purpose for which the individual gave affirmative express consent or to effect a purpose enumerated in paragraph (1), (3), or (5) of section 3(b) and, in the case of non-sensitive data, the processing purpose for which the covered entity made a disclosure pursuant to section 7(a)(4);

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third party data if the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) shall enter into and comply with all provisions of the contract required under subsection (e).

(e) A covered entity that transfers covered data to a third party shall enter into a written contract with such third party that —

(1) identifies the specific purposes for which the covered data is being made available to third party;

(2) specifies that the covered entity is transferring the covered data to the third party solely for the specific purposes set forth in the contract and that the third party may only use the covered data for such specific purposes;

(3) requires the third party to comply with all applicable provisions of and regulations promulgated under this Act with respect to the covered data that the covered entity transfers to the third party and must provide the same level of privacy and security protection for the covered data as required by covered entities under this Act.

(f) A covered entity or service provider shall exercise reasonable due diligence in—

(1) selecting a service provider; and

(2) deciding to transfer covered data to a third party.

(g) Solely for the purposes of this section, the requirements for service providers to contract with, assist, and follow the instructions of covered entities shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the service provider is providing a service to a government entity.

Section 17. Enforcement.

(a) The Attorney General, District Attorney, or a City Corporation Counsel may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State, against any covered entity or service provider that violated this Act to—

(1) enjoin such act or practice;

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

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

(4) obtain reasonable attorneys' fees and other litigation costs reasonably incurred.

Section 18. Enforcement by Persons.

(a) Beginning on the date that is 2 years after the date on which this Act takes effect, any person or class of persons subject to a violation of this Act or a regulation promulgated under this Act by a covered entity or service provider may bring a civil action against such entity in any court of competent jurisdiction.

(b) In a civil action brought under paragraph (a) in which a plaintiff prevails, the court may award the plaintiff—

(1) an amount equal to the sum of any compensatory damages;

(2) injunctive relief;

(3) declaratory relief; and

(4) reasonable attorney's fees and litigation costs.

(c) With respect to a claim under this section for injunctive relief, such claim may be brought by a person or class of persons if—prior to initiating any action against a covered entity for injunctive relief—the person or class or persons provides to the covered entity or service provider 30 days' written notice identifying the specific provisions of this Act the person or class of persons alleges have been or are being violated. The notice described shall not apply more than once to any alleged underlying violation by the same covered entity.

In the event a cure is possible, if within the 30 days the covered entity or service provider actually cures the noticed violation or violations and provides the person or class of persons an express written statement that the violation or violations has been cured and that no further violations shall occur, no action for injunctive relief for such violation may be initiated against the covered entity. The dismissal shall not apply more than once to any alleged underlying violation by the same covered entity.

(d) This section shall only apply to a claim alleging a violation of section 4, 6, 7, 8, 9, 10, 11(b)(3)(C), 12(a), 13(a), or 16, or a regulation promulgated under any such section.

(e) This section shall not apply to any claim against a small business.

Section 19. Relationship to Federal and State Laws.

(a) A covered entity or service provider 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.), the Fair Credit Reporting Act (15 U.S.C. 1681et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; part 99 of title 34, Code of Federal Regulations) to the extent such covered entity is a school as defined in 20 U.S.C. 1232g(a)(3) or 34 C.F.R. 99.1(a), section 444 of the General Education Provisions Act (commonly known as the "Family Educational Rights and Privacy Act of 1974") (20 U.S.C. 1232g) and part 99 of title 34, Code of Federal Regulations (or any successor regulation), the Confidentiality of Alcohol and Drug Abuse Patient Records at 42 U.S.C. 290dd-2 and its implementing regulations at 42 CFR part 2, the Genetic Information Non-discrimination Act (GINA), 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 data privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this Act, except for section 13, solely and exclusively with respect to data subject to the requirements of such regulations, part, title, or Act.

(b) A covered entity or service provider 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 13, solely and exclusively with respect to data subject to the requirements of such regulations, part, title, or Act.

Section 20. 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.

Section 21. Rulemaking.

(a) The Attorney General may promulgate rules for the purposes of carrying out this Act, including, but not limited to the following areas:

(1) adjusting the monetary thresholds in January of every odd-numbered year to reflect any increase in the Consumer Price Index, and the data collected thresholds in the definition of "large data holder" and "small business" as appropriate;

(2) further defining "precise geolocation information," such as where the size defined is not sufficient to protect individual privacy in sparsely populated areas, or when the covered data is used for normal operational purposes, such as billing;

(3) updating or adding categories to the definition of "sensitive covered data" any other type of covered data that may require a similar level of protection as the types of covered data listed in the definition of "sensitive covered data" as a result of any new method of collecting, processing, or transferring covered data;

(4) further defining and adding to the permissible purposes under section 3(b) for which covered entities and service providers may use covered data, as long as such purposes are consistent with the reasonable expectations of individuals;

(5) further defining what constitutes reasonable policies, practices, and procedures under section 5;

(6) establishing processes by which covered entities are to comply with the provisions of section 8. Such regulations may take into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by the covered entity, including whether the covered entity is a large data holder, nonprofit organization, small business, third party, or data broker;

(B) the sensitivity of covered data collected, processed, or transferred by the covered entity;

(C) the volume of covered data collected, processed, or transferred by the covered entity;

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates; and

(E) standards for ensuring the deletion of covered data under this Act where appropriate.

(7) establishing rules and procedures to further the purposes of section 8 and to facilitate an individual's or the individual's authorized agent's ability to delete covered data, correct inaccurate covered data, or obtain covered data, with the goal of minimizing the administrative burden on individuals, taking into account available technology, security concerns, and the burden on the covered entity, to govern a covered entity's determination that a request for information received by from an individual is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the individual with

the covered entity while the individual is logged into the account as a verifiable request and providing a mechanism for an individual who does not maintain an account with the covered entity to request information through the covered entity's authentication of the individual's identity;

(8) establishing additional permissive exceptions necessary to protect the rights of individuals, prevent unjust or unreasonable outcomes from the exercise of access, correction, deletion, or portability rights, or as otherwise necessary to fulfill the purposes of this section. In establishing such exceptions, the Attorney General should consider any relevant changes in technology, means for protecting privacy and other rights, and beneficial uses of covered data by covered entities;

(9) establishing how often, and under what circumstances, an individual may request a correction pursuant to Section 8;

(10) the development and use of a recognizable and uniform opt-out logo or button by all covered entities to promote awareness of the opportunity to opt out of targeted advertising and transfers to third parties;

(11) requiring covered entities obligated to conduct impact assessments under section 12(b) or 15(d) to establish a process to ensure that audits are thorough and independent;

(12) requiring additional information necessary for compliance with the impact assessments required under sections 12(b) and 15(d);

(13) excluding from the algorithmic impact assessments required under section 12(b) any covered algorithm that presents low or minimal consequential risk of harm to an individual or group of individuals;

(14) setting compliance requirements for service providers and third parties under section 16;

(b) By July 1, 2024, the Attorney General shall establish or recognize one or more acceptable privacy protective, centralized mechanisms, including global privacy signals such as browser or device privacy settings, other tools offered by covered entities or service providers, and registries of identifiers, for individuals to exercise all rights enumerated in section 9 through a single interface for a covered entity or service provider to utilize to allow an individual to make such opt out designations with respect to covered data related to such individual. Any such centralized opt-out mechanism shall—

(1) require covered entities or service providers acting on behalf of covered entities to inform individuals about the centralized opt-out choice;

(2) not be required to be the default setting, but may be the default setting provided that in all cases the mechanism clearly represents the individual's affirmative, freely given, and unambiguous choice to opt out;

(3) be consumer-friendly, clearly described, and easy-to-use by a reasonable individual;

(4) be provided in any covered language in which the covered entity provides products or services subject to the opt-out; and

(5) be provided in a manner that is reasonably accessible to and usable by individuals with disabilities.

Section 22. Effective Date.

This Act shall take effect on the date that is 180 days after the date of enactment of this Act.