H.812

Introduced by Representative Priestley of Bradford

Referred to Committee on

Date:

Subject: Commerce and trade; privacy; data loyalty

Statement of purpose of bill as introduced: This bill proposes to increase privacy protections and data security by regulating how certain businesses store, share, and sell the personal data of Vermont consumers.

An act relating to data loyalty

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 9 V.S.A. chapter 61A is added to read:

CHAPTER 61A. DATA LOYALTY

§ 2411a. SHORT TITLE AND DEFINITIONS

(a) This chapter shall be known, and may be cited, as the "Vermont Duty of Data Loyalty Act."

(b) As used in this chapter:

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

(2)(A) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a

fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual.

(B) "Biometric data" does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

(iii) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(3) "Collect" and "collection" mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means, which includes receiving information from the consumer either actively, through interactions such as user registration, or passively, by observing the consumer's behavior.

(4) "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.

(5) "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.

(6)(A) "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.

(B) "Covered data" does not include:

(i) deidentified data;

(ii) employee data; or

(iii) public information.

(7)(A) "Covered entity" means a person, other than an individual acting in a noncommercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data.

(B) "Covered entity" includes a person that controls, is controlled by, or is under common control with the covered entity. A person shall not be

considered to be a covered entity for purposes of this chapter insofar as the person is acting as a service provider.

(C) "Covered entity" does not include:

(i) a federal, state, tribal, territorial, or local government entity, including a body, authority, board, bureau, commission, district, agency, or political subdivision of the federal government or state, tribal, territorial, or local government;

(ii) a person that is collecting, processing, or transferring covered data on behalf of a federal, state, tribal, territorial, or local government entity, insofar as the person is acting as a service provider to the government entity;

(iii) a person 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; or

(iv) a small business.

(8) "Covered language" means the 10 most common languages spoken in the United States, according to the most recent U.S. Census.

(9) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's covered data obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website,

application, or service with which the consumer intentionally interacts. Cross-context behavioral advertising includes retargeting, the use of "look-alike" consumer behavioral profiles, and the use of first-party data in a third-party context.

(10)(A) "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 shall not be considered to be a data broker for purposes of this chapter if the entity is acting as a service provider.

(B) For purposes of this subdivision (10), 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 not fewer than 5,000 individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data.

(11)(A) "Decision space" means the array of aesthetic and functional elements within an information technology, including physical, hardware, and

software features that shape a trusting party's expectations about how a technology functions and can be used.

(B) "Decision space" includes interactive settings and choices presented to a trusting party when interfacing with a digital service or technology, including:

(i) the size, shape, and prominence of control elements, settings, and choices;

(ii) hypertext and hypermedia;

(iii) coloration and font choice;

(iv) buttons, sliders, switches, radio buttons, and check boxes;

(v) scroll bars and hyperlinks; and

(vi) motion-captured gestures.

(12) "Deidentified 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 reasonable technical measures to ensure that the information cannot, at any point, be used to reidentify any individual or device that identifies or is linked or reasonably linkable to an individual;

(B) publicly commits in a clear and conspicuous manner to:

(i) process and transfer the information solely in a deidentified form without any reasonable means for reidentification; and

(ii) not attempt to reidentify 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 subdivision (12) 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.

(13) "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.

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

(15) "Employee" means an individual who is an employee, director, officer, staff member 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.

(16) "Employee data" means:

(A) information relating to a job applicant collected by a covered entity acting as a prospective employer of the job applicant in the course of the application or hiring process, if the 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 the information is collected, processed, or transferred solely for purposes related to the 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 employer by an employee who is acting in a professional capacity, if the information is collected, processed, or transferred solely for purposes related to the 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 the 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 the information in case of an emergency; or

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

(17) "Exposure" means the degree to which a trusting party has made themselves vulnerable to harm or loss due to entrusting a covered entity with the trusting party's data and mediated experiences. A trusting party's exposure when interacting with an information technology is shaped by what a covered entity can see or knows about that trusting party, which choices and options are available to the trusting party, and what the trusting party can see or know about the covered entity. A covered entity shall assess a trusting party's exposure by considering the nature and length of the relationship between the parties; the nature of the data collected, processed, or transferred, including whether any of the data is sensitive covered data; and the nature of the choices and signals mediated or controlled by the covered entity. For the purposes of this subdivision, vulnerability to harm or loss includes vulnerability to the following:

(A) physical harm that results in bodily injury or death;

(B) economic harm resulting in monetary loss, loss in the value of some asset, or time spent to protect oneself from risk of harm due to the breach or misuse of covered data;

(C) reputational harms affecting an individual's reputation, standing in the community, business opportunities, or employment;

(D) psychological harm in the form of emotional distress, which entails feelings of annoyance, frustration, fear, embarrassment, anger, and various degrees of anxiety, or disturbance, which entails intrusions that disturb tranquility, interrupt activities, or unreasonably consume a trusting party's time;

(E) autonomy harms, such as:

(i) coercion, where a trusting party's freedom to act or choose has been impaired;

(ii) manipulation, where there exists undue influence over a trusting party's behavior or decision making;

(iii) failure to inform, where a covered entity has failed to provide trusting parties with sufficient information to make decisions;

(iv) thwarted expectations, where a covered entity engages in acts or practices that undermines a trusting party's choices regarding data practices;

(v) lack of control, where a trusting party is rendered unable to make meaningful choices about the trusting party's covered data or to prevent future misuse of the covered data; and

(vi) chilling effects, where a trusting party is inhibited from engaging in lawful activities;

(F) discrimination harms, where an act or practice involving covered data entrenches inequality or disadvantages individuals based on gender, sex, sexual orientation, race, color, national origin, age, disability, group membership, or other characteristics or affiliations;

(G) relationship harms, where the misuse or mishandling of covered data damages personal relationships, professional relationships, or relationships with organizations; and

(H) loss, which includes attention capture and opportunity costs of engagement with an information technology.

(18) "First-party advertising or marketing" means advertising or marketing conducted by a covered entity that collected covered data from the trusting party linked or reasonably linkable to that data, through either direct communications with a user 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

the covered entity, or on a website or app operated by or on behalf of the 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 subdivision (A) of this subdivision (19).

(20) "Individual" means a natural person who is a resident of Vermont or is present in Vermont and is considered a consumer for purposes of the Vermont Consumer Protection Act.

(21) "Information relationship" means the discrete or ongoing interactions between individuals and covered entities that are mediated by information technologies.

(22) "Information technology" means any technology, product, device, service, or method used by a covered entity to collect, process, or transfer covered data.

(23)(A) "Large data holder" means a covered entity or service provider that, in the most recent calendar year:

(i) had annual gross revenues of $250,000,000.00 or more; and

(ii) collected, processed, or transferred the:

(I) covered data of more than 5,000 individuals or devices that identify or are linked or reasonably linkable to one 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

(II) sensitive covered data of more than 2,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals.

(B) "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.

(24) "Legitimate interest" means a lawful objective that does not conflict with the best interests of reasonable trusting parties. Collection or processing is strictly necessary to effect a legitimate interest pursued by the covered entity if such interest is not overridden by the interests or rights and

freedoms of the trusting party pursuant to this chapter that require the protection of covered data.

(25) "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.

(26) "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 or conduct regarding a product or service.

(27)(A) "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 one 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.

(B) "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.

(28) "Predispute arbitration agreement" means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

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

(30) "Process" means to conduct or direct any operation or set of operations performed, whether by manual or automated means, on covered data or on sets of covered data, including analyzing, organizing, structuring, maintaining, retaining, storing, using, adapting or altering, retrieving, consulting, aligning or combining, deleting, erasing, destroying, or otherwise handling covered data.

(31) "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.

(32)(A) "Public 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:

(i) 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 along with a disclosure that has been made to the general public as required by federal, state, or local law;

(ii) 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; or

(iii) publicity given to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.

(B) "Public information" does not include:

(i) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(ii) any inference made exclusively from multiple independent sources of public information;

(iii) biometric data;

(iv) public information that has been combined with covered data;

(v) genetic information, unless otherwise made available by the individual to whom the information pertains; or

(vi) intimate images known to have been created or shared without consent.

(33) "Reasonable trusting party" means a hypothetical ordinary person who enters into information relationships and makes choices within the relationships that entail only a reasonable allocation of risks and benefits between the covered entity and the reasonable trusting party.

(34) "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.

(35) "Scraping" means the automated collection of covered data, whether structured or unstructured, by a third party from an information technology for the purpose of processing or onward transfer.

(36) "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 care 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) Precise geolocation information.

(F) An individual's private communications, such as voicemails, emails, text messages, direct messages, or mail, or information identifying the parties to the communications, and any information that pertains to the transmission of the 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 subdivision (F) if the communications are made

from or to a device provided by an employer to an employee, provided the employer provides conspicuous notice that the employer may access the communications.

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

(H) 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 the information.

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

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

(K) Information revealing the video content requested or selected by an individual collected by a covered entity, excluding covered data used solely for transfers for independent video measurement.

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

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

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

(O) Any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data listed in subdivisions (A)–(N) of this subdivision (36).

(37) "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 pursuant to this chapter shall be treated as a service provider pursuant to this chapter with respect to such data.

(38) "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 which the 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.

(39) "Small business" means a covered entity or a service provider that meets the following criteria for the period of the three 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 three years:

(A) The covered entity or service provider's average annual gross revenues during the period did not exceed $41,000,000.00.

(B) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 2,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, provided all covered data for such purpose was deleted or deidentified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy.

(C) The covered entity is not a data broker.

(40)(A) "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.

(B) "Targeted advertising" does not include:

(i) advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback;

(ii) contextual advertising, which is when an advertisement is displayed based on the content in which the advertisement appears and does not vary based on who is viewing the advertisement; or

(iii) processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content performance, reach, or frequency, including independent measurement.

(41)(A) "Third party" means any person or entity, including a covered entity, that:

(i) collects, processes, or transfers covered data:

(I) that the person or entity did not collect directly from the individual linked or linkable to such covered data; or

(II) that 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) "Third party" does not include a person that collects covered data from another person if the two persons are related by common ownership or

corporate control, but only if a reasonable trusting party's expectation would be that such persons share information.

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

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

(44) "Trusting party" means any individual who entrusts the individual's personal data and mediated experiences to a covered entity.

(45) "Unique identifier" means an identifier to the extent that the identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to one 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.

§ 2411b. DUTY OF LOYALTY

(a) A covered entity owes a duty of loyalty to all trusting parties. This duty is defined by the extent of a reasonable trusting party's exposure.

(b)(1) Pursuant to this duty, a covered entity shall not collect, process, or transfer covered data in a way that conflicts with the best interests of trusting

parties or design or implement an information technology in a way that conflicts with the best interests of trusting parties.

(2) A covered entity's acts or practices conflict with the best interests of trusting parties when either the collection, processing, or transfer of covered data or the design or implementation of an information technology results in a disproportionate allocation of benefits in favor of the covered entity relative to the degree of individual and collective risk posed to the trusting parties.

§ 2411c. COLLECTION

Data minimization and purpose limitation. A covered entity shall not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is strictly necessary and proportionate to:

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

(2) effect a legitimate interest of the covered entity.

§ 2411d. PERSONALIZATION

(a) A covered entity or service provider that directly delivers a targeted advertisement shall do so only where the delivery of the targeted advertisement does not conflict with the best interests of trusting parties.

(b) A covered entity or service provider shall not:

(1) collect, process, or transfer covered data for the purpose of delivering a cross-context behavioral advertisement; or

(2) engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

(c) First-party advertising or marketing does not violate the duty of loyalty.

§ 2411e. GATEKEEPING

(a) A covered entity is prohibited from transferring covered data to a third party or service provider except where allowed under the data minimization rule pursuant to section 2411c of this chapter. When a covered entity does transfer covered data to a third party or service provider, that covered entity shall, in accordance with section 2411n of this chapter, require the third party or service provider, as a condition of receipt of such covered data, to contractually agree to be bound by the duties and obligations of this chapter. Trusting parties whose covered data is transferred shall have the right to enforce such contracts directly as intended third-party beneficiaries.

(b) 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 in accordance with this chapter and any rules adopted pursuant to this chapter.

(c) A covered entity shall implement reasonable safeguards and protections in any information technologies to prevent unauthorized third parties from scraping covered data concerning trusted parties.

§ 2411f. INFLUENCING

(a) A covered entity shall not design or implement an information technology in a way that:

(1) causes or is likely to cause substantial harm to trusting parties that is not reasonably avoidable by trusting parties and not outweighed by countervailing benefits to trusting parties or to competition;

(2) misleads or is likely to mislead a reasonable trusting party in a material way; or

(3) will exploit predictable biases to interfere with a trusting party's decision-making process in an adversarial way.

(b) A covered entity shall not process covered data or design information technologies in a way that:

(1) materially interferes with the ability of trusting parties to understand a term or condition of a covered entity's product or service;

(2) takes unreasonable advantage of:

(A) a lack of understanding on the part of a trusting party of the material risks, costs, or conditions of a covered entity's product or service;

(B) the inability of a trusting party to protect the interests of the trusting party in selecting or using a covered entity's product or service; or

(C) the reasonable reliance by a trusting party on a covered entity to act in the interests of the trusting party; or

(3) has the purpose or substantial effect of obscuring, subverting, or impairing the autonomy, decision making, or choice of a reasonable trusting party in an interaction with the service of the entity by such trusting party, in a way that conflicts with the best interests of the trusting party, which includes the covered entity:

(A) selecting a default software or platform setting that favors the interests of the covered entity over the interests of the trusting party with respect to covered data; or

(B) modifying the decision space of the user on the platform or service of the covered entity to emphasize or promote choices that benefit the interests of the covered entity over the interests of the consumer.

(c) A covered entity shall not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this chapter through:

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

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

§ 2411g. MEDIATION

(a) In designing, deploying, and maintaining information technologies that facilitate a trusting party's interaction with individuals, including natural persons and legal entities, covered entities shall maintain reasonable procedures designed to prevent and mitigate:

(1) the foreseeable risks to physical and mental health;

(2) patterns of use that indicate or encourage addiction-like behaviors;

(3) physical harm, online bullying, and harassment; and

(4) unfair, deceptive, or abusive marketing practices.

(b)(1) A covered entity shall provide readily accessible and easy-to-use safeguards to enable trusting parties to control their experience and covered data on the platform, including settings to:

(A) limit the ability of other individuals to contact or find a trusting party;

(B) prevent other individuals from viewing a trusting party's personal data collected by or shared on the platform, in particular restricting public access to covered data;

(C) limit features that increase, sustain, or extend use of the covered entity's service, such as automatic playing of media, rewards for time spent on the platform, and notifications;

(D) opt out of algorithmic recommendation systems that use covered data;

(E) delete the trusting party's account and request removal of covered data;

(F) restrict the sharing of the precise geolocation information of a trusting party and to provide notice regarding the tracking of a trusting party's precise geolocation information; and

(G) limit the time spent by a trusting party on the platform.

(2) The safeguards required pursuant to subdivision (1) of this subsection shall, by default, be set at the most protective setting.

§ 2411h. 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 or the design of information technologies. A covered entity and service provider shall:

(1) identify, assess, and mitigate risks of harm or loss to trusting parties related to the products and services of the covered entity;

(2) identify the benefits that flow to trusting parties and the covered entity; and

(3) implement reasonable training and safeguards within the covered entity and service provider to promote compliance with this chapter.

(b) The policies, practices, and procedures established by a covered entity and a service provider pursuant to subsection (a) of this section shall, as applicable, correspond with:

(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, third party, or data broker;

(2) whether the covered data collected, processed, or transferred by the covered entity or service provider is sensitive covered data;

(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.

(c) On or before July 1, 2027, and biennially thereafter, each covered entity shall conduct a data loyalty assessment. The assessment shall weigh the relative benefits of the covered entity's covered data collecting, processing,

and transfer practices against the risks of such practices to trusting parties. The covered entity shall make a summary of such data loyalty assessment publicly available in a place that is easily accessible to individuals. The data loyalty assessment shall:

(1) be reasonable and appropriate in scope given the:

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

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

(C) relative benefits conferred upon the covered entity and trusting parties by the collecting, processing, and transfer of covered data by the covered entity; and

(D) risks posed to trusting parties 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 pursuant to subdivision (1) of this subsection;

(3) include additional information required by rules adopted by the Attorney General;

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

(5) if the covered entity is a large data holder, be approved by the privacy protection officer pursuant to subdivision 2411m(c)(2) of this chapter, as applicable.

§ 2411i. TRANSPARENCY

(a) Each covered entity 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.

(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 provide a reasonable opportunity for each individual to object to any further materially different collection, processing, or transfer of previously collected covered data under the changed policy, either by terminating the individual's information relationship with the covered entity or by exercising any applicable consumer data rights pursuant to this chapter.

(c) Nothing in this section may be construed to affect the requirements for covered entities pursuant to this chapter.

§ 2411j. INDIVIDUAL DATA RIGHTS

(a) In accordance with subsections (b) and (c) of this section, a covered entity shall provide a trusting party, after receiving a verified request from the trusting party, with the right to:

(1) access:

(A) in a format that a reasonable individual can understand and download from the internet, the covered data 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 the categories of any service providers to which 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) export, to the extent technically feasible, 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) portable, structured, interoperable, and machine-readable format.

(b)(1) Subject to subsections (c) and (d) of this section, each request under subsection (a) of this section shall be completed by any:

(A) large data holder not later than 45 days after the request from an individual, unless it is demonstrably impracticable or impracticably costly to verify the individual; or

(B) covered entity that is not a large data holder not later than 60 days after the request from an individual, unless it is demonstrably impracticable or impracticably costly to verify the individual.

(2) A response period set forth in subdivision (1) of this subsection may be extended once by 45 additional days when reasonably necessary, considering the complexity and number of the individual's requests, provided the covered entity informs the individual of any such extension within the initial 45-day response period, together with the reason for the extension.

(c) A covered entity:

(1) shall provide an individual with the opportunity to exercise each of the rights described in subsection (a) of this section;

(2) shall allow, for the first two times within a 12-month period that an individual exercises the individual's right pursuant to subdivision (1) of this subsection, the individual to exercise such right free of charge; and

(3) may charge a reasonable fee to an individual who exercises the individual's right pursuant to subdivision (1) of this subsection more than two times within a 12-month period.

(d) A covered entity shall not permit an individual to exercise a right described in subsection (a) of this section, 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 pursuant to 15 U.S.C. § 45; or

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

(e) If a covered entity cannot reasonably verify that a request to exercise a right set forth in subsection (a) of this section 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 shall:

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

(f) A covered entity may decline, with adequate explanation to the individual, to comply with a request to exercise a right described in subsection (a) of this section, in whole or in part, that would:

(1) require the covered entity to retain any covered data collected for a single, onetime transaction, if the covered data is not processed or transferred by the covered entity for any purpose other than completing the transaction, subject to subdivision (g)(1) of this section;

(2) be demonstrably impracticable or prohibitively costly to comply with, upon the covered entity providing a description to the requester detailing the inability to comply with the request, subject to subdivision (g)(2) of this section;

(3) require the covered entity to attempt to reidentify deidentified 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 U.S. Constitution;

(9) prevent a covered entity from being able to maintain a confidential record of deletion requests that are 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; or

(10) 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) delete covered data that would unreasonably interfere with the provision of education services by a school or institution of higher education.

(g) In a circumstance that would allow a denial pursuant to:

(1) subdivision (f)(1) of this section, a covered entity shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so; and

(2) subdivision (f)(2) of this section, the receipt of a large number of verified requests, on its own, shall not be considered to render compliance with a request demonstrably impracticable.

(h) A large data holder 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 received pursuant to subdivision (a)(1) of this section;

(B) the number of verified deletion requests received pursuant to subdivision (a)(3) of this section;

(C) the total number of requests received pursuant to subdivisions (A) and (B) of this subdivision (1) that the large data holder complied with in whole or in part and denied; and

(D) the average number of days it took the large data holder to respond to requests made pursuant to subdivisions (a)(1) and (a)(3) of this section; and

(2) disclose not later than July 1 of each applicable calendar year the information compiled pursuant to subdivision (1) of this subsection within the large data holder's privacy policy or on its publicly accessible website that is accessible from a hyperlink included in the privacy policy.

§ 2411k. RETALIATION PROHIBITED

(a) A covered entity shall not retaliate against a trusting party for exercising any of the rights guaranteed pursuant to this chapter or any rules adopted pursuant to this chapter, 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) of this section shall 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 shall 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 subdivision 2411k(b)(2) of this chapter; 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 section, no covered entity shall offer different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

§ 2411l. CIVIL RIGHTS AND ALGORITHMS

(a)(1) A covered entity or a service provider shall 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.

(2) Subdivision (1) of this subsection does not apply to:

(A) the collection, processing, or transfer of covered data for the purpose of:

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

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

(B) any private club or group not open to the public, as those terms are defined in 42 U.S.C. § 2000a(e).

(b) Notwithstanding any other provision of law, on or before July 1, 2028, and annually thereafter, a covered entity that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group of individuals, and uses the covered algorithm, solely or in part, to collect, process, or transfer covered data, shall conduct a data loyalty assessment of such algorithm. The data loyalty 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 proposed uses of the covered algorithm;

(3) a detailed description of the data used by the covered algorithm, including the specific categories 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; and

(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) minors;

(B) making or facilitating advertising for, or determining access to or restrictions on the use of housing, education, employment, health care, 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 effect on the basis of individuals' race, color, religion, national origin, sex, or disability status;

(E) disparate effect on the basis of individuals' political party registration status; and

(F) any other information as required by the Attorney General.

(c) Notwithstanding any other provision of law, on or before July 1, 2028, a covered entity or service provider that knowingly develops a covered algorithm that is designed to, solely or in part, collect, process, or transfer covered data in furtherance of a consequential decision shall, prior to deploying the covered algorithm, 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 potential harms identified under this section.

(d) In complying with this section, a covered entity and a service provider shall focus the data loyalty 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 a loyalty assessment or evaluation, submit the data loyalty assessment or evaluation conducted pursuant to subsection (b) or (c) of this section to the Attorney General and shall make a summary of such loyalty 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 18 U.S.C. § 1839, or other confidential or proprietary information from public disclosure pursuant to this subsection.

§ 2411m. EXECUTIVE RESPONSIBILITY

(a) On or before July 1, 2028, an executive officer of a large data holder shall annually, in good faith, certify to the Attorney General that the entity maintains:

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

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

(b) A certification submitted pursuant to subsection (a) of this section:

(1) 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; and

(2) 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 shall designate one or more qualified employees as privacy protection officers and one 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 protection officer or a data security officer pursuant to this subsection 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 chapter; and

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

(2) A large data holder shall designate at least one of the officers described in this subsection to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to meeting the requirements in subdivision (1) of this subsection, 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 chapter and ensure such audits are accessible to the Attorney General upon request;

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

(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.

§ 2411n. 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) of this section, but does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

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

(3) shall assist a covered entity in responding to a request made by an individual pursuant to section 2411j or 2411k of this chapter 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 the 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 the service provider 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 2411j or 2411k of this chapter;

(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 the other service provider to satisfy the obligations of the service provider with respect to the service provider data, including that the other service provider be treated as a service provider pursuant to this chapter;

(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 chapter, which

may include making available a report of an independent assessment arranged by the service provider on terms agreed to be the service provider and the covered entity, providing information necessary to enable the covered entity to conduct and document a data loyalty assessment required under this chapter, and making available the report required under subdivision 2411m(c)(2)(B) of this chapter;

(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 this section; and

(8) shall either:

(A) allow and cooperate with reasonable assessments by the covered entity or the covered entity's designated assessor; or

(B) 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 chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments.

(b) A person or entity shall 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 subdivision (a)(4) of this section 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 pursuant to this chapter; and

(4) prohibits:

(A) collecting, processing, or transferring covered data in a way that is not permitted pursuant to subsection (a) of this section; and

(B) combining service provider data with covered data that 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 subdivisions 2411a(b)(36)(A)–(N) of this chapter.

(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 chapter, is not

liable for a violation of this chapter by the service provider or covered entity to which 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 chapter.

(4) A covered entity or service provider that receives covered data in compliance with the requirements of this chapter is not in violation of this chapter 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, to effect a purpose enumerated in subdivision 2411a(b)(36)(A), (C), or (E) of this chapter and, in the case of nonsensitive data, the processing purpose for which the covered entity made a disclosure pursuant to this chapter;

(2) for purposes of subdivision (1) of this subsection, 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 pursuant to subsection (e) of this section.

(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 the 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 shall only use the covered data for such specific purposes; and

(3) requires the third party to comply with all applicable provisions of and rules adopted pursuant to this chapter 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 of the covered entity under this chapter.

(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.

§ 2411o. ENFORCEMENT

A covered entity or service provider that violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

§ 2411p. APPLICABILITY

(a) A covered entity or service provider that is required to comply with and is in compliance with the following shall be deemed to be in compliance with the related requirements of this chapter:

(1) 15 U.S.C. § 6801 (Title V of the Gramm-Leach-Bliley Act);

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

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

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

(5) 20 U.S.C. § 1232g (Family Educational Rights and Privacy Act), 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);

(6) 42 U.S.C. § 290dd-2 (Confidentiality of Alcohol and Drug Abuse Patient Records);

(7) 42 U.S.C. § 2000ff (Genetic Information Nondiscrimination Act); and

(8) regulations promulgated pursuant to 42 U.S.C. § 1320d-2 (Health Insurance Portability and Accountability Act of 1996).

(b) A covered entity or service provider that is required to comply with the following and is in compliance shall be deemed to be in compliance with the requirements of subsection 2411e(b) of this chapter:

(1) 15 U.S.C. § 6801 (Title V of the Gramm-Leach-Bliley Act);

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

(3) 42 U.S.C. § 1320d (Part C of Title XI of the Social Security Act); or

(4) regulations promulgated pursuant to 42 U.S.C. § 1320d-2 (Health Insurance Portability and Accountability Act of 1996).

(c) Nothing in this chapter shall be construed to limit or diminish First Amendment freedoms guaranteed under the U.S. Constitution.

§ 2411q. RULEMAKING

(a) The Attorney General shall have the same authority under this chapter to make rules, conduct civil investigations, bring civil actions, and enter into assurances of discontinuance as provided under chapter 63 of this title.

(b) Rules adopted by the Attorney General pursuant to subsection (a) of this section shall include:

(1) the establishment of new subsidiary duties of loyalty;

(2) 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;

(3) 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;

(4) updating or adding categories to the definition of "sensitive covered data" to include 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;

(5) establishing a list of practices that constitute legitimate interests under subdivision 2411a(b)(36) of this chapter, provided such purposes are consistent with the reasonable expectations of individuals;

(6) further defining what constitutes reasonable policies, practices, and procedures pursuant to section 2411h of this chapter;

(7) establishing the form and content of the transparency obligations pursuant to section 2411i of this chapter;

(8) establishing processes by which covered entities are to comply with the provisions in section 2411j of this chapter and considering:

(A) the size, 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, 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 chapter where appropriate;

(9) establishing rules and procedures to further the purposes of section 2411j of this chapter 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;

(10) establishing additional permissive exceptions necessary to protect the rights of individuals and 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;

(11) establishing how often, and under what circumstances, an individual may request a correction pursuant to section 2411j of this chapter;

(12) 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;

(13) requiring covered entities obligated to conduct loyalty assessments pursuant to subsection 2411h(c) or 2411l(b) of this chapter to establish a process to ensure that audits are thorough and independent;

(14) requiring additional information necessary for compliance with the data loyalty assessments required pursuant to subsection 2411h(c) or 2411l(b) of this chapter; and

(15) excluding from the algorithmic loyalty assessments required pursuant to subsection 2411l(b) of this chapter any covered algorithm that presents low or minimal consequential risk of harm to an individual or group of individuals.

Sec. 2. EFFECTIVE DATE

This act shall take effect on January 1, 2027.