

STATE OF NEW YORK

5827

2025-2026 Regular Sessions

IN ASSEMBLY

February 20, 2025

Introduced by M. of A. SOLAGES -- read once and referred to the Committee on Science and Technology

AN ACT to amend the general business law, in relation to establishing consumers' foundational data privacy rights, creating oversight mechanisms, and establishing enforcement mechanisms; and to amend the state finance law, in relation to establishing the privacy and security victims relief fund

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

1 Section 1. Article 46 of the general business law is redesignated
2 article 60 and sections 1600 and 1601 are redesignated sections 6000 and
3 6001.

4 § 2. The general business law is amended by adding a new article 46 to
5 read as follows:

6 ARTICLE 46
7 DATA PRIVACY AND PROTECTION

8 Title I. Short title and definitions (§§ 1600--1601).
9 Title II. Duty of loyalty (§§ 1610--1613).
10 Title III. Consumer data rights (§§ 1620--1629).
11 Title IV. Corporate accountability (§§ 1640--1644).
12 Title V. Enforcement, applicability, and miscellaneous (§§
13 1650--1654).

14 TITLE I
15 SHORT TITLE AND DEFINITIONS

16 Section 1600. Short title.
17 1601. Definitions.
18 § 1600. Short title. This article shall be known and may be cited as
19 the "American Data Privacy and Protection Act".

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

LBD09203-01-5

§ 1601. Definitions. As used in this article:

1. (a) "Affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of paragraph (b) of this subdivision.

(b) The requirements of this paragraph with respect to a request from a covered entity to an individual are the following:

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

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

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

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

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

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

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

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

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

(c) A covered entity may not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(d) A covered entity may not obtain or attempt to obtain the affirmative express consent of an individual through:

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

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

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

3. (a) "Biometric information" means any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including:

- (i) fingerprints;
- (ii) voice prints;
- (iii) iris or retina scans;
- (iv) facial or hand mapping, geometry, or templates; or
- (v) gait or personally identifying physical movements.

(b) "Biometric information" does not include:

- (i) a digital or physical photograph;
- (ii) an audio or video recording; or
- (iii) data generated from a digital or physical photograph, or an audio or video recording, that cannot be used to identify an individual.

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

5. "Control" means, with respect to an entity:

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

(b) control over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

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

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

7. (a) "Covered data" means information 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, and may include derived data and unique persistent identifiers.

(b) "Covered data" does not include:

- (i) de-identified data;
- (ii) employee data;
- (iii) publicly available information; or
- (iv) inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

8. (a) "Covered entity":

(i) means any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and:

(A) is subject to the Federal Trade Division Act (15 U.S.C. 41 et seq.);

(B) is a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all acts amendatory thereof and supplementary thereto; or

(C) is an organization not organized to carry on business for its own profit or that of its members; and

(ii) includes any entity or person that controls, is controlled by, or is under common control with the covered entity.

(b) "Covered entity" does not include:

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

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

(iii) an entity that serves as a 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.

(c) An entity shall not be considered to be a covered entity for purposes of this article in so far as the entity is acting as a service provider as defined in subdivision thirty of this section.

9. "Covered language" means the ten languages with the most users in the United States, according to the most recent United States Census.

10. "Covered minor" means an individual under the age of seventeen.

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

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

(b) publicly commits in a clear and conspicuous manner:

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

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

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

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

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

12. "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.

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

14. "Division" means the division of consumer protection.

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

16. "Employee data" means:

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

1 for purposes related to the employee's status as a current or former job
2 applicant of such employer;

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

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

14 (d) emergency contact information collected by an employer that
15 relates to an employee of that employer, if such information is
16 collected, processed, or transferred solely for the purpose of having an
17 emergency contact on file for the employee and for processing or trans-
18 ferring such information in case of an emergency; or

19 (e) information relating to an employee (or a spouse, dependent, other
20 covered family member, or beneficiary of such employee) that is neces-
21 sary for the employer to collect, process, or transfer solely for the
22 purpose of administering benefits to which such employee (or spouse,
23 dependent, other covered family member, or beneficiary of such employee)
24 is entitled on the basis of the employee's position with that employer.

25 17. "Executive agency" means any department, board, bureau, commis-
26 sion, division, office, council, committee or officer of the state, a
27 public benefit corporation or public authority at least one of whose
28 members is appointed by the governor.

29 18. "First party advertising or marketing" means advertising or
30 marketing conducted by a first party either through direct communi-
31 cations with a user such as direct mail, email, or text message communi-
32 cations, or advertising or marketing conducted entirely within the first
33 party context, such as in a physical location operated by the first
34 party, or on a website or app operated by the first party.

35 19. "Genetic information" means any covered data, regardless of its
36 format, that concerns an individual's genetic characteristics, includ-
37 ing:

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

41 (b) genotypic and phenotypic information that results from analyzing
42 raw sequence data described in paragraph (a) of this subdivision.

43 20. "Individual" means a natural person residing in the state.

44 21. (a) "Knowledge" means:

45 (i) with respect to a covered entity that is a covered high-impact
46 social media company, the entity knew or should have known the individ-
47 ual was a covered minor;

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

52 (iii) with respect to a covered entity or service provider that does
53 not meet the requirements of subparagraph (i) or (ii) of this paragraph,
54 actual knowledge.

1 (b) For purposes of this subdivision, the term "covered high-impact
2 social media company" means a covered entity that provides any inter-
3 net-accessible platform where:

4 (i) such covered entity generates three billion dollars or more in
5 annual revenue;

6 (ii) such platform has three hundred million or more monthly active
7 users for not fewer than three of the preceding twelve months on the
8 online product or service of such covered entity; and

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

11 22. (a) "Large data holder" means a covered entity or service provider
12 that, in the most recent calendar year:

13 (i) had annual gross revenues of two hundred fifty million dollars or
14 more; and

15 (ii) collected, processed, or transferred:

16 (A) the covered data of more than five million individuals or devices
17 that identify or are linked or reasonably linkable to one or more indi-
18 viduals, excluding covered data collected and processed solely for the
19 purpose of initiating, rendering, billing for, finalizing, completing,
20 or otherwise collecting payment for a requested product or service; and

21 (B) the sensitive covered data of more than two hundred thousand indi-
22 viduals or devices that identify or are linked or reasonably linkable to
23 one or more individuals.

24 (b) "Large data holder" does not include any instance in which the
25 covered entity or service provider would qualify as a large data holder
26 solely on the basis of collecting or processing:

27 (i) personal email addresses;

28 (ii) personal telephone numbers; or

29 (iii) log-in information of an individual or device to allow the indi-
30 vidual or device to log in to an account administered by the covered
31 entity or service provider.

32 (c) For purposes of determining whether any covered entity or service
33 provider is a large data holder, the term "revenue", with respect to any
34 covered entity or service provider that is not organized to carry on
35 business for its own profit or that of its members:

36 (i) means the gross receipts the covered entity or service provider
37 received, in whatever form, from all sources, without subtracting any
38 costs or expenses; and

39 (ii) includes contributions, gifts, grants, dues or other assessments,
40 income from investments, and proceeds from the sale of real or personal
41 property.

42 23. "Market research" means the collection, processing, or transfer of
43 covered data as reasonably necessary and proportionate to investigate
44 the market for or marketing of products, services, or ideas, where the
45 covered data is not:

46 (a) integrated into any product or service;

47 (b) otherwise used to contact any individual or individual's device;
48 or

49 (c) used to advertise or market to any individual or individual's
50 device.

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

1 25. (a) "Precise geolocation information" means information that is
2 derived from a device or technology that reveals the past or present
3 physical location of an individual or device that identifies or is
4 linked or reasonably linkable to one or more individuals, with suffi-
5 cient precision to identify street level location information of an
6 individual or device or the location of an individual or device within a
7 range of eighteen hundred fifty feet or less.

8 (b) "Precise geolocation information" does not include geolocation
9 information identifiable or derived solely from the visual content of a
10 legally obtained image, including the location of the device that
11 captured such image.

12 26. "Process" means to conduct or direct any operation or set of oper-
13 ations performed on covered data, including analyzing, organizing,
14 structuring, retaining, storing, using, or otherwise handling covered
15 data.

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

21 28. (a) "Publicly available information" means any information that a
22 covered entity or service provider has a reasonable basis to believe has
23 been lawfully made available to the general public from:

24 (i) federal, state, or local government records, if the covered entity
25 collects, processes, and transfers such information in accordance with
26 any restrictions or terms of use placed on the information by the rele-
27 vant government entity;

28 (ii) widely distributed media;

29 (iii) a website or online service made available to all members of the
30 public, for free or for a fee, including where all members of the
31 public, for free or for a fee, can log in to the website or online
32 service;

33 (iv) a disclosure that has been made to the general public as required
34 by federal, state, or local law; or

35 (v) the visual observation of the physical presence of an individual
36 or a device in a public place, not including data collected by a device
37 in the individual's possession.

38 (b)(i) For purposes of this paragraph, information from a website or
39 online service is not available to all members of the public if the
40 individual who made the information available via the website or online
41 service has restricted the information to a specific audience.

42 (ii) "Publicly available information" does not include:

43 (A) any obscene visual depiction (as defined in section 1460 of title
44 18, United States Code);

45 (B) any inference made exclusively from multiple independent sources
46 of publicly available information that reveals sensitive covered data
47 with respect to an individual;

48 (C) biometric information;

49 (D) publicly available information that has been combined with covered
50 data;

51 (E) genetic information, unless otherwise made available by the indi-
52 vidual to whom the information pertains as described in subparagraph
53 (ii) or (iii) of paragraph (a) of this subdivision; or

54 (F) intimate images known to be nonconsensual.

55 29. (a) "Sensitive covered data" means the following types of covered
56 data:

1 (i) A government-issued identifier, such as a social security number,
2 passport number, or driver's license number, that is not required by law
3 to be displayed in public.

4 (ii) Any information that describes or reveals the past, present, or
5 future physical health, mental health, disability, diagnosis, or health-
6 care condition or treatment of an individual.

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

12 (iv) Biometric information.

13 (v) Genetic information.

14 (vi) Precise geolocation information.

15 (vii) An individual's private communications such as voicemails,
16 emails, texts, direct messages, or mail, or information identifying the
17 parties to such communications, voice communications, video communi-
18 cations, and any information that pertains to the transmission of such
19 communications, including telephone numbers called, telephone numbers
20 from which calls were placed, the time calls were made, call duration,
21 and location information of the parties to the call, unless the covered
22 entity or a service provider acting on behalf of the covered entity is
23 the sender or an intended recipient of the communication. Communi-
24 cations are not private for purposes of this clause if such communi-
25 cations are made from or to a device provided by an employer to an
26 employee insofar as such employer provides conspicuous notice that such
27 employer may access such communications.

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

30 (ix) Information identifying the sexual behavior of an individual in a
31 manner inconsistent with the individual's reasonable expectation regard-
32 ing the collection, processing, or transfer of such information.

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

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

43 (xii) Information revealing the video content requested or selected by
44 an individual collected by a covered entity that is not a provider of a
45 service described in subdivision four of section sixteen hundred eleven
46 of this article. This subparagraph does not include covered data used
47 solely for transfers for independent video measurement.

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

50 (xiv) An individual's race, color, ethnicity, religion, or union
51 membership.

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

54 (xvi) Any other covered data collected, processed, or transferred for
55 the purpose of identifying the types of covered data listed in subpara-
56 graphs (i) through (xv) of this paragraph.

(b) The director of the division of consumer protection may promulgate rules and regulations to include in the definition of "sensitive covered data" any other type of covered data that may require a similar level of protection as the types of covered data listed in subparagraphs (i) through (xvi) of paragraph (a) of this subdivision as a result of any new method of collecting, processing, or transferring covered data.

30. (a) "Service provider" means a person or entity that:

(i) 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

(ii) receives covered data from or on behalf of a covered entity or a federal, state, tribal, territorial, or local government entity.

(b) A service provider that receives service provider data from another service provider as permitted under this article shall be treated as a service provider under this article with respect to such data.

31. "Service provider data" means covered data that is collected or processed by or has been transferred to a service provider by or on behalf of a covered entity, a federal, state, tribal, territorial, or local government entity, or another service provider for the purpose of allowing the service provider to whom such covered data is transferred to perform a service or function on behalf of, and at the direction of, such covered entity or federal, state, tribal, territorial, or local government entity.

32. The term "state privacy authority" means the director of the division of consumer protection.

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

34. (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; and

(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 solely for measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.

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

(i) collects, processes, or transfers covered data that the person or entity did not collect directly from the individual linked or linkable to such covered data; and

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

(b) Third party does not include a person or entity that collects covered data from another entity if the two entities are related by common ownership or corporate control, but only if a reasonable consum-

er's reasonable expectation would be that such entities share information.

36. (a) "Third-party collecting entity":

(i) 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

(ii) 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.

(b) For purposes of this subdivision, the term "principal source of revenue" means, for the prior twelve-month period, either:

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

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

(c) An entity may not be considered to be a third-party collecting entity for purposes of this article if the entity is acting as a service provider.

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

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

39. "Unique identifier":

(a) means an identifier to the extent that such identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to 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; and

(b) does not include an identifier assigned by a covered entity for the specific purpose of giving effect to an individual's exercise of affirmative express consent or opt-outs of the collection, processing, and transfer of covered data pursuant to section sixteen hundred twenty-three of this article or otherwise limiting the collection, processing, or transfer of such information.

40. "Widely distributed media" means information that is available to the general public, including information from a telephone book or online directory, a television, internet, or radio program, the news media, or an internet site that is available to the general public on an unrestricted basis, but does not include an obscene visual depiction (as defined in section 1460 of title 18, United States Code).

TITLE II

DUTY OF LOYALTY

Section 1610. Data minimization.

1611. Loyalty duties.

1612. Privacy by design.

1613. Loyalty to individuals with respect to pricing.

§ 1610. Data minimization. 1. A covered entity may not collect, process, or transfer covered data unless the collection, processing, or

1 transfer is limited to what is reasonably necessary and proportionate
2 to:

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

5 (b) effect a purpose permitted under subdivision two of this section.

6 2. A covered entity may collect, process, or transfer covered data for
7 any of the following purposes if the collection, processing, or transfer
8 is limited to what is reasonably necessary and proportionate to such
9 purpose:

10 (a) To initiate, manage, or complete a transaction or fulfill an order
11 for specific products or services requested by an individual, including
12 any associated routine administrative, operational, and account-servic-
13 ing activity such as billing, shipping, delivery, storage, and account-
14 ing.

15 (b) With respect to covered data previously collected in accordance
16 with this article, notwithstanding this exception:

17 (i) to process such data as necessary to perform system maintenance or
18 diagnostics;

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

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

23 (iv) to perform inventory management or reasonable network management;

24 (v) to protect against spam; or

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

27 (c) To authenticate users of a product or service.

28 (d) To fulfill a product or service warranty.

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

33 (f) To prevent, detect, protect against, or respond to fraud, harass-
34 ment, or illegal activity. For purposes of this paragraph, the term
35 "illegal activity" means a violation of a federal, state, or local law
36 punishable as a felony or misdemeanor that can directly harm.

37 (g) To comply with a legal obligation imposed by federal, tribal,
38 local, or state law, or to investigate, establish, prepare for, exer-
39 cise, or defend legal claims involving the covered entity or service
40 provider.

41 (h) To prevent an individual, or group of individuals, from suffering
42 harm where the covered entity or service provider believes in good faith
43 that the individual, or group of individuals, is at risk of death, seri-
44 ous physical injury, or other serious health risk.

45 (i) To effectuate a product recall pursuant to federal or state law.

46 (j) (i) To conduct a public or peer-reviewed scientific, historical,
47 or statistical research project that:

48 (A) is in the public interest; and

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

52 (ii) Not later than eighteen months after the effective date of this
53 article, the division should issue guidelines to help covered entities
54 ensure the privacy of affected users and the security of covered data,
55 particularly as data is being transferred to and stored by researchers.
56 Such guidelines should consider risks as they pertain to projects using

1 covered data with special considerations for projects that are exempt
2 under part 46 of title 45, Code of Federal Regulations (Protection of
3 Human Subjects under United States Law) (or any successor regulation) or
4 are excluded from the criteria for institutional review board review.

5 (k) To deliver a communication that is not an advertisement to an
6 individual, if the communication is reasonably anticipated by the indi-
7 vidual within the context of the individual's interactions with the
8 covered entity.

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

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

16 (i) a notice describing such transfer, including the name of the enti-
17 ty or entities receiving the individual's covered data and their privacy
18 policies as described in section sixteen hundred twenty-one of this
19 article; and

20 (ii) a reasonable opportunity to withdraw any previously given
21 consents in accordance with the requirements of affirmative express
22 consent under this article related to the individual's covered data and
23 a reasonable opportunity to request the deletion of the individual's
24 covered data, as described in section sixteen hundred twenty-two of this
25 article.

26 (n) To ensure the data security and integrity of covered data, as
27 described in section sixteen hundred twenty-seven of this article.

28 (o) With respect to covered data previously collected in accordance
29 with this article, a service provider acting at the direction of a
30 government entity, or a service provided to a government entity by a
31 covered entity, and only insofar as authorized by statute, to prevent,
32 detect, protect against or respond to a public safety incident, includ-
33 ing trespass, natural disaster, or national security incident. This
34 paragraph does not permit, however, the transfer of covered data for
35 payment or other valuable consideration to a government entity.

36 (p) With respect to covered data collected in accordance with this
37 article, notwithstanding this exception, to process such data as neces-
38 sary to provide first party advertising or marketing of products or
39 services provided by the covered entity for individuals who are not-cov-
40 ered minors.

41 (q) With respect to covered data previously collected in accordance
42 with this article, notwithstanding this exception and provided such
43 collection, processing, and transferring otherwise complies with the
44 requirements of this article, including subdivision three of section
45 sixteen hundred twenty-three of this article, to provide targeted adver-
46 tising.

47 3. The division shall issue guidance regarding what is reasonably
48 necessary and proportionate to comply with this section. Such guidance
49 shall take into consideration:

50 (a) the size of, and the nature, scope, and complexity of the activ-
51 ities engaged in by, the covered entity, including whether the covered
52 entity is a large data holder, nonprofit organization, covered entity
53 meeting the requirements of section sixteen hundred twenty-eight of this
54 article, third party, or third-party collecting entity;

55 (b) the sensitivity of covered data collected, processed, or trans-
56 ferred by the covered entity;

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

3 (d) the number of individuals and devices to which the covered data
4 collected, processed, or transferred by the covered entity relates.

5 4. A covered entity or service provider may not engage in deceptive
6 advertising or marketing with respect to a product or service offered to
7 an individual.

8 5. Nothing in this article shall be construed to limit or diminish
9 First Amendment freedoms guaranteed under the Constitution of the United
10 States or under the state constitution.

11 § 1611. Loyalty duties. 1. Notwithstanding the provisions of section
12 sixteen hundred ten of this title, and unless an exception applies, with
13 respect to covered data, a covered entity or service provider may not:

14 (a) collect, process, or transfer a social security number, except
15 when necessary to facilitate an extension of credit, authentication,
16 fraud and identity fraud detection and prevention, the payment or
17 collection of taxes, the enforcement of a contract between parties, or
18 the prevention, investigation, or prosecution of fraud or illegal activ-
19 ity, or as otherwise required by federal, state, or local law;

20 (b) collect or process sensitive covered data, except where such
21 collection or processing is strictly necessary to provide or maintain a
22 specific product or service requested by the individual to whom the
23 covered data pertains, or is strictly necessary to effect a purpose
24 enumerated in paragraphs (a) through (l) and (n) through (o) of subdivi-
25 sion two of section sixteen hundred ten of this title;

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

28 (i) the transfer is made pursuant to the affirmative express consent
29 of the individual;

30 (ii) the transfer is necessary to comply with a legal obligation
31 imposed by federal, state, tribal, or local law, or to establish, exer-
32 cise, or defend legal claims;

33 (iii) the transfer is necessary to prevent an individual from imminent
34 injury where the covered entity believes in good faith that the individ-
35 ual is at risk of death, serious physical injury, or serious health
36 risk;

37 (iv) with respect to covered data collected in accordance with this
38 article, notwithstanding this exception, a service provider acting at
39 the direction of a government entity, or a service provided to a govern-
40 ment entity by a covered entity, and only insofar as authorized by stat-
41 ute, the transfer is necessary to prevent, detect, protect against or
42 respond to a public safety incident including trespass, natural disas-
43 ter, or national security incident. This paragraph does not permit,
44 however, the transfer of covered data for payment or other valuable
45 consideration to a government entity;

46 (v) in the case of the transfer of a password, the transfer is neces-
47 sary to use a designated password manager or is to a covered entity for
48 the exclusive purpose of identifying passwords that are being re-used
49 across sites or accounts;

50 (vi) in the case of the transfer of genetic information, the transfer
51 is necessary to perform a medical diagnosis or medical treatment specif-
52 ically requested by an individual, or to conduct medical research in
53 accordance with conditions of paragraph (j) of subdivision two of
54 section sixteen hundred ten of this title; or

55 (vii) to transfer assets in the manner described in paragraph (m) of
56 subdivision two of section sixteen hundred ten of this title; or

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

§ 1612. Privacy by design. 1. A covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data and that:

(a) consider applicable federal laws, rules, or regulations related to covered data the covered entity or service provider collects, processes, or transfers;

(b) identify, assess, and mitigate privacy risks related to covered minors (including, if applicable, with respect to a covered entity that is not an entity meeting the requirements of section sixteen hundred twenty-eight of this article, in a manner that considers the developmental needs of different age ranges of covered minors) to result in reasonably necessary and proportionate residual risk to covered minors;

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

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

2. The policies, practices, and procedures established by a covered entity and a service provider under subdivision one of this section, shall correspond with, as applicable:

(a) 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, entity meeting the requirements of section sixteen hundred twenty-eight of this article, third party, or third-party collecting entity, taking into account the role of the covered entity or service provider and the information available to it;

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

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

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

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

3. Not later than one year after the date of enactment of this article, the division shall issue guidance as to what constitutes reasonable policies, practices, and procedures as required by this section. The division shall consider unique circumstances applicable to nonprofit organizations, to entities meeting the requirements of section sixteen hundred twenty-eight of this article, and to service providers.

§ 1613. Loyalty to individuals with respect to pricing. 1. A covered entity may not retaliate against an individual for exercising any of the rights guaranteed by this article, or any regulations promulgated under this article, 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.

2. Nothing in subdivision one of this section may be construed to:

(a) 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;

(b) 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 program;

(c) 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;

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

(e) 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 paragraph (c) of subdivision one of section sixteen hundred twenty-two of this article; or

(f) 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.

3. For purposes of this section, the term "bona fide loyalty program" includes rewards, premium features, discount or club card programs.

TITLE III

CONSUMER DATA RIGHTS

Section 1620. Consumer awareness.

1621. Transparency.

1622. Individual data ownership and control.

1623. Right to consent and object.

1624. Data protections for children and minors.

1625. Third-party collecting entities.

1626. Civil rights and algorithms.

1627. Data security and protection of covered data.

1628. Small business protections.

1629. Unified opt-out mechanisms.

§ 1620. Consumer awareness. 1. Not later than ninety days after the effective date of this article, the division shall publish, on the public website of the division, a webpage that describes each provision, right, obligation, and requirement of this article, listed separately

1 for individuals and for covered entities and service providers, and the
2 remedies, exemptions, and protections associated with this article, in
3 plain and concise language and in an easy-to-understand manner.

4 2. The division shall update the information published under subdivi-
5 sion one of this section on a quarterly basis as necessitated by any
6 change in law, regulation, guidance, or judicial decisions.

7 3. The division shall publish the information required to be published
8 under subdivision one of this section in the ten languages with the most
9 users in the state, according to the most recent United States Census.

10 § 1621. Transparency. 1. Each covered entity shall make publicly
11 available, in a clear, conspicuous, not misleading, and easy-to-read and
12 readily accessible manner, a privacy policy that provides a detailed and
13 accurate representation of the data collection, processing, and transfer
14 activities of the covered entity.

15 2. A covered entity or service provider shall have a privacy policy
16 that includes, at a minimum, the following:

17 (a) The identity and the contact information of:

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

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

25 (b) The categories of covered data the covered entity or service
26 provider collects or processes.

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

29 (d) Whether the covered entity or service provider transfers covered
30 data and, if so, each category of service provider and third party to
31 which the covered entity or service provider transfers covered data, the
32 name of each third-party collecting entity to which the covered entity
33 or service provider transfers covered data, and the purposes for which
34 such data is transferred to such categories of service providers and
35 third parties or third-party collecting entities, except for a transfer
36 to a governmental entity pursuant to a court order or law that prohibits
37 the covered entity or service provider from disclosing such transfer.

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

43 (f) A prominent description of how an individual can exercise the
44 rights described in this article.

45 (g) A general description of the covered entity's or service provid-
46 er's data security practices.

47 (h) The effective date of the privacy policy.

48 (i) Whether or not any covered data collected by the covered entity or
49 service provider is transferred to, processed in, stored in, or other-
50 wise accessible to the People's Republic of China, Russia, Iran, or
51 North Korea.

52 3. The privacy policy required under subdivision one of this section
53 shall be made available to the public in each covered language in which
54 the covered entity or service provider:

55 (a) provides a product or service that is subject to the privacy poli-
56 cy; or

1 (b) carries out activities related to such product or service.

2 4. The covered entity or service provider shall also provide the
3 disclosures under this section in a manner that is reasonably accessible
4 to and usable by individuals with disabilities.

5 5. (a) If a covered entity makes a material change to its privacy
6 policy or practices, the covered entity shall notify each individual
7 affected by such material change before implementing the material change
8 with respect to any prospectively collected covered data and, except as
9 provided in paragraphs (a) through (o) of subdivision two of section
10 sixteen hundred ten of this article, provide a reasonable opportunity
11 for each individual to withdraw consent to any further materially
12 different collection, processing, or transfer of previously collected
13 covered data under the changed policy.

14 (b) The covered entity shall take all reasonable electronic measures
15 to provide direct notification regarding material changes to the privacy
16 policy to each affected individual, in each covered language in which
17 the privacy policy is made available, and taking into account available
18 technology and the nature of the relationship.

19 (c) Nothing in this section may be construed to affect the require-
20 ments for covered entities under section sixteen hundred eleven or
21 sixteen hundred twenty-three of this article.

22 (d) Each large data holder shall retain copies of previous versions of
23 its privacy policy for at least ten years beginning after the date of
24 enactment of this article and publish them on its website. Such large
25 data holder shall make publicly available, in a clear, conspicuous, and
26 readily accessible manner, a log describing the date and nature of each
27 material change to its privacy policy over the past ten years. The
28 descriptions shall be sufficient for a reasonable individual to under-
29 stand the material effect of each material change. The obligations in
30 this paragraph shall not apply to any previous versions of a large data
31 holder's privacy policy, or any material changes to such policy, that
32 precede the date of enactment of this article.

33 6. (a) In addition to the privacy policy required under subdivision
34 one of this section, a large data holder that is a covered entity shall
35 provide a short-form notice of its covered data practices in a manner
36 that is:

37 (i) concise, clear, conspicuous, and not misleading;

38 (ii) readily accessible to the individual, based on what is reasonably
39 anticipated within the context of the relationship between the individ-
40 ual and the large data holder;

41 (iii) inclusive of an overview of individual rights and disclosures to
42 reasonably draw attention to data practices that may reasonably be unex-
43 pected to a reasonable person or that involve sensitive covered data;
44 and

45 (iv) no more than five hundred words in length.

46 (b) The division shall promulgate rules and regulations establishing
47 the minimum data disclosures necessary for the short-form notice
48 required under paragraph (a) of this subdivision, which shall not exceed
49 the content requirements in subdivision two of this section and shall
50 include templates or models of short-form notices.

51 § 1622. Individual data ownership and control. 1. In accordance with
52 subdivisions two and three of this section, a covered entity shall
53 provide an individual, after receiving a verified request from the indi-
54 vidual, with the right to:

55 (a) access:

1 (i) in a human-readable format that a reasonable individual can under-
2 stand and download from the internet, the covered data (except covered
3 data in a back-up or archival system) of the individual making the
4 request that is collected, processed, or transferred by the covered
5 entity or any service provider of the covered entity within the twenty-
6 four months preceding the request;

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

13 (iii) a description of the purpose for which the covered entity trans-
14 ferred the covered data of the individual to a third party or service
15 provider;

16 (b) correct any verifiable substantial inaccuracy or substantially
17 incomplete information with respect to the covered data of the individ-
18 ual that is processed by the covered entity and instruct the covered
19 entity to make reasonable efforts to notify all third parties or service
20 providers to which the covered entity transferred such covered data of
21 the corrected information;

22 (c) delete covered data of the individual that is processed by the
23 covered entity and instruct the covered entity to make reasonable
24 efforts to notify all third parties or service provider to which the
25 covered entity transferred such covered data of the individual's
26 deletion request; and

27 (d) to the extent technically feasible, export to the individual or
28 directly to another entity the covered data of the individual that is
29 processed by the covered entity, including inferences linked or reason-
30 ably linkable to the individual but not including other derived data,
31 without licensing restrictions that limit such transfers in:

32 (i) a human-readable format that a reasonable individual can under-
33 stand and download from the internet; and

34 (ii) a portable, structured, interoperable, and machine-readable
35 format.

36 2. A covered entity may not condition, effectively condition, attempt
37 to condition, or attempt to effectively condition the exercise of a
38 right described in subdivision one of this section through:

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

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

45 3. (a) Subject to subdivisions four and five of this section, each
46 request under subdivision one of this section shall be completed by any:

47 (i) large data holder within forty-five days of such request from an
48 individual, unless it is demonstrably impracticable or impracticably
49 costly to verify such individual;

50 (ii) covered entity that is not a large data holder or a covered enti-
51 ty meeting the requirements of section sixteen hundred twenty-eight of
52 this title within sixty days of such request from an individual, unless
53 it is demonstrably impracticable or impracticably costly to verify such
54 individual; or

55 (iii) covered entity meeting the requirements of section sixteen
56 hundred twenty-eight of this title within ninety days of such request

1 from an individual, unless it is demonstrably impracticable or impracti-
2 cably costly to verify such individual.

3 (b) A response period set forth in this subdivision may be extended
4 once by forty-five additional days when reasonably necessary, consider-
5 ing the complexity and number of the individual's requests, so long as
6 the covered entity informs the individual of any such extension within
7 the initial forty-five-day response period, together with the reason for
8 the extension.

9 4. A covered entity:

10 (a) shall provide an individual with the opportunity to exercise each
11 of the rights described in subdivision one of this section; and

12 (b) with respect to:

13 (i) the first two times that an individual exercises any right
14 described in subdivision one of this section in any twelve-month period,
15 shall allow the individual to exercise such right free of charge; and

16 (ii) any time beyond the initial two times described in subparagraph
17 (i) of this paragraph, may allow the individual to exercise such right
18 for a reasonable fee for each request.

19 5. (a) A covered entity may not permit an individual to exercise a
20 right described in subdivision one of this section, in whole or in part,
21 if the covered entity:

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

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

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

30 (iv) reasonably believes that the exercise of the right would require
31 the covered entity to engage in an unfair or deceptive practice under
32 section 5 of the Federal Trade Division Act (15 U.S.C. 45); or

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

36 (b) If a covered entity cannot reasonably verify that a request to
37 exercise a right described in subdivision one of this section is made by
38 the individual whose covered data is the subject of the request (or an
39 individual authorized to make such a request on the individual's
40 behalf), the covered entity:

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

44 (ii) may not process or transfer such additional information for any
45 other purpose.

46 (c) (i) A covered entity may decline, with adequate explanation to the
47 individual, to comply with a request to exercise a right described in
48 subdivision one of this section, in whole or in part, that would:

49 (A) require the covered entity to retain any covered data collected
50 for a single, one-time transaction, if such covered data is not proc-
51 essed or transferred by the covered entity for any purpose other than
52 completing such transaction;

53 (B) be demonstrably impracticable or prohibitively costly to comply
54 with, and the covered entity shall provide a description to the reque-
55 stor detailing the inability to comply with the request;

1 (C) require the covered entity to attempt to re-identify de-identified
2 data;

3 (D) require the covered entity to maintain covered data in an iden-
4 tifiable form or collect, retain, or access any data in order to be
5 capable of associating a verified individual request with covered data
6 of such individual;

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

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

11 (G) interfere with law enforcement, judicial proceedings, investi-
12 gations, or reasonable efforts to guard against, detect, prevent, or
13 investigate fraudulent, malicious, or unlawful activity, or enforce
14 valid contracts;

15 (H) violate federal or state law or the rights and freedoms of another
16 individual, including under the Constitution of the United States or the
17 state constitution;

18 (I) prevent a covered entity from being able to maintain a confiden-
19 tial record of deletion requests, maintained solely for the purpose of
20 preventing covered data of an individual from being recollected after
21 the individual submitted a deletion request and requested that the
22 covered entity no longer collect, process, or transfer such data;

23 (J) fall within an exception enumerated in the regulations promulgated
24 by the division pursuant to subparagraph (iv) of this subdivision; or

25 (K) with respect to requests for deletion;

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

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

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

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

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

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

42 (ii) In a circumstance that would allow a denial pursuant to subpara-
43 graph (i) of this subdivision, a covered entity shall partially comply
44 with the remainder of the request if it is possible and not unduly
45 burdensome to do so.

46 (iii) For purposes of clause (B) of subparagraph (i) of this para-
47 graph, the receipt of a large number of verified requests, on its own,
48 may not be considered to render compliance with a request demonstrably
49 impracticable.

50 (iv) The division may, by regulation as described in subdivision seven
51 of this section, establish additional permissive exceptions necessary to
52 protect the rights of individuals, alleviate undue burdens on covered
53 entities, prevent unjust or unreasonable outcomes from the exercise of
54 access, correction, deletion, or portability rights, or as otherwise
55 necessary to fulfill the purposes of this section. In establishing such
56 exceptions, the division should consider any relevant changes in tech-

1 nology, means for protecting privacy and other rights, and beneficial
2 uses of covered data by covered entities.

3 6. A large data holder that is a covered entity shall, for each calen-
4 dar year in which it was a large data holder, do the following:

5 (a) Compile the following metrics for the prior calendar year:

6 (i) The number of verified access requests under paragraph (a) of
7 subdivision one of this section.

8 (ii) The number of verified deletion requests under paragraph (c) of
9 subdivision one of this section.

10 (iii) The number of requests to opt-out of covered data transfers
11 under subdivision two of section sixteen hundred twenty-three of this
12 title.

13 (iv) The number of requests to opt-out of targeted advertising under
14 subdivision three of section sixteen hundred twenty-three of this title.

15 (v) The number of requests in each of subparagraphs (i) through (iv)
16 of this paragraph that such large data holder (A) complied with in whole
17 or in part and (B) denied.

18 (vi) The median or mean number of days within which such large data
19 holder substantively responded to the requests in each of subparagraphs
20 (i) through (iv) of this paragraph.

21 (b) Disclose by July first of each applicable calendar year the infor-
22 mation compiled in paragraph (a) of this subdivision within such large
23 data holder's privacy policy required under section sixteen hundred
24 twenty-one of this title or on the publicly accessible website of such
25 large data holder that is accessible from a hyperlink included in the
26 privacy policy.

27 7. Not later than two years after the effective date of this article,
28 the division shall promulgate rules and regulations as necessary to
29 establish processes by which covered entities are to comply with the
30 provisions of this section. Such regulations shall take into consider-
31 ation:

32 (a) the size of, and the nature, scope, and complexity of the activ-
33 ities engaged in by the covered entity, including whether the covered
34 entity is a large data holder, nonprofit organization, covered entity
35 meeting the requirements of section sixteen hundred twenty-eight of this
36 title, third party, or third-party collecting entity;

37 (b) the sensitivity of covered data collected, processed, or trans-
38 ferred by the covered entity;

39 (c) the volume of covered data collected, processed, or transferred by
40 the covered entity;

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

43 (e) after consulting the National Institute of Standards and Technolo-
44 gy, standards for ensuring the deletion of covered data under this arti-
45 cle where appropriate.

46 8. A covered entity shall facilitate the ability of individuals to
47 make requests under subdivision one of this section in any covered
48 language in which the covered entity provides a product or service. The
49 mechanisms by which a covered entity enables individuals to make
50 requests under subdivision one of this section shall be readily accessi-
51 ble and usable by individuals with disabilities.

52 § 1623. Right to consent and object. 1. A covered entity shall provide
53 an individual with a clear and conspicuous, easy-to-execute means to
54 withdraw any affirmative express consent previously provided by the
55 individual that is as easy to execute by a reasonable individual as the

1 means to provide consent, with respect to the processing or transfer of
2 the covered data of the individual.

3 2. (a) A covered entity:

4 (i) may not transfer or direct the transfer of the covered data of an
5 individual to a third party if the individual objects to the transfer;
6 and

7 (ii) shall allow an individual to object to such a transfer through an
8 opt-out mechanism, as described in section sixteen hundred twenty-nine
9 of this title.

10 (b) Except as provided in subparagraph (iii) of paragraph (c) of
11 subdivision two of section sixteen hundred twenty-five of this title, a
12 covered entity need not allow an individual to opt out of the
13 collection, processing, or transfer of covered data made pursuant to the
14 exceptions in paragraphs (a) through (o) of subdivision two of section
15 sixteen hundred ten of this article.

16 3. (a) A covered entity or service provider that directly delivers a
17 targeted advertisement shall:

18 (i) prior to engaging in targeted advertising to an individual or
19 device and at all times thereafter, provide such individual with a clear
20 and conspicuous means to opt out of targeted advertising;

21 (ii) abide by any opt-out designation by an individual with respect to
22 targeted advertising and notify the covered entity that directed the
23 service provider to deliver the targeted advertisement of the opt-out
24 decision; and

25 (iii) allow an individual to make an opt-out designation with respect
26 to targeted advertising through an opt-out mechanism, as described in
27 section sixteen hundred twenty-nine of this title.

28 (b) A covered entity or service provider that receives an opt-out
29 notification pursuant to subparagraph (ii) of paragraph (a) of this
30 subdivision or this paragraph shall abide by such opt-out designations
31 by an individual and notify any other person that directed the covered
32 entity or service provider to serve, deliver, or otherwise handle the
33 advertisement of the opt-out decision.

34 4. A covered entity may not condition, effectively condition, attempt
35 to condition, or attempt to effectively condition the exercise of any
36 individual right under this section through:

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

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

43 § 1624. Data protections for children and minors. 1. A covered entity
44 may not engage in targeted advertising to any individual if the covered
45 entity has knowledge that the individual is a covered minor.

46 2. (a) A covered entity may not transfer or direct the transfer of the
47 covered data of a covered minor to a third party if the covered entity:

48 (i) has knowledge that the individual is a covered minor; and

49 (ii) has not obtained affirmative express consent from the covered
50 minor or the covered minor's parent or guardian.

51 (b) A covered entity or service provider may collect, process, or
52 transfer covered data of an individual the covered entity or service
53 provider knows is under the age of eighteen solely in order to submit
54 information relating to child victimization to law enforcement or to the
55 nonprofit, national resource center and clearinghouse designated to

1 provide assistance to victims, families, child-serving professionals,
2 and the general public on missing and exploited children issues.

3 3. (a) There is established within the division in the privacy bureau
4 established in title V of this article, an office to be known as the
5 "Youth Privacy and Marketing Office" (the "office").

6 (b) The office shall be headed by a director, who shall be appointed
7 by the chair of the office.

8 (c) The office shall be responsible for assisting the division in
9 addressing, as it relates to this article:

10 (i) the privacy of children and minors; and

11 (ii) marketing directed at children and minors.

12 (d) The director of the office shall hire adequate staff to carry out
13 the duties described in paragraph (c) of this subdivision, including by
14 hiring individuals who are experts in data protection, digital advertis-
15 ing, data analytics, and youth development.

16 (e) Not later than two years after the effective date of this article,
17 and annually thereafter, the office shall submit to the governor, the
18 majority and minority leaders of the senate and the majority and minori-
19 ty leaders of the assembly a report that includes:

20 (i) a description of the work of the office regarding emerging
21 concerns relating to youth privacy and marketing practices; and

22 (ii) an assessment of how effectively the office has, during the peri-
23 od for which the report is submitted, assisted the division to address
24 youth privacy and marketing practices.

25 (f) Not later than ten days after the date on which a report is
26 submitted under paragraph (e) of this subdivision, the division shall
27 publish the report on its website.

28 § 1625. Third-party collecting entities. 1. (a) Each third-party
29 collecting entity shall place a clear, conspicuous, not misleading, and
30 readily accessible notice on the website or mobile application of the
31 third-party collecting entity (if the third-party collecting entity
32 maintains such a website or mobile application) that:

33 (a) notifies individuals that the entity is a third-party collecting
34 entity using specific language that the division shall develop through
35 rulemaking under section 553 of title 5, United States Code;

36 (b) includes a link to the website established under paragraph (c) of
37 subdivision two of this section; and

38 (c) is reasonably accessible to and usable by individuals with disa-
39 bilities.

40 2. (a) Not later than January thirty-first of each calendar year that
41 follows a calendar year during which a covered entity acted as a third-
42 party collecting entity and processed covered data pertaining to more
43 than five thousand individuals or devices that identify or are linked or
44 reasonably linkable to an individual, such covered entity shall register
45 with the division in accordance with this subdivision.

46 (b) In registering with the division as required under paragraph (a)
47 of this subdivision, a third-party collecting entity shall do the
48 following:

49 (i) Pay to the division a registration fee of one hundred dollars.

50 (ii) Provide the division with the following information:

51 (A) the legal name and primary physical, email, and internet addresses
52 of the third-party collecting entity;

53 (B) a description of the categories of covered data the third-party
54 collecting entity processes and transfers;

1 (C) the contact information of the third-party collecting entity,
2 including a contact person, a telephone number, an email address, a
3 website, and a physical mailing address; and

4 (D) a link to a website through which an individual may easily exer-
5 cise the rights provided under this subdivision.

6 (c) The division shall establish and maintain on a website a searcha-
7 ble, publicly available, central registry of third-party collecting
8 entities that are registered with the division under this subdivision
9 that includes the following:

10 (i) A listing of all registered third-party collecting entities and a
11 search feature that allows members of the public to identify individual
12 third-party collecting entities.

13 (ii) For each registered third-party collecting entity, the informa-
14 tion provided under paragraph (b) of this subdivision.

15 (iii) (A) A "Do Not Collect" registry link and mechanism by which an
16 individual may, easily submit a request to all registered third-party
17 collecting entities that are not consumer reporting agencies (as defined
18 in section 603(f) of the Fair Credit Reporting Act (15 U.S.C.
19 1681a(f))), and to the extent such third-party collecting entities are
20 not acting as consumer reporting agencies (as so defined), to:

21 (I) delete all covered data related to such individual that the third-
22 party collecting entity did not collect from such individual directly or
23 when acting as a service provider; and

24 (II) ensure that the third-party collecting entity no longer collects
25 covered data related to such individual without the affirmative express
26 consent of such individual, except insofar as the third-party collecting
27 entity is acting as a service provider.

28 (B) Each third-party collecting entity that receives such a request
29 from an individual shall delete all the covered data of the individual
30 not later than thirty days after the request is received by the third-
31 party collecting entity.

32 (C) Notwithstanding the provisions of clauses (A) and (B) of this
33 subparagraph, a third-party collecting entity may decline to fulfill a
34 "Do Not Collect" request from an individual who it has actual knowledge
35 has been convicted of a crime related to the abduction or sexual exploi-
36 tation of a child, and the data the entity is collecting is necessary to
37 effectuate the purposes of a national or state-run sex offender registry
38 or the congressionally designated entity that serves as the nonprofit
39 national resource center and clearinghouse to provide assistance to
40 victims, families, child-serving professionals, and the general public
41 on missing and exploited children issues.

42 3. (a) A third-party collecting entity that fails to register or
43 provide the notice as required under this section shall be liable for:

44 (i) a civil penalty of one hundred dollars for each day the third-par-
45 ty collecting entity fails to register or provide notice as required
46 under this section, not to exceed a total of ten thousand dollars for
47 any year; and

48 (ii) an amount equal to the registration fees due under subparagraph
49 (i) of paragraph (b) of subdivision two of this section for each year
50 that the third-party collecting entity failed to register as required
51 under paragraph (a) of such subdivision.

52 (b) Nothing in this subdivision shall be construed as altering, limit-
53 ing, or affecting any enforcement authorities or remedies under this
54 article.

55 § 1626. Civil rights and algorithms. 1. (a) A covered entity or a
56 service provider may not collect, process, or transfer covered data in a

1 manner that discriminates in or otherwise makes unavailable the equal
2 enjoyment of goods or services on the basis of race, color, religion,
3 national origin, sex, or disability.

4 (b) This subdivision shall not apply to:

5 (i) the collection, processing, or transfer of covered data for the
6 purpose of:

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

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

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

12 2. (a) Whenever the division obtains information that a covered entity
13 or service provider may have collected, processed, or transferred
14 covered data in violation of subdivision one of this section, the divi-
15 sion shall transmit such information as allowable under federal and
16 state law to any executive agency with authority to initiate enforcement
17 actions or proceedings relating to such violation.

18 (b) Not later than three years after the effective date of this arti-
19 cle, and annually thereafter, the division shall submit to the senate
20 and the assembly a report that includes a summary of:

21 (i) the types of information the division transmitted to executive
22 agencies under paragraph (a) of this subdivision during the previous
23 one-year period; and

24 (ii) how such information relates to federal or state civil rights
25 laws.

26 (c) In transmitting information under paragraph (a) of this subdivi-
27 sion, the division may consult and coordinate with, and provide techni-
28 cal and investigative assistance, as appropriate, to such executive
29 agency.

30 (d) The division may implement this subdivision by executing agree-
31 ments or memoranda of understanding with the appropriate executive agen-
32 cies.

33 3. (a)(i) Notwithstanding any other provision of law, not later than
34 two years after the effective date of this article, and annually there-
35 after, a large data holder that uses a covered algorithm in a manner
36 that poses a consequential risk of harm to an individual or group of
37 individuals, and uses such covered algorithm solely or in part, to
38 collect, process, or transfer covered data shall conduct an impact
39 assessment of such algorithm in accordance with subparagraph (ii) of
40 this paragraph.

41 (ii) The impact assessment required under subparagraph (i) of this
42 paragraph shall provide the following:

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

45 (B) A statement of the purpose and proposed uses of the covered algo-
46 rithm.

47 (C) A detailed description of the data used by the covered algorithm,
48 including the specific categories of data that will be processed as
49 input and any data used to train the model that the covered algorithm
50 relies on, if applicable.

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

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

54 (F) A detailed description of steps the large data holder has taken or
55 will take to mitigate potential harms from the covered algorithm to an
56 individual or group of individuals, including related to:

1 (I) covered minors;

2 (II) making or facilitating advertising for, or determining access to,
3 or restrictions on the use of housing, education, employment, health-
4 care, insurance, or credit opportunities;

5 (III) determining access to, or restrictions on the use of, any place
6 of public accommodation, particularly as such harms relate to the
7 protected characteristics of individuals, including race, color, reli-
8 gion, national origin, sex, or disability;

9 (IV) disparate impact on the basis of individuals' race, color, reli-
10 gion, national origin, sex, or disability status; or

11 (V) disparate impact on the basis of individuals' political party
12 registration status.

13 (b) Notwithstanding any other provision of law, not later than two
14 years after the effective date of this article, a covered entity or
15 service provider that knowingly develops a covered algorithm that is
16 designed, solely or in part, to collect, process, or transfer covered
17 data in furtherance of a consequential decision shall prior to deploying
18 the covered algorithm in interstate commerce evaluate the design, struc-
19 ture, and inputs of the covered algorithm, including any training data
20 used to develop the covered algorithm, to reduce the risk of the poten-
21 tial harms identified under subparagraph (ii) of paragraph (a) of this
22 subdivision.

23 (c) (i) In complying with paragraphs (a) and (b) of this subdivision,
24 a covered entity and a service provider may focus the impact assessment
25 or evaluation on any covered algorithm, or portions of a covered algo-
26 rithm, that will be put to use and may reasonably contribute to the risk
27 of the potential harms identified under subparagraph (ii) of paragraph
28 (a) of this subdivision.

29 (ii) (A) A covered entity and a service provider:

30 (I) shall, not later than thirty days after completing an impact
31 assessment or evaluation, submit the impact assessment or evaluation
32 conducted under paragraphs (a) and (b) of this subdivision to the divi-
33 sion;

34 (II) shall, upon request, make such impact assessment and evaluation
35 available to the legislature; and

36 (III) may make a summary of such impact assessment and evaluation
37 publicly available in a place that is easily accessible to individuals.

38 (B) Covered entities and service providers may redact and segregate
39 any trade secret (as defined in section 1839 of title 18, United States
40 Code) or other confidential or proprietary information from public
41 disclosure under this subparagraph and the division shall abide by its
42 obligations under federal and state law in regard to such information.

43 (iii) The division may not use any information obtained solely and
44 exclusively through a covered entity or a service provider's disclosure
45 of information to the division in compliance with this section for any
46 purpose other than enforcing this article with the exception of enforc-
47 ing consent orders, including the study and report provisions in para-
48 graph (f) of this subdivision. This subparagraph does not preclude the
49 division from providing this information to the legislature in response
50 to a subpoena.

51 (d) Not later than two years after the effective date of this article,
52 the division shall, in consultation with the secretary of state, or
53 their respective designees, publish guidance regarding compliance with
54 this section.

(e) The division shall have authority to promulgate rules and regulations as necessary to establish processes by which a large data holder:

(i) shall submit an impact assessment to the division under item (I) of clause (A) of subparagraph (ii) of paragraph (c) of this subdivision; and

(ii) may exclude from this subdivision any covered algorithm that presents low or minimal consequential risk of harm to an individual or group of individuals.

(f) (i) The division, in consultation with the secretary of state or the secretary's designee, shall conduct a study, to review any impact assessment or evaluation submitted under this subdivision. Such study shall include an examination of:

(A) best practices for the assessment and evaluation of covered algorithms; and

(B) methods to reduce the risk of harm to individuals that may be related to the use of covered algorithms.

(ii) (A) Not later than three years after the effective date of this article, the division, in consultation with the secretary or the secretary's designee, shall submit to the governor and the legislature a report containing the results of the study conducted under subparagraph (i) of this paragraph, together with recommendations for such legislation and administrative action as the division determines appropriate.

(B) Not later than three years after submission of the initial report under clause (A) of this subparagraph, and as the division determines necessary thereafter, the division shall submit to the governor and the legislature an updated version of such report.

§ 1627. Data security and protection of covered data. 1. (a) A covered entity or service provider shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.

(b) The reasonable administrative, technical, and physical data security practices required under paragraph (a) of this subdivision shall be appropriate to:

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

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

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

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

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

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

2. The data security practices of the covered entity and of the service provider required under subdivision one of this section shall include, for each respective entity's own system or systems, at a minimum, the following practices:

(a) Identifying and assessing any material internal and external risk to, and vulnerability in, the security of each system maintained by the covered entity that collects, processes, or transfers covered data, or service provider that collects, processes, or transfers covered data on

1 behalf of the covered entity, including unauthorized access to or risks
2 to such covered data, human vulnerabilities, access rights, and the use
3 of service providers. With respect to large data holders, such activ-
4 ities shall include a plan to receive and reasonably respond to unsolic-
5 ited reports of vulnerabilities by any entity or individual and by
6 performing a reasonable investigation of such reports.

7 (b) Taking preventive and corrective action designed to mitigate
8 reasonably foreseeable risks or vulnerabilities to covered data identi-
9 fied by the covered entity or service provider, consistent with the
10 nature of such risk or vulnerability and the entity's role in collect-
11 ing, processing, or transferring the data. Such action may include
12 implementing administrative, technical, or physical safeguards or chang-
13 es to data security practices or the architecture, installation, or
14 implementation of network or operating software, among other actions.

15 (c) Evaluating and making reasonable adjustments to the action
16 described in paragraph (b) of this subdivision in light of any material
17 changes in technology, internal or external threats to covered data, and
18 the covered entity or service provider's own changing business arrange-
19 ments or operations.

20 (d) Disposing of covered data in accordance with a retention schedule
21 that shall require the deletion of covered data when such data is
22 required to be deleted by law or is no longer necessary for the purpose
23 for which the data was collected, processed, or transferred, unless an
24 individual has provided affirmative express consent to such retention.
25 Such disposal shall include destroying, permanently erasing, or other-
26 wise modifying the covered data to make such data permanently unreadable
27 or indecipherable and unrecoverable to ensure ongoing compliance with
28 this section. Service providers shall establish practices to delete or
29 return covered data to a covered entity as requested at the end of the
30 provision of services unless retention of the covered data is required
31 by law, consistent with paragraph (f) of subdivision one of section
32 sixteen hundred forty-one of this article.

33 (e) Training each employee with access to covered data on how to safe-
34 guard covered data and updating such training as necessary.

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

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

39 3. The division may promulgate technology-neutral rules and regu-
40 lations to establish processes for complying with this section. The
41 division shall consult with the office of information technology
42 services in establishing such processes.

43 § 1628. Small business protections. 1. Any covered entity or service
44 provider that can establish that it met the requirements described in
45 subdivision two of this section for the period of the three preceding
46 calendar years (or for the period during which the covered entity or
47 service provider has been in existence if such period is less than three
48 years) shall:

49 (a) be exempt from compliance with paragraph (d) of subdivision one of
50 section sixteen hundred twenty-two of this title, paragraphs (a), (b),
51 (c), (e), (f) and (g) of subdivision two of section sixteen hundred
52 twenty-seven of this title, and subdivision three of section sixteen
53 hundred forty of this article; and

54 (b) at the covered entity's sole discretion, have the option of
55 complying with paragraph (b) of subdivision one of section sixteen
56 hundred twenty-two of this title by, after receiving a verified request

1 from an individual to correct covered data of the individual under such
2 section, deleting such covered data in its entirety instead of making
3 the requested correction.

4 2. The requirements of this subdivision are, with respect to a covered
5 entity or a service provider, the following:

6 (a) The covered entity or service provider's average annual gross
7 revenues during the period did not exceed forty-one million dollars.

8 (b) The covered entity or service provider, on average, did not annu-
9 ally collect or process the covered data of more than two hundred thou-
10 sand individuals during the period beyond the purpose of initiating,
11 rendering, billing for, finalizing, completing, or otherwise collecting
12 payment for a requested service or product, so long as all covered data
13 for such purpose was deleted or de-identified within ninety days, except
14 when necessary to investigate fraud or as consistent with a covered
15 entity's return policy.

16 (c) The covered entity or service provider did not derive more than
17 fifty percent of its revenue from transferring covered data during any
18 year (or part of a year if the covered entity has been in existence for
19 less than one year) that occurs during the period.

20 3. For purposes of this section, the term "revenue" as it relates to
21 any covered entity or service provider that is not organized to carry on
22 business for its own profit or that of its members, means the gross
23 receipts the covered entity or service provider received in whatever
24 form from all sources without subtracting any costs or expenses, and
25 includes contributions, gifts, grants, dues or other assessments, income
26 from investments, or proceeds from the sale of real or personal proper-
27 ty.

28 § 1629. Unified opt-out mechanisms. 1. For the rights established
29 under subdivisions two and three of section sixteen hundred twenty-three
30 (except as provided for under paragraph (p) of subdivision two of
31 section sixteen hundred ten of this article), and subparagraph (iii) of
32 paragraph (c) of subdivision two of section sixteen hundred twenty-five
33 of this title, following public notice and opportunity to comment and
34 not later than eighteen months after the effective date of this article,
35 the division shall establish or recognize one or more acceptable privacy
36 protective, centralized mechanisms, including global privacy signals
37 such as browser or device privacy settings, other tools offered by
38 covered entities or service providers, and registries of identifiers,
39 for individuals to exercise all such rights through a single interface
40 for a covered entity or service provider to utilize to allow an individ-
41 ual to make such opt-out designations with respect to covered data
42 related to such individual.

43 2. Any such centralized opt-out mechanism shall:

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

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

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

53 (d) permit the covered entity or service provider acting on behalf of
54 a covered entity to have an authentication process the covered entity or
55 service provider acting on behalf of a covered entity may use to deter-
56 mine if the mechanism represents a legitimate request to opt out;

(e) be provided in any covered language in which the covered entity provides products or services subject to the opt-out; and
(f) be provided in a manner that is reasonably accessible to and usable by individuals with disabilities.

TITLE IV
CORPORATE ACCOUNTABILITY

Section 1640. Executive responsibility.

1641. Service providers and third parties.

1642. Technical compliance programs.

1643. Division approved compliance guidelines.

1644. Digital content forgeries.

§ 1640. Executive responsibility. 1. Beginning one year after the effective date of this article, an executive officer of a large data holder shall annually certify, in good faith, to the division, in a manner specified by the division that the entity maintains:

(a) internal controls reasonably designed to comply with this article; and

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

2. A certification submitted under subdivision one of this section 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 ninety days before the submission of the certification. A certification submitted under subdivision one of this section 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.

3. (a) A covered entity or service provider that has more than fifteen employees, shall designate:

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

(ii) one or more qualified employees (in addition to any employee designated under subparagraph (i) of this paragraph) as data security officers.

(b) An employee who is designated by a covered entity or a service provider as a privacy officer or a data security officer pursuant to paragraph (a) of this subdivision shall, at a minimum:

(i) 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 article; and

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

(c) A large data holder shall designate at least one of the officers described in paragraph (a) of this subdivision to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the requirements in paragraph (b) of this subdivision, either directly or through a supervised designee or designees:

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

1 (ii) conduct biennial and comprehensive audits to ensure the policies,
2 practices, and procedures of the large data holder ensure the large data
3 holder is in compliance with this article and ensure such audits are
4 accessible to the division upon request;

5 (iii) develop a program to educate and train employees about compli-
6 ance requirements of this article;

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

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

12 4. (a) Not later than one year after the effective date of this arti-
13 cle or one year after the date on which a covered entity first meets the
14 definition of large data holder, whichever is earlier, and biennially
15 thereafter, each covered entity that is a large data holder shall
16 conduct a privacy impact assessment that weighs the benefits of the
17 large data holder's covered data collecting, processing, and transfer
18 practices against the potential adverse consequences of such practices,
19 including substantial privacy risks, to individual privacy.

20 (b) A privacy impact assessment required under paragraph (a) of this
21 subdivision shall be:

22 (i) reasonable and appropriate in scope given:

23 (A) the nature of the covered data collected, processed, and trans-
24 ferred by the large data holder;

25 (B) the volume of the covered data collected, processed, and trans-
26 ferred by the large data holder; and

27 (C) the potential material risks posed to the privacy of individuals
28 by the collecting, processing, and transfer of covered data by the large
29 data holder;

30 (ii) documented in written form and maintained by the large data hold-
31 er unless rendered out of date by a subsequent assessment conducted
32 under paragraph (a) of this subdivision; and

33 (iii) approved by the privacy protection officer designated in para-
34 graph (c) of subdivision three of this section of the large data holder,
35 as applicable.

36 (c) In assessing the privacy risks, including substantial privacy
37 risks, the large data holder must include reviews of the means by which
38 technologies, including blockchain and distributed ledger technologies
39 and other emerging technologies, are used to secure covered data.

40 5. (a) Not later than one year after the effective date of this arti-
41 cle, and biennially thereafter, each covered entity that is not a large
42 data holder and does not meet the requirements for covered entities
43 under section sixteen hundred twenty-eight of this article shall conduct
44 a privacy impact assessment. Such assessment shall weigh the benefits of
45 the covered entity's covered data collecting, processing, and transfer
46 practices that may cause a substantial privacy risk against the poten-
47 tial material adverse consequences of such practices to individual
48 privacy.

49 (b) A privacy impact assessment required under paragraph (a) of this
50 subdivision shall be:

51 (i) reasonable and appropriate in scope given:

52 (A) the nature of the covered data collected, processed, and trans-
53 ferred by the covered entity;

54 (B) the volume of the covered data collected, processed, and trans-
55 ferred by the covered entity; and

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

4 (ii) documented in written form and maintained by the covered entity
5 unless rendered out of date by a subsequent assessment conducted under
6 paragraph (a) of this subdivision.

7 (c) In assessing the privacy risks, including substantial privacy
8 risks, the covered entity may include reviews of the means by which
9 technologies, including blockchain and distributed ledger technologies
10 and other emerging technologies, are used to secure covered data.

11 § 1641. Service providers and third parties. 1. A service provider:

12 (a) shall adhere to the instructions of a covered entity and only
13 collect, process, and transfer service provider data to the extent
14 necessary and proportionate to provide a service requested by the
15 covered entity, as set out in the contract required by subdivision two
16 of this section, and this paragraph does not require a service provider
17 to collect, process, or transfer covered data if the service provider
18 would not otherwise do so;

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

22 (c) shall assist a covered entity in responding to a request made by
23 an individual under section sixteen hundred twenty-two or sixteen
24 hundred twenty-three of this article, by either:

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

29 (ii) fulfilling a request by a covered entity to execute an individual
30 rights request that the covered entity has determined should be complied
31 with, by either:

32 (A) complying with the request pursuant to the covered entity's
33 instructions; or

34 (B) providing written verification to the covered entity that it does
35 not hold covered data related to the request, that complying with the
36 request would be inconsistent with its legal obligations, or that the
37 request falls within an exception to section sixteen hundred twenty-two
38 or sixteen hundred twenty-three of this article;

39 (d) may engage another service provider for purposes of processing
40 service provider data on behalf of a covered entity only after providing
41 that covered entity with notice and pursuant to a written contract that
42 requires such other service provider to satisfy the obligations of the
43 service provider with respect to such service provider data, including
44 that the other service provider be treated as a service provider under
45 this article;

46 (e) shall, upon the reasonable request of the covered entity, make
47 available to the covered entity information necessary to demonstrate the
48 compliance of the service provider with the requirements of this arti-
49 cle, which may include making available a report of an independent
50 assessment arranged by the service provider on terms agreed to by the
51 service provider and the covered entity, providing information necessary
52 to enable the covered entity to conduct and document a privacy impact
53 assessment required by subdivision four or five of section sixteen
54 hundred forty of this title, and making available the report required
55 under paragraph (b) of subdivision three of section sixteen hundred
56 twenty-six of this article;

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

5 (g) shall develop, implement, and maintain reasonable administrative,
6 technical, and physical safeguards that are designed to protect the
7 security and confidentiality of covered data the service provider proc-
8 esses consistent with section sixteen hundred twenty-seven of this arti-
9 cle; and

10 (h) shall allow and cooperate with, reasonable assessments by the
11 covered entity or the covered entity's designated assessor; alternative-
12 ly, the service provider may arrange for a qualified and independent
13 assessor to conduct an assessment of the service provider's policies and
14 technical and organizational measures in support of the obligations
15 under this article using an appropriate and accepted control standard or
16 framework and assessment procedure for such assessments. The service
17 provider shall provide a report of such assessment to the covered entity
18 upon request.

19 2. (a) A person or entity may only act as a service provider pursuant
20 to a written contract between the covered entity and the service provid-
21 er, or a written contract between one service provider and a second
22 service provider as described under paragraph (d) of subdivision one of
23 this section, if the contract:

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

27 (ii) clearly sets forth:

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

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

30 (C) the type of data subject to collecting, processing, or trans-
31 ferring;

32 (D) the duration of processing; and

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

36 (iii) does not relieve a covered entity or a service provider of any
37 requirement or liability imposed on such covered entity or service
38 provider under this article; and

39 (iv) prohibits:

40 (A) collecting, processing, or transferring covered data in contraven-
41 tion to subdivision one of this section; and

42 (B) combining service provider data with covered data which the
43 service provider receives from or on behalf of another person or persons
44 or collects from the interaction of the service provider with an indi-
45 vidual, provided that such combining is not necessary to effectuate a
46 purpose described in paragraphs (a) through (o) of subdivision two of
47 section sixteen hundred ten of this article and is otherwise permitted
48 under the contract required by this subdivision.

49 (b) Each service provider shall retain copies of previous contracts
50 entered into in compliance with this subdivision with each covered enti-
51 ty to which it provides requested products or services.

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

1 (b) A person that is not limited in its processing of covered data
2 pursuant to the instructions of a covered entity, or that fails to
3 adhere to such instructions, is a covered entity and not a service
4 provider with respect to a specific processing of covered data. A
5 service provider that continues to adhere to the instructions of a
6 covered entity with respect to a specific processing of covered data
7 remains a service provider. If a service provider begins, alone or
8 jointly with others, determining the purposes and means of the process-
9 ing of covered data, it is a covered entity and not a service provider
10 with respect to the processing of such data.

11 (c) A covered entity that transfers covered data to a service provider
12 or a service provider that transfers covered data to a covered entity or
13 another service provider, in compliance with the requirements of this
14 article, is not liable for a violation of this article by the service
15 provider or covered entity to whom such covered data was transferred, if
16 at the time of transferring such covered data, the covered entity or
17 service provider did not have actual knowledge that the service provider
18 or covered entity would violate this article.

19 (d) A covered entity or service provider that receives covered data in
20 compliance with the requirements of this article is not in violation of
21 this article as a result of a violation by a covered entity or service
22 provider from which such data was received.

23 4. A third party:

24 (a) shall not process third party data for a processing purpose other
25 than, in the case of sensitive covered data, the processing purpose for
26 which the individual gave affirmative express consent or to effect a
27 purpose enumerated in paragraph (a), (c), or (e) of subdivision two of
28 section sixteen hundred ten of this article and, in the case of non-sen-
29 sitive data, the processing purpose for which the covered entity made a
30 disclosure pursuant to paragraph (d) of subdivision two of section
31 sixteen hundred twenty-one of this article; and

32 (b) for purposes of paragraph (a) of this subdivision, may reasonably
33 rely on representations made by the covered entity that transferred the
34 third party data if the third party conducts reasonable due diligence on
35 the representations of the covered entity and finds those representa-
36 tions to be credible.

37 5. (a) A covered entity or service provider shall exercise reasonable
38 due diligence in:

39 (i) selecting a service provider; and

40 (ii) deciding to transfer covered data to a third party.

41 (b) Not later than two years after the effective date of this article,
42 the division shall publish guidance regarding compliance with this
43 subdivision, taking into consideration the burdens on large data hold-
44 ers, covered entities who are not large data holders, and covered enti-
45 ties meeting the requirements of section sixteen hundred twenty-eight of
46 this article.

47 6. Solely for the purposes of this section, the requirements for
48 service providers to contract with, assist, and follow the instructions
49 of covered entities shall be read to include requirements to contract
50 with, assist, and follow the instructions of a government entity if the
51 service provider is providing a service to a government entity.

52 § 1642. Technical compliance programs. 1. Not later than three years
53 after the effective date of this article, the division shall promulgate
54 rules and regulations to establish a process for the proposal and
55 approval of technical compliance programs under this section used by a
56 covered entity to collect, process, or transfer covered data.

1 2. The technical compliance programs established under this section
2 shall, with respect to a technology, product, service, or method used by
3 a covered entity to collect, process, or transfer covered data:

4 (i) establish publicly available guidelines for compliance with this
5 article; and

6 (ii) meet or exceed the requirements of this article.

7 3. (a) Any request for approval, amendment, or repeal of a technical
8 compliance program may be submitted to the division by any person,
9 including a covered entity, a representative of a covered entity, an
10 association of covered entities, or a public interest group or organiza-
11 tion. Within ninety days after the request is made, the division shall
12 publish the request and provide an opportunity for public comment on the
13 proposal.

14 (b) Beginning one year after the effective date of this article, the
15 division shall act upon a request for the proposal and approval of a
16 technical compliance program not later than one year after the filing of
17 the request and shall set forth publicly in writing the conclusions of
18 the division with regard to such request.

19 4. Final action by the division on a request for approval, amendment,
20 or repeal of a technical compliance program, or the failure to act with-
21 in the one-year period after a request for approval, amendment, or
22 repeal of a technical compliance program is made under subdivision three
23 of this section, may be appealed to a court of appropriate jurisdiction.

24 5. (a) Prior to commencing an investigation or enforcement action
25 against any covered entity under this article, the division and the
26 attorney general shall consider the covered entity's history of compli-
27 ance with any technical compliance program approved under this section
28 and any action taken by the covered entity to remedy noncompliance with
29 such program. If such enforcement action described in section sixteen
30 hundred fifty-two of this article is brought, the covered entity's
31 history of compliance with any technical compliance program approved
32 under this section and any action taken by the covered entity to remedy
33 noncompliance with such program shall be taken into consideration when
34 determining liability or a penalty. The covered entity's history of
35 compliance with any technical compliance program shall not affect any
36 burden of proof or the weight given to evidence in an enforcement or
37 judicial proceeding.

38 (b) Approval of a technical compliance program shall not limit the
39 authority of the division, including the division's authority to
40 commence an investigation or enforcement action against any covered
41 entity under this article or any other provision of law.

42 (c) Nothing in this subdivision shall provide any individual, class of
43 individuals, or person with any right to seek discovery of any non-publ-
44 ic division deliberation or activity or impose any pleading requirement
45 on the division if the division brings an enforcement action of any
46 kind.

47 § 1643. Division approved compliance guidelines. 1. (a) A covered
48 entity that is not a third-party collecting entity and meets the
49 requirements of section sixteen hundred twenty-eight of this article, or
50 a group of such covered entities, may apply to the division for approval
51 of one or more sets of compliance guidelines governing the collection,
52 processing, and transfer of covered data by the covered entity or group
53 of covered entities.

54 (b) Such application shall include:

55 (i) a description of how the proposed guidelines will meet or exceed
56 the requirements of this article;

1 (ii) a description of the entities or activities the proposed set of
2 compliance guidelines is designed to cover;

3 (iii) a list of the covered entities that meet the requirements of
4 section sixteen hundred twenty-eight of this article and are not third-
5 party collecting entities, if any are known at the time of application,
6 that intend to adhere to the compliance guidelines; and

7 (iv) a description of how such covered entities will be independently
8 assessed for adherence to such compliance guidelines, including the
9 independent organization not associated with any of the covered entities
10 that may participate in guidelines that will administer such guidelines.

11 (c) (i)(A) Within ninety days after the receipt of proposed guidelines
12 submitted pursuant to paragraph (b) of this subdivision, the division
13 shall publish the application and provide an opportunity for public
14 comment on such compliance guidelines.

15 (B) The division shall approve an application regarding proposed
16 guidelines under paragraph (b) of this subdivision if the applicant
17 demonstrates that the compliance guidelines:

18 (I) meet or exceed requirements of this article;

19 (II) provide for the regular review and validation by an independent
20 organization not associated with any of the covered entities that may
21 participate in the guidelines and that is approved by the division to
22 conduct such reviews of the compliance guidelines of the covered entity
23 or entities to ensure that the covered entity or entities continue to
24 meet or exceed the requirements of this article; and

25 (III) include a means of enforcement if a covered entity does not meet
26 or exceed the requirements in the guidelines, which may include referral
27 to the division for enforcement consistent with section sixteen hundred
28 fifty of this article or referral to the attorney general for enforce-
29 ment consistent with section sixteen hundred fifty-one of this article.

30 (C) Within one year after receiving an application regarding proposed
31 guidelines under paragraph (b) of this subdivision, the division shall
32 issue a determination approving or denying the application and providing
33 its reasons for approving or denying such application.

34 (ii) (A) If the independent organization administering a set of guide-
35 lines makes material changes to guidelines previously approved by the
36 division, the independent organization shall submit the updated guide-
37 lines to the division for approval. As soon as feasible, the division
38 shall publish the updated guidelines and provide an opportunity for
39 public comment.

40 (B) The division shall approve or deny any material change to the
41 guidelines within one year after receipt of the submission for approval.

42 2. If at any time the division determines that the guidelines previ-
43 ously approved no longer meet the requirements of this article or a
44 regulation promulgated under this article or that compliance with the
45 approved guidelines is insufficiently enforced by the independent organ-
46 ization administering the guidelines, the division shall notify the
47 covered entities or group of such entities and the independent organiza-
48 tion of the determination of the division to withdraw approval of such
49 guidelines and the basis for doing so. Within one hundred eighty days
50 after receipt of such notice, the covered entity or group of such enti-
51 ties and the independent organization may cure any alleged deficiency
52 with the guidelines or the enforcement of such guidelines and submit
53 each proposed cure to the division. If the division determines that such
54 cures eliminate the alleged deficiency in the guidelines, then the divi-
55 sion may not withdraw approval of such guidelines on the basis of such
56 determination.

1 3. A covered entity that is eligible to participate under paragraph
2 (a) of subdivision one of this section and participates in guidelines
3 approved under this section shall be deemed in compliance with the rele-
4 vant provisions of this article if such covered entity is in compliance
5 with such guidelines.

6 § 1644. Digital content forgeries. Not later than one year after the
7 effective date of this article, and annually thereafter, the secretary
8 of state or the secretary's designee shall publish a report regarding
9 digital content forgeries. Each report under this section shall include
10 the following:

11 1. A definition of digital content forgeries along with accompanying
12 explanatory materials.

13 2. A description of the common sources of digital content forgeries in
14 the United States and commercial sources of digital content forgery
15 technologies.

16 3. An assessment of the uses, applications, and harms of digital
17 content forgeries.

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

23 5. A description of the types of digital content forgeries, including
24 those used to commit fraud, cause harm, or violate any provision of law.

25 6. Any other information determined appropriate by the secretary of
26 state or the secretary's designee.

27 TITLE V

28 ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

29 Section 1650. Enforcement by the division of consumer protection.

30 1651. Enforcement by the attorney general.

31 1652. Enforcement by persons.

32 1653. Construction.

33 1654. Severability.

34 § 1650. Enforcement by the division of consumer protection. 1.(a) The
35 division shall establish within the division a new bureau to be known as
36 the "bureau of privacy" ("the bureau") related to consumer protection
37 and competition.

38 (b) The mission of the bureau shall be to assist the division in
39 carrying out the duties of the division under this article and related
40 duties under other provisions of law.

41 (c) The bureau shall be established, staffed, and fully operational
42 not later than one year after the effective date of this article.

43 2. The director of the bureau shall establish within the bureau an
44 office to be known as the "office of business mentorship" to provide
45 guidance and education to covered entities and service providers regard-
46 ing compliance with this article. Covered entities or service providers
47 may request advice from the division or the office of business mentor-
48 ship with respect to a course of action that the covered entity or
49 service provider proposes to pursue and that may relate to the require-
50 ments of this article.

51 3. (a) A violation of this article or of a rule or regulation promul-
52 gated under this article shall be treated as a violation of a rule
53 defining an unfair or deceptive act or practice.

54 (b) (i) Except as provided in paragraphs (c), (d), and (e) of this
55 subdivision, the division shall enforce this article and the regulations
56 promulgated under this article.

1 (ii) Any person who violates this article or a rule or regulation
2 promulgated under this article shall be subject to the penalties and
3 entitled to the privileges and immunities provided in the Federal Trade
4 Division Act (15 U.S.C. 41 et seq.).

5 (c) If the division brings a civil action alleging that an act or
6 practice violates this article or a regulation promulgated under this
7 article, the division may not seek a cease and desist order against the
8 same defendant to stop that same act or practice on the grounds that
9 such act or practice constitutes an unfair or deceptive act or practice.

10 (d) Notwithstanding any jurisdictional limitation of the division with
11 respect to consumer protection or privacy, the division shall enforce
12 this article and the rules and regulations promulgated under this arti-
13 cle, in the same manner provided in paragraphs (a), (b), (c), and (e) of
14 this subdivision, with respect to common carriers subject to the Commu-
15 nications Act of 1934 (47 U.S.C. 151 et seq.) and all acts amendatory
16 thereof and supplementary thereto and organizations not organized to
17 carry on business for their own profit or that of their members.

18 (e) In any judicial or administrative action to enforce this article
19 or a rule or regulation promulgated under this article, the amount of
20 any civil penalty obtained against a covered entity or service provider,
21 or any other monetary relief ordered to be paid by a covered entity or
22 service provider to provide redress, payment, compensation, or other
23 relief to individuals that cannot be located or the payment of which
24 would otherwise not be practicable, shall be deposited into the privacy
25 and security victims relief fund established by section eighty-five of
26 the state finance law.

27 § 1651. Enforcement by the attorney general. 1. In any case in which
28 the attorney general has reason to believe that an interest of the resi-
29 dents of that state has been, may be, or is adversely affected by a
30 violation of this article or of a rule or regulation promulgated under
31 this article by a covered entity or service provider, the attorney
32 general may bring a civil action or special proceeding to recover a
33 civil penalty provided for by this article in any court of competent
34 jurisdiction in this state, in the name of the people of the state of
35 New York to:

36 (a) enjoin such act or practice;

37 (b) enforce compliance with this article or such rule or regulation;

38 (c) obtain damages, civil penalties, restitution, or other compen-
39 sation on behalf of the residents of the state; or

40 (d) obtain reasonable attorneys' fees and other litigation costs
41 reasonably incurred.

42 2. (a) Except as provided in paragraph (b) of this subdivision, the
43 attorney general shall notify the division in writing prior to initiat-
44 ing a civil action under subdivision one of this section. Such notifica-
45 tion shall include a copy of the complaint to be filed to initiate such
46 action. Upon receiving such notification, the division may intervene in
47 such action as a matter of right.

48 (b) If the notification required by paragraph (a) of this section is
49 not feasible, the attorney general shall notify the division immediately
50 after initiating the civil action.

51 3. In any case in which a civil action is instituted by or on behalf
52 of the division for violation of this article or of a rule or regulation
53 promulgated under this article, no attorney general may, during the
54 pendency of such action, institute a civil action against any defendant
55 named in the complaint in the action instituted by or on behalf of the
56 division for a violation of this article or of a rule or regulation

1 promulgated under this article that is alleged in such complaint, if
2 such complaint alleges such violation affected the residents of the
3 state or individuals nationwide. If the division brings a civil action
4 against a covered entity or service provider for a violation of this
5 article or of a rule or regulation promulgated under this article that
6 affects the interests of the residents of the state, the attorney gener-
7 al may intervene in such action as a matter of right.

8 4. Nothing in this section may be construed to prevent the attorney
9 general from exercising the powers conferred on the attorney general to
10 conduct investigations, to administer oaths or affirmations, or to
11 compel the attendance of witnesses or the production of documentary or
12 other evidence.

13 5. Except as provided in subdivision three of this section, nothing in
14 this section may be construed as altering, limiting, or affecting the
15 authority of the attorney general to exercise the powers conferred on
16 the attorney general by the laws of the state, including the ability to
17 conduct investigations, administer oaths or affirmations, or compel the
18 attendance of witnesses or the production of documentary or other
19 evidence.

20 § 1652. Enforcement by persons. 1. (a) Beginning on the date that is
21 two years after the effective date of this article, any person or class
22 of persons for a violation of this article or of a rule or regulation
23 promulgated under this article by a covered entity or service provider
24 may bring a civil action against such entity in any court of competent
25 jurisdiction.

26 (b) In a civil action brought under paragraph (a) of this subdivision
27 in which a plaintiff prevails, the court may award the plaintiff:

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

29 (ii) injunctive relief;

30 (iii) declaratory relief; and

31 (iv) reasonable attorney's fees and litigation costs.

32 (c) (i) Prior to a person bringing a civil action under paragraph (a)
33 of this subdivision, such person shall notify the division and the
34 attorney general in writing that such person intends to bring such civil
35 action. Upon receiving such notice, the division and attorney general
36 shall each or jointly make a determination and respond to such person
37 not later than sixty days after receiving such notice, as to whether
38 they will intervene in such action.

39 (ii) Subparagraph (i) of this paragraph shall not be construed to
40 limit the authority of the division or the attorney general to later
41 commence a proceeding or civil action or intervene by motion if the
42 division or the attorney general does not commence a proceeding or civil
43 action within the sixty-day period.

44 (iii) Any written communication from counsel for an aggrieved party to
45 a covered entity or service provider requesting a monetary payment from
46 that covered entity or service provider regarding a specific claim
47 described in a letter sent pursuant to subdivision four of this section,
48 not including filings in court proceedings, arbitrations, mediations,
49 judgment collection processes, or other communications related to previ-
50 ously initiated litigation or arbitrations, shall be considered to have
51 been sent in bad faith and shall be unlawful as defined in this article,
52 if the written communication was sent prior to the date that is sixty
53 days after either a state attorney general or the division has received
54 the notice required under subparagraph (i) of this paragraph.

55 (d) Beginning on the date that is five years after the effective date
56 of this article and every five years thereafter, the division shall

1 conduct a study to determine the economic impacts in the United States
2 of demand letters sent pursuant to this section and the scope of the
3 rights of a person under this section to bring forth civil actions
4 against covered entities and service providers. Such study shall include
5 the following:

6 (i) The impact on insurance rates in the state.

7 (ii) The impact on the ability of covered entities to offer new
8 products or services.

9 (iii) The impact on the creation and growth of new startup companies,
10 including new technology companies.

11 (iv) Any emerging risks, benefits, and long-term trends in relevant
12 marketplaces, supply chains, and labor availability.

13 (v) The impact on reducing, preventing, or remediating harms to indi-
14 viduals, including from fraud, identity theft, spam, discrimination,
15 defective products, and violations of rights.

16 (vi) The impact on the volume and severity of data security incidents,
17 and the ability to respond to data security incidents.

18 (vii) Other intangible direct and indirect costs and benefits to indi-
19 viduals.

20 (e) Not later than five years after the first day on which persons and
21 classes of persons are able to bring civil actions under this subdivi-
22 sion, and every five years thereafter, the division shall submit to the
23 governor and the legislature a report that contains the results of the
24 study conducted under paragraph (d) of this subdivision.

25 2. (a) (i) Notwithstanding any other provision of law, no pre-dispute
26 arbitration agreement with respect to an individual under the age of
27 eighteen is enforceable with regard to a dispute arising under this
28 article.

29 (ii) Notwithstanding any other provision of law, no pre-dispute arbi-
30 tration agreement is enforceable with regard to a dispute arising under
31 this article concerning a claim related to gender or partner-based
32 violence or physical harm.

33 (b) Notwithstanding any other provision of law, no pre-dispute joint-
34 action waiver with respect to an individual under the age of eighteen is
35 enforceable with regard to a dispute arising under this article.

36 (c) For purposes of this subdivision:

37 (i) "Pre-dispute arbitration agreement" means any agreement to arbi-
38 trate a dispute that has not arisen at the time of the making of the
39 agreement.

40 (ii) "Pre-dispute joint-action waiver" means an agreement, whether or
41 not part of a pre-dispute arbitration agreement, that would prohibit or
42 waive the right of one of the parties to the agreement to participate in
43 a joint, class, or collective action in a judicial, arbitral, adminis-
44 trative, or other related forum, concerning a dispute that has not yet
45 arisen at the time of the making of the agreement.

46 3. (a) Subject to paragraph (c) of this subdivision, with respect to a
47 claim under this section for:

48 (i) injunctive relief; or

49 (ii) an action against a covered entity or service provider that meets
50 the requirements of section sixteen hundred twenty-eight of this arti-
51 cle, such claim may be brought by a person or class of persons if, prior
52 to asserting such claim, the person or class of persons provides to the
53 covered entity or service provider forty-five days' written notice iden-
54 tifying the specific provisions of this article the person or class of
55 persons alleges have been or are being violated.

1 (b) Subject to paragraph (c) of this subdivision, in the event a cure
2 is possible, if within the forty-five days the covered entity or service
3 provider demonstrates to the court that it has cured the noticed
4 violation or violations and provides the person or class of persons an
5 express written statement that the violation or violations has been
6 cured and that no further violations shall occur, a claim for injunctive
7 relief shall not be permitted and may be reasonably dismissed.

8 (c) The notice described in paragraph (a) of this subdivision and the
9 reasonable dismissal in paragraph (b) of this subdivision shall not
10 apply more than once to any alleged underlying violation by the same
11 covered entity.

12 4. If a person or identified members of a class of persons represented
13 by counsel in regard to an alleged violation or violations of this arti-
14 cle and has correspondence sent to a covered entity or service provider
15 by counsel alleging a violation or violations of the provisions of this
16 article and requests a monetary payment, such correspondence shall
17 include the following language: "Please visit the website of the New
18 York State Division of Consumer Protection for a general description of
19 your rights under the New York Data Privacy and Protection Act" followed
20 by a hyperlink to the webpage of the division required under section
21 sixteen hundred twenty of this article. If such correspondence does not
22 include such language and hyperlink, a civil action brought under this
23 section by such person or identified members of the class of persons
24 represented by counsel may be dismissed without prejudice and shall not
25 be reinstated until such person or persons has complied with this subdi-
26 vision.

27 5. (a) This section shall only apply to a claim alleging a violation
28 of section sixteen hundred eleven, sixteen hundred thirteen, sixteen
29 hundred twenty-one, sixteen hundred twenty-two, sixteen hundred twenty-
30 three, subdivision one or two of section sixteen hundred twenty-four,
31 paragraph (iii) of subdivision two of section sixteen hundred twenty-
32 five, subdivision one of section sixteen hundred twenty-six, subdivision
33 one of section sixteen hundred twenty-seven, or section sixteen hundred
34 forty-one of this article, or of a rule or regulation promulgated under
35 any such section.

36 (b) This section shall not apply to any claim against a covered entity
37 that has less than twenty-five million dollars per year in revenue,
38 collects, processes, or transfers the covered data of fewer than fifty
39 thousand individuals, and derives less than fifty percent of its revenue
40 from transferring covered data.

41 § 1653. Construction. 1. Nothing in this article or in a rule or regu-
42 lation promulgated under this article may be construed to limit the
43 authority of the division, or any other executive agency, under any
44 other provision of law.

45 2. (a) Nothing in this article or in a rule or regulation promulgated
46 under this article may be construed to modify, impair or supersede the
47 operation of the antitrust law or any other provision of law.

48 (b) Nothing in this article or in a rule or regulation promulgated
49 under this article shall be construed as operating to limit any law
50 detering anticompetitive conduct or diminishing the need for full
51 application of the federal antitrust law. Nothing in this article or in
52 a rule or regulation promulgated under this article explicitly or
53 implicitly precludes the application of the antitrust law.

54 (c) For purposes of this section, the term antitrust law has the same
55 meaning as in subsection (a) of the first section of the Clayton Act (15
56 U.S.C. 12), except that such term includes section 5 of the Federal

1 Trade Division Act (15 U.S.C. 45) to the extent that such section 5
2 applies to unfair methods of competition.

3 3. (a) A covered entity that is required to comply with title V of the
4 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information
5 Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et
6 seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d
7 et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), the
8 Family Educational Rights and Privacy Act (20 U.S.C. 1232g; part 99 of
9 title 34, Code of Federal Regulations) to the extent such covered entity
10 is a school as defined in 20 U.S.C. 1232g(a)(3) or 34 C.F.R. 99.1(a),
11 section 444 of the General Education Provisions Act (commonly known as
12 the "Family Educational Rights and Privacy Act of 1974") (20 U.S.C.
13 1232g) and part 99 of title 34, Code of Federal Regulations (or any
14 successor regulation), the Confidentiality of Alcohol and Drug Abuse
15 Patient Records at 42 U.S.C. 290dd-2 and its implementing regulations at
16 42 CFR part 2, the Genetic Information Non-discrimination Act (GINA), or
17 the regulations promulgated pursuant to section 264(c) of the Health
18 Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2
19 note), and is in compliance with the data privacy requirements of such
20 regulations, part, title, or Act (as applicable), shall be deemed to be
21 in compliance with the related requirements of this article, except for
22 section sixteen hundred twenty-seven of this article, solely and exclu-
23 sively with respect to data subject to the requirements of such regu-
24 lations, part, title, or Act. Not later than one year after the effec-
25 tive date of this article, the division shall issue guidance describing
26 the implementation of this paragraph.

27 (b) A covered entity that is required to comply with title V of the
28 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information
29 Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et
30 seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et
31 seq.), or the regulations promulgated pursuant to section 264(c) of the
32 Health Insurance Portability and Accountability Act of 1996 (42 U.S.C.
33 1320d-2 note), and is in compliance with the information security
34 requirements of such regulations, part, title, or Act (as applicable),
35 shall be deemed to be in compliance with the requirements of section
36 sixteen hundred twenty-seven of this article, solely and exclusively
37 with respect to data subject to the requirements of such regulations,
38 part, title, or Act. Not later than one year after the effective date of
39 this article, the division shall issue guidance describing the implemen-
40 tation of this paragraph.

41 4. Nothing in this article, nor any amendment, standard, rule,
42 requirement, assessment, or regulation promulgated under this article,
43 may be construed to preempt, displace, or supplant any federal or state
44 common law rights or remedies, or any statute creating a remedy for
45 civil relief, including any cause of action for personal injury, wrong-
46 ful death, property damage, or other financial, physical, reputational,
47 or psychological injury based in negligence, strict liability, products
48 liability, failure to warn, an objectively offensive intrusion into the
49 private affairs or concerns of the individual, or any other legal theory
50 of liability under any federal or state common law, or any state statu-
51 tory law.

52 § 1654. Severability. If any provision of this article, or the appli-
53 cation thereof to any person or circumstance, is held invalid, the
54 remainder of this article, and the application of such provision to
55 other persons not similarly situated or to other circumstances, shall
56 not be affected by the invalidation.

1 § 3. The state finance law is amended by adding a new section 85 to
2 read as follows:

3 § 85. Privacy and security victims relief fund. 1. There is hereby
4 established in the custody of the state comptroller a special fund to be
5 known as the privacy and security victims relief fund.

6 2. Such fund shall consist of all moneys required to be deposited in
7 the privacy and security victims relief fund pursuant to the provisions
8 of section sixteen hundred fifty of the general business law, together
9 with moneys appropriated for the purpose of such fund, all moneys trans-
10 ferred to such fund pursuant to law, contributions consisting of prom-
11 ises or grants of any money or property of any kind or value, or any
12 other thing of value, including grants or other financial assistance
13 from any agency of government and all moneys required by the provisions
14 of this section or any other law to be paid into or credited to this
15 fund.

16 3. Moneys of the fund, when allocated, shall be available to the
17 director of the division of consumer protection and shall be used, with-
18 out fiscal year limitation:

19 (a) to provide redress, payment, compensation, or other monetary
20 relief to individuals affected by an act or practice for which relief
21 has been obtained under article forty-six of the general business law;
22 and

23 (b) to the extent that the individuals described in paragraph (a) of
24 this subdivision cannot be located or such redress, payments, compen-
25 sation, or other monetary relief are otherwise not practicable, the
26 division of consumer protection may use such funds for the purpose of:

27 (i) funding the activities of the office of business mentorship estab-
28 lished under subdivision two of section sixteen hundred fifty of the
29 general business law; or

30 (ii) engaging in technological research that the division of consumer
31 protection considers necessary to enforce or administer article forty-
32 six of the general business law.

33 4. The moneys when allocated, shall be paid out of the fund on the
34 audit and warrant of the comptroller on vouchers certified or approved
35 by the director of the division of consumer protection, or by an officer
36 or employee of the division of consumer protection designated by the
37 director.

38 5. The director of the division of consumer protection shall promul-
39 gate rules and regulations pertaining to the allocation of moneys from
40 this fund.

41 § 4. This act shall take effect on the one hundred eightieth day after
42 it shall have become a law.