STATE OF NEW YORK

3586

2021-2022 Regular Sessions

IN ASSEMBLY

January 28, 2021

Introduced by M. of A. KIM, DICKENS, COOK, HYNDMAN, COLTON, SAYEGH, GUNTHER, MONTESANO, ENGLEBRIGHT, NIOU, J. RIVERA -- Multi-Sponsored by -- M. of A. DE LA ROSA -- read once and referred to the Committee on Consumer Affairs and Protection

AN ACT to amend the civil rights law and the general business law, in relation to establishing the "It's Your Data Act"

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "It's Your Data Act".

§ 2. Section 50 of the civil rights law is amended to read as follows:

§ 50. Right of privacy. A person, firm or corporation that **collects, stores, and/or** uses for **the purpose of** advertising [~~purposes, or for the purposes of~~], trade, **data-mining, or generating commercial or economic value,** the name, portrait [~~or~~], picture**, video, voice, likeness, and all other personal data, biometric data, and location data** of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, **or, if such consent is obtained, subsequently fails to exercise reasonable care consistent with its obligations as bailee of that individual's name, portrait, picture, video, voice, likeness, and all other personal data, biometric data, and location data,** is guilty of a misdemeanor.

§ 3. Section 51 of the civil rights law, as amended by chapter 674 of the laws of 1995, is amended to read as follows:

§ 51. Action for injunction and for damages. Any person [~~whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without the written consent~~]**, firm or corporation that collects, stores, and/or uses for the purpose of advertising, trade, data-mining, or generating commercial or economic value, name, portrait, picture, video, voice, likeness, and all other personal data, biometric data, and location data of any living person**

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD06064-01-1

without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, or, when such consent is obtained, subsequently fails to exercise reasonable care consistent with its obligations as bailee of that individual's name, portrait, picture, video, voice, likeness, and all other personal data, biometric data, and location data first obtained as above provided may maintain an equitable action in the supreme court of this state against the person, firm or corporation so using his or her name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained by reason of such use and if the defendant shall have knowingly used such person's name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data in such manner as is forbidden or declared to be unlawful by section fifty of this article, the jury, in its discretion, may award exemplary damages. But nothing contained in this article shall be so construed as to prevent any person, firm or corporation from selling or otherwise transferring any material containing such name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data in whatever medium to any user of such name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data or to any third party [~~for sale~~] or transfer directly or indirectly to such a user, for use, provided that the transferring party undertakes reasonable steps to ensure that any such use is consistent with the selling or transferring party's obligations as bailee of that individual's name, portrait, picture, video, voice, likeness, and all other personal data, biometric data, and location data and use in a manner lawful under this article; nothing contained in this article shall be so construed as to prevent any person, firm or corporation, practicing the profession of photography, from exhibiting in or about his or its establishment specimens of the work of such establishment, unless the same is continued by such person, firm or corporation after written notice objecting thereto has been given by the person portrayed; and nothing contained in this article shall be so construed as to prevent any person, firm or corporation from using the name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data of any manufacturer or dealer in connection with the goods, wares and merchandise manufactured, produced or dealt in by him or her which he or she has sold or disposed of with such name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data used in connection therewith; or from using the name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data of any author, composer or artist in connection with his or her literary, musical or artistic productions which he or she has sold or disposed of with such name, portrait, picture [~~or~~], video, voice, likeness, and all other personal data, biometric data, and location data used in connection therewith. Nothing contained in this section shall be construed to prohibit the copyright owner of a sound recording from disposing of, dealing in, licensing or selling that sound recording to any party, if the right to dispose of, deal in, license or sell such sound recording has been conferred by contract or other written document by such living person or the holder of such right. Nothing contained in the foregoing sentence shall be deemed to abrogate or otherwise limit any rights or remedies otherwise conferred by federal law or state law.

§ 4. The general business law is amended by adding a new article 32-A to read as follows:

ARTICLE 32-A
IT'S YOUR DATA ACT

Section 676. Definitions.
676-a. Transparency of the collection, use, retention, and sharing of personal information.
676-b. Fair collection and use of personal information.
676-c. Deletion of personal information.
676-d. Access to retained personal information.
676-e. Access to disclosure of personal information.
676-f. Consent to additional collection or sharing of personal information.
676-g. No discrimination by a business against a consumer for exercise of rights.
676-h. Reasonable security.
676-i. Business implementation of duties.
676-j. Exceptions.
676-k. Consumer's private right of action.
676-l. Agency enforcement action.
676-m. Construction.
676-n. Attorney general regulations.
676-o. Intermediate transactions.
676-p. Non-waiver.
676-q. Severability.

§ 676. Definitions. 1. For the purposes of this article:

(a) "Aggregate consumer information" means information that relates to a group of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. Aggregate consumer information does not mean one or more individual consumer records that have been de-identified.

(b) "Biometric information" means an individual's physiological, biological or behavioral characteristics or an electronic representation of such, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(i) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of New York, and that satisfies one or more of the following thresholds:

(1) has annual gross revenues in excess of fifty million dollars, as adjusted pursuant to paragraph (f) of subdivision one of section six hundred seventy-six-n of this article;

(2) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or discloses for commercial purposes, alone or in combination, the personal information of fifty thousand or more consumers, households, or devices; or

(3) derives fifty percent or more of its annual revenues from selling consumers' personal information; and

(ii) Any entity that controls or is controlled by a business, as defined in subparagraph (i) of this paragraph, and that shares common branding with such business.

(d) "Control" or "controlled" means ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a business.

(e) "Common branding" means a shared name, servicemark, or trademark.

(f) "Operational purpose" means the use of personal information when reasonably necessary and proportionate to achieve one of the following operational purposes:

(i) auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this paragraph and other standards;

(ii) detecting and responding to security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;

(iii) debugging to identify and repair errors that impair existing intended functionality;

(iv) short-term, transient use, provided the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction;

(v) performing or providing services on behalf of the business or service provider, including maintaining or servicing accounts, billing or collecting for requested products or services, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider;

(vi) undertaking internal research for technological development and demonstration;

(vii) undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, or to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business;

(viii) customization of content; or

(ix) customization of advertising or marketing.

(g) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This shall include, but shall not be limited to, receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(h) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. Commercial purposes shall not include engaging in speech that state or federal courts have recognized as noncommercial speech, including, but not limited to, political speech and journalism.

(i) "Consumer" means a natural person who is a resident of the state of New York.

(j) "De-identified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information:

(i) takes reasonable measures to ensure that the data is de-identified;

(ii) publicly commits to maintain and use the data in a de-identified fashion and not to attempt to re-identify the data; and

(iii) contractually prohibits downstream recipients from attempting to re-identify the data.

(k) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request under this article, and any new, consumer-friendly means of contacting a business, as approved by the attorney general pursuant to section six hundred seventy-six-n of this article.

(l) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(m) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(n) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(o) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(p) "Personal information" means information that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device. Personal information shall not include publicly available information, information that is de-identified, or aggregate consumer information.

(q) "Publicly available" means information that is lawfully made available from federal, state, or local government records. Publicly available does not mean information collected by a business about a consumer without the consumer's knowledge.

(r) "Service" or "services" means work, labor, and services, including services furnished in connection with the production, sale or repair of goods.

(s) "Service provider" means an individual sole proprietorship, partnership, limited liability company, corporation, association, or other

legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which such business discloses a consumer's personal information for an operational purpose pursuant to a written or electronic contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for such business, or as otherwise permitted by this article, including a prohibition on retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with such business.

(t) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the secretary of state, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify. A business shall not be obligated to provide any personal information to a consumer if such business cannot verify that the consumer making the request is the consumer about whom such business has collected personal information or is a person authorized by the consumer to act on such consumer's behalf.

(u) "Third party" means a person or business that is not any of the following:

(i) the business that collects personal information from consumers under this article; or

(ii) a person to whom the business discloses a consumer's personal information for an operational purpose pursuant to a written contract, provided that the contract:

(1) prohibits the person receiving the personal information from:

(A) selling the personal information;

(B) retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract; and

(C) retaining, using, or disclosing the information outside of the direct business relationship between the person and the business; and

(2) includes a certification made by the person receiving the personal information that the person understands the restrictions in clause one of this paragraph and will comply with such restrictions.

2. For references to a category or categories of personal information required to be disclosed pursuant to this article:

(a) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(b) "Research" means scientific and systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be:

(i) compatible with an operational purpose for which the personal information was collected;

(ii) subsequently de-identified, or in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable

of being associated with, or be linked, directly or indirectly, to a particular consumer;

(iii) made subject to technical safeguards to prevent re-identification of the consumer to whom the information may pertain;

(iv) subject to business processes that specifically prohibit re-identification of the information;

(v) made subject to business processes to prevent inadvertent release of de-identified information;

(vi) protected from any re-identification attempts;

(vii) used solely for research purposes that are compatible with the context in which the personal information was collected;

(viii) not be used for any commercial purpose; and

(ix) subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(c) (i) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

(ii) For purposes of this article, a business does not sell personal information when:

(1) a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided such third party does not also sell the personal information, unless such disclosure would be consistent with the provisions of this article. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content shall not constitute a consumer's intent to interact with a third party;

(2) the business uses or discloses an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information;

(3) the business uses or discloses personal information of a consumer with a service provider that is necessary to perform an operational purpose and the business has provided notice that information being used or disclosed in its terms and conditions consistent with section six hundred seventy-six-i of this article; or

(4) the business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or disclosed consistently with this article. A third party may not materially alter how it uses or discloses the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, unless it first obtains opt-in consent, as set forth in this article.

§ 676-a. Transparency of the collection, use, retention, and sharing of personal information. Any business that collects a consumer's personal information shall disclose the following information in its online privacy policy or policies, if the business has an online privacy policy, and update such information at least once every twelve months:

1. a description of a consumer's rights pursuant to sections six hundred seventy-six-b, six hundred seventy-six-d, six hundred seventy-six-e, six hundred seventy-six-f and six hundred seventy-six-g of this article and one or more designated methods for submitting requests pursuant to sections six hundred seventy-six-c, six hundred seventy-six-d, and six hundred seventy-six-e of this article;

2. a description of the personal information such business collects about consumers;

3. the categories of sources from which the personal information is collected;

4. a description of the methods such business uses to collect personal information;

5. the specific purposes for collecting, disclosing, or retaining personal information;

6. a description of the personal information it discloses about consumers, or if the business does not disclose consumers' personal information, the business shall disclose such fact;

7. the categories of third parties with whom such business shares personal information with, or if the business does not disclose consumers' personal information to third parties, the business shall disclose such fact;

8. the categories of service providers with whom such business shares personal information with, or if the business does not disclose consumers' personal information to service providers, the business shall disclose such fact;

9. a description of the length of time for which personal information is retained; and

10. if personal data is de-identified such that it is no longer considered personal information but subsequently retained, used, or shared by the business, a description of the method or methods of de-identification.

§ 676-b. Fair collection and use of personal information. 1. Subject to section six hundred seventy-six-f of this article a business that collects a consumer's personal information shall limit its collection and sharing of personal information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention, and shall require any such third party to exercise care over the consumer's personal information consistent with the original business's obligations as bailee of such information.

2. Subject to section six hundred seventy-six-f of this article, a business that collects a consumer's personal information shall be obligated to exercise reasonable care with respect to the collection, storage, and use of that information, consistent with its obligations as a bailee, and shall limit its use and retention of personal information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided however that data collected or retained solely for security or fraud prevention may not be used for related operational purposes.

§ 676-c. Deletion of personal information. 1. A consumer shall have the right to request that a business delete any personal information about such consumer which the business has collected from the consumer.

2. A business that collects personal information about consumers shall disclose, pursuant to the notice requirements of section six hundred seventy-six-i of this article, the consumer's rights to request the deletion of the consumer's personal information.

3. A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision one of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

4. A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if:

(a) such retention of personal information is reasonably anticipated within the context of a business's ongoing business relationship with the consumer; or

(b) it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(i) complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer;

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

(iii) debug to identify and repair errors that impair existing intended functionality;

(iv) exercise free speech, ensure the right of another consumer to exercise his or her right of free speech;

(v) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent; or

(vi) comply with a legal obligation.

§ 676-d. Access to retained personal information. 1. If a business collects personal information about a consumer, the consumer shall have the right to ask the business for the following information, and the business shall have the duty to provide it, promptly and free of charge, upon receipt of a verifiable request:

(a) the specific pieces of personal information that the business retains about that consumer;

(b) the specific sources from which the business collected the personal information; and

(c) its purpose for collecting the personal information.

2. When a business receives a verifiable consumer request from a consumer for the specific pieces of their personal information, such business shall disclose such information in an electronic, portable, machine-readable, and readily-useable format or formats that allow the consumer to understand such information and to transmit such information to another entity without hindrance.

§ 676-e. Access to disclosure of personal information. If a business discloses personal information about a consumer to a third party, the consumer shall have the right to request the following information from the business, and such business shall have the duty to provide it, promptly and free of charge, upon receipt of a verifiable request:

1. the categories of personal information that the business disclosed about the consumer, and the categories of third parties to whom the personal information was disclosed, by category of personal information for each category of third party; and

2. the specific third parties to whom the personal information was disclosed.

§ 676-f. Consent to additional collection or sharing of personal information. 1. Other than as described in section six hundred seventy-six-b of this article, a business shall not collect or share a consumer's personal information unless the consumer has affirmatively authorized the collection or disclosure. This right to collect or share a consumer's personal information may be referred to as the right to "opt-in consent".

2. Any personal information of a consumer collected or shared by a business upon the affirmative authorization of the consumer shall remain the property of such consumer, and the business shall be required to exercise reasonable care in the collection and sharing of such data, consistent with its obligations towards the consumer as bailee of his or her personal information.

3. A business shall request a user's opt-in consent separately from any other permission or consent, with the option to decline consent at least as prominent as the option to provide consent.

4. If a consumer declines to provide their opt-in consent to the disclosure of their personal information, a business shall refrain for at least twelve months before again requesting that the consumer provide their opt-in consent to the disclosure of their personal information.

5. A business may make available a setting or other user control that the consumer may affirmatively access in order to consent to additional data collection or sharing.

6. A business that obtains a consumer's opt-in consent to collect or disclose their personal information pursuant to this section shall provide consumers the ability to withdraw such consent through a readily usable and automated means at any time.

§ 676-g. No discrimination by a business against a consumer for exercise of rights. A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this article or does not provide consent to additional data collection or sharing under section six hundred seventy-six-f of this article including, but not limited to, by:

1. denying goods or services to the consumer;

2. charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

3. providing a different level or quality of goods or services to the consumer; or

4. suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

§ 676-h. Reasonable security. 1. A business or service provider shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the information and the purposes for which the personal information will be used, to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.

2. A business or service provider may employ any lawful security measures that allow it to comply with the requirements set forth in this section.

§ 676-i. Business implementation of duties. 1. A business shall:

(a) make available to consumers two or more designated methods for submitting requests pursuant to sections six hundred seventy-six-c, six

hundred seventy-six-d, and six hundred seventy-six-e of this article, including, at a minimum, a telephone number, and, if the business maintains an internet web site, a web site address;

(b) disclose and deliver the required information to a consumer free of charge within forty-five days of receiving a verifiable consumer request. A business shall take steps to determine whether the request is a verifiable consumer request from the identified consumer. The time period may be extended once by forty-five days when reasonably necessary, provided the consumer is provided notice of the extension within the first forty-five day period. The disclosure shall cover the twelve month period preceding the request. It shall be delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option, if the consumer does not maintain an account with the business. The business shall not require the consumer to create an account with the business in order to make a verifiable request;

(c) ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this article are informed of all requirements in this article, and how to direct consumers to exercise their rights in this article; and

(d) limit the use of any personal information collected from the consumer in connection with a business's verification of the consumer's request solely for the purposes of verification.

2. A business shall not be obligated to provide the information required by sections six hundred seventy-six-d and six hundred seventy-six-e of this article to the same consumer more than twice in a twelve month period.

§ 676-j. Exceptions. 1. The obligations imposed on businesses by this article shall not restrict a business's or service provider's ability to:

(a) comply with federal, state, or local laws;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;

(c) cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law;

(d) exercise or defend legal claims;

(e) collect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate; or

(f) collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of the state. For purposes of this section, commercial conduct takes place wholly outside of the state if the business collected information while the consumer was outside of the state, no part of the sale of the consumer's personal information occurred in the state, and no personal information collected while the consumer was in the state is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when such consumer is in the state and then collecting such personal information when such consumer and stored personal information is outside of the state.

2. Nothing in this article shall require a business to violate an evidentiary privilege under state or federal law or prevent a business from providing the personal information of a consumer who is covered by an evidentiary privilege under state or federal law as part of a privileged communication.

3. This article shall not apply to any of the following:

(a) medical information governed by part 2.6 of the Confidentiality of Medical Information Act or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued or established by the United States department of health and human services, 45 C.F.R. parts 160 and 164, the Health Insurance Portability and Accountability Act of 1996, or the Health Information Technology for Economic and Clinical Health Act;

(b) a provider of health care governed by part 2.6 of the Confidentiality of Medical Information Act or a covered entity governed by the privacy, security, and breach notification rules issued or established by the United States department of health and human services, 45 C.F.R. parts 160 and 164, or the Health Insurance Portability and Accountability Act of 1996, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in paragraph (a) of this subdivision;

(c) information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the "Common Rule", pursuant to good clinical practice guidelines issued by the International Council for Harmonization or pursuant to human subject protection requirements of the United States Food and Drug Administration;

(d) the sale of personal information to or from a consumer reporting agency if such information is to be reported in, or used to generate, a consumer report as defined in section three hundred eighty-a of this chapter and use of that information is limited by the federal Fair Credit Reporting Act, 15 USC 1681;

(e) personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act or any financial privacy laws or regulations of the state of New York, and implementing regulations, if it is in conflict with such law; or

(f) personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994, if it is in conflict with such act.

4. Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to sections six hundred seventy-six-c, six hundred seventy-six-d, and six hundred seventy-six-e of this article:

(a) the time period for a business to respond to any verified consumer request may be extended by up to ninety additional days where necessary, taking into account the complexity and number of the requests. A business shall inform the consumer of any such extension within forty-five days of receipt of the request, together with the reasons for the delay;

(b) if a business does not take action on the request of the consumer, such business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business; and

(c) if requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. Such business shall bear the burden

of demonstrating that any verified consumer request is manifestly unfounded or excessive.

5. A business that discloses personal information to a service provider shall not be liable under this article if the service provider receiving the personal information uses it in violation of the restrictions set forth in this article, provided that, at the time of disclosing the personal information, such business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall not be liable under this article for the obligations of a business for which it provides services as set forth in this article.

6. This article shall not be construed to: (a) require a business to collect or retain personal information about a consumer longer than it would be retained such information in the ordinary course of business; or

(b) require a business to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information.

7. The rights afforded to consumers and the obligations imposed on a business pursuant to this article shall not adversely affect the rights and freedoms of other consumers.

8. The rights afforded to consumers and the obligations imposed on any business pursuant to this article shall not apply to the extent that they infringe on the noncommercial activities of a publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service.

§ 676-k. Consumer's private right of action. 1. A consumer who has suffered a violation of this article may bring a lawsuit against the business that committed such violation. A violation of this article shall be deemed to constitute an injury in fact to the consumer who has suffered such violation, and the consumer need not suffer monetary or property loss as a result of such violation in order to bring an action for a violation of this article.

2. A consumer who prevails in such an action shall obtain the following remedies:

(a) damages in an amount not to exceed seven hundred fifty dollars per consumer per violation or actual damages, whichever is greater;

(b) injunctive or declaratory relief, as the court deems proper;

(c) reasonable attorney fees and costs; and

(d) any other relief the court deems proper.

3. In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

4. A consumer bringing an action pursuant to this section shall notify the attorney general within thirty days of the filing of such action.

§ 676-l. Agency enforcement action. 1. The attorney general, county district attorney, or city corporation counsel having proper jurisdiction may bring a civil action in the name of the people of the state of New York against any person, business, or service provider who violates any provision of this article.

2. Any person, business, or service provider who violates the provisions of this article may be liable for a civil penalty of up to seven thousand five hundred dollars for each intentional violation and of up to two thousand five hundred dollars for each unintentional violation.

§ 676-m. Construction. This article is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information. The provisions of this article are not limited to information collected electronically or over the internet, but shall apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this article, but in the event of a conflict between other laws and the provisions of this article, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

§ 676-n. Attorney general regulations. 1. Within one year of the effective date of this article, the attorney general shall adopt regulations to further the purposes of this article, including, but not limited to:

(a) detailing as needed the types of information that are personal information in technology, data collection practices, obstacles to implementation, and privacy concerns;

(b) establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights;

(c) facilitating and governing the submission of a request by a consumer to opt out of the sale of personal information pursuant to section six hundred seventy-six-f of this article;

(d) governing business compliance with a consumer's opt-out request;

(e) developing a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information;

(f) adjusting the monetary threshold in clause one of subparagraph (i) of paragraph (c) of subdivision one of section six hundred seventy-six of this article in January of every odd-numbered year to reflect any increase in the consumer price index;

(g) establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this article are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings; and

(h) establishing rules and procedures to further the purposes of sections six hundred seventy-six-d and six hundred seventy-six-e of this article and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to section six hundred seventy-six-i of this article, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not

maintain an account with the business to request information through the business' authentication of the consumer's identity.

2. The attorney general may update the foregoing regulations, and adopt additional regulations, as necessary to further the purposes of this article.

3. Before adopting any regulations, the attorney general shall solicit broad public participation concerning those regulations.

§ 676-o. Intermediate transactions. If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this article, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this article.

§ 676-p. Non-waiver. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this article, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business' sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

§ 676-q. Severability. If any provision of this article or the application thereof to any person, business, service provider, or circumstances is held invalid, such invalidity shall not affect other provisions or applications of this article which can be given effect without the invalid provision or application, and to this end the provisions of this article are declared to be severable.

§ 5. This act shall take effect one year after it shall have become a law.