

STATE OF NEW YORK

974--A

2025-2026 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 8, 2025

Introduced by M. of A. ROZIC, HEVESI, BICHOTTE HERMELYN, BEEPHAN, WOERNER, LEE, TORRES, SIMONE -- read once and referred to the Committee on Consumer Affairs and Protection -- reported and referred to the Committee on Codes -- recommitted to the Committee on Codes in accordance with Assembly Rule 3, sec. 2 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to the management and oversight of personal data

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

1 Section 1. Short title. This act shall be known and may be cited as
2 the "New York data protection act".

3 § 2. Legislative intent. 1. Privacy is a fundamental right and an
4 essential element of freedom. Advances in technology have produced ramp-
5 ant growth in the amount and categories of personal data being gener-
6 ated, collected, stored, analyzed, and potentially shared, which
7 presents both promise and peril. Companies collect, use and share our
8 personal data in ways that can be difficult for ordinary consumers to
9 understand. Opaque data processing policies make it impossible to evalu-
10 ate risks and compare privacy-related protections across services,
11 stifling competition. Algorithms quietly make decisions with critical
12 consequences for New York consumers, often with no human accountability.
13 Behavioral advertising generates profits by turning people into products
14 and their activity into assets. New York consumers deserve more notice
15 and more control over their data and their digital privacy.

16 2. This act seeks to help New York consumers regain their privacy. It
17 gives New York consumers the ability to exercise more control over their
18 personal data and requires businesses to be responsible, thoughtful, and
19 accountable managers of that information. To achieve this, this act

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

LBD02963-03-6

1 provides New York consumers a number of new rights, including clear
2 notice of how their data is being used, processed and shared; the ability
3 to access and obtain a copy of their data in a commonly used electronic
4 format, with the ability to transfer it between services; and the
5 ability to correct inaccurate data and to delete their data. This act
6 also imposes obligations upon businesses to maintain reasonable data
7 security for personal data, to notify New York consumers of foreseeable
8 harms arising from use of their data and to obtain specific consent for
9 that use, and to conduct regular assessments to ensure that data is not
10 being used for unacceptable purposes. These data assessments can be
11 obtained and evaluated by the New York State Attorney General, who is
12 empowered to obtain penalties for violations of this act and prevent
13 future violations.

14 § 3. The general business law is amended by adding a new article 42-A
15 to read as follows:

16 ARTICLE 42-A

17 NEW YORK DATA PROTECTION ACT

18 Section 1200. Definitions.

19 1201. Jurisdictional scope.

20 1202. Consumer rights.

21 1203. Controller, processor, and third party responsibilities.

22 1204. Limitations.

23 1205. Enforcement.

24 1206. Miscellaneous.

25 § 1200. Definitions. The following definitions apply for the purposes
26 of this article unless the context clearly requires otherwise:

27 1. "Biometric information" means any measurable physical, physiological,
28 or behavioral characteristic that is attributable to a person,
29 including, but not limited to facial characteristics, fingerprint characteristics,
30 hand characteristics, eye characteristics, vocal characteristics,
31 and any other characteristics that can be used to identify a
32 person including, but not limited to: fingerprints; handprints; retina
33 and iris patterns; DNA sequence; voice; gait; and facial geometry.
34 "Biometric information" does not include a digital or physical photograph,
35 an audio or video recording, or any data generated from a digital
36 or physical photograph, or an audio or video recording, unless such data
37 is generated to identify a specific individual.

38 2. "Business associate" has the same meaning as in Title 45 of the
39 C.F.R., established pursuant to the federal Health Insurance Portability
40 and Accountability Act of 1996.

41 3. "Consent" means a clear affirmative act signifying a freely given,
42 specific, informed, and unambiguous indication of a consumer's agreement
43 to the processing of data relating to the consumer. Consent may be
44 withdrawn at any time, and a controller must provide clear, conspicuous,
45 and consumer-friendly means to withdraw consent. The burden of establishing
46 consent is on the controller. Consent does not include: (a) an
47 agreement of general terms of use or a similar document that references
48 unrelated information in addition to personal data processing; (b) an
49 agreement obtained through fraud, deceit or deception; (c) any act that
50 does not constitute a user's intent to interact with another party such
51 as hovering over, pausing or closing any content; or (d) a pre-checked
52 box or similar default.

53 4. "Consumer" means a natural person who is a New York resident acting
54 only in an individual or household context. It does not include a
55 natural person known to be acting in a professional or employment
56 context.

1 5. "Controller" means the person who, alone or jointly with others,
2 determines the purposes and means of the processing of personal data.

3 6. "Covered entity" has the same meaning as in Title 45 of the C.F.R.,
4 established pursuant to the federal Health Insurance Portability and
5 Accountability Act of 1996.

6 7. "Decisions that produce legal or similarly significant effects"
7 means decisions made by the controller that result in the provision or
8 denial by the controller of financial or lending services, housing,
9 insurance, education enrollment or opportunity, criminal justice,
10 employment opportunities, health care services or access to essential
11 goods or services.

12 8. "Deidentified data" means data that cannot reasonably be used to
13 infer information about, or otherwise be linked to an identified or
14 identifiable particular consumer, household, or device, provided that
15 the processor or controller that processes the data:

16 (a) implements reasonable technical safeguards to ensure that the data
17 cannot be associated with a consumer, household or device;

18 (b) publicly commits to process the data only as deidentified data and
19 not attempt to reidentify the data, except that the controller or
20 processor may attempt to reidentify the information solely for the
21 purpose of determining whether its deidentification processes satisfy
22 the requirements of this subdivision;

23 (c) contractually obligates any recipients of the deidentified data to
24 comply with all provisions of this article; and

25 (d) any deidentified data not otherwise exempt under this article,
26 once subsequently reidentified shall not be considered deidentified.

27 9. "Device" means any physical object that is capable of connecting to
28 the internet, directly or indirectly, or to another device and is
29 intended for use by a natural person or household or, if used outside
30 the home, for use by the general public.

31 10. "Household" means a group, however identified, of consumers who
32 cohabitate with one another at the same residential address and may
33 share use of common devices or services.

34 11. "Identified or identifiable" means a natural person who can be
35 identified, directly or indirectly, such as by reference to an identifi-
36 er such as a name, an identification number, precise geolocation data,
37 or an online or device identifier.

38 12. "Person" means a natural person or a legal entity, including but
39 not limited to a proprietorship, partnership, limited partnership,
40 corporation, company, limited liability company or corporation, associ-
41 ation, or other firm or similar body, or any unit, division, agency,
42 department, or similar subdivision thereof.

43 13. "Personal data" means any data that identifies or could reasonably
44 be linked, directly or indirectly, with a specific natural person, or
45 household. "Personal data" does not include deidentified data, informa-
46 tion that is lawfully made publicly available from federal, state or
47 local government records, or information that a controller has a reason-
48 able basis to believe is lawfully made available to the general public
49 by the consumer or from widely distributed media.

50 14. "Precise geolocation data" means information derived from technol-
51 ogy, including, but not limited to, global position system level lati-
52 tude and longitude coordinates or other mechanisms, that directly iden-
53 tifies the specific location of an individual with precision and
54 accuracy within a radius of one thousand seven hundred fifty feet,
55 except as prescribed by regulations. Precise geolocation data does not
56 include the content of communications or any data generated by or

1 connected to advance utility metering infrastructure systems or equip-
2 ment for use by a utility.

3 15. "Process", "processes" or "processing" means an operation or set
4 of operations which are performed on data or on sets of data, including
5 but not limited to the collection, use, access, sharing, monetization,
6 analysis, retention, creation, generation, derivation, recording, organ-
7 ization, structuring, storage, disclosure, transmission, analysis,
8 disposal, licensing, destruction, deletion, modification, or deidentifi-
9 cation of data.

10 16. "Processor" means a person that processes personal data on behalf
11 of the controller.

12 17. "Profiling" means any form of automated processing performed on
13 personal data to evaluate, analyze, or predict personal aspects related
14 to an identified or identifiable natural person's economic situation,
15 health, personal preferences, interests, reliability, behavior,
16 location, or movements. Profiling does not include evaluation, analy-
17 sis, or prediction based solely upon a natural person's current search
18 query or activities on, or current visit to, the controller's website or
19 online application.

20 18. "Sale", "sell", or "sold" means the disclosure, transfer, convey-
21 ance, sharing, licensing, making available, processing, granting of
22 permission or authorization to process, or other exchange of personal
23 data, or providing access to personal data for monetary or other valu-
24 able consideration by the controller to a third party. "Sale" does not
25 include the following:

26 (a) the disclosure of data to a processor who processes the data on
27 behalf of the controller and which is contractually prohibited from
28 using it for any purpose other than as instructed by the controller;

29 (b) the disclosure or transfer of data as an asset that is part of a
30 merger, acquisition, bankruptcy, or other transaction in which another
31 entity assumes control or ownership of all or a majority of the control-
32 ler's assets; or

33 (c) the disclosure of personal data to a third party necessary for
34 purposes of providing a product, service, or interaction with such third
35 party, when the consumer directs the controller to disclose the personal
36 data or intentionally uses the controller to interact with a third
37 party; or

38 (d) the disclosure or transfer of personal data to an affiliate of the
39 controller under the same branding;

40 19. "Sensitive data" means personal data that reveals:

41 (a) racial or ethnic origin, religious beliefs, mental or physical
42 health condition or diagnosis, sex life, sexual orientation, gender
43 identity or citizenship or immigration status;

44 (b) biometric information for the purpose of uniquely identifying a
45 natural person;

46 (c) precise geolocation data; or

47 (d) social security, financial account, passport or driver's license
48 numbers.

49 20. "Targeted advertising" means advertising based upon profiling. It
50 does not include recommendations by a controller to a consumer with whom
51 the controller has an existing relationship that are made on the
52 controller's websites or online applications and are based solely upon
53 personal data that the controller has collected from the consumer on
54 such websites or online applications regarding content, products, or
55 services provided by the controller.

1 21. "Third party" means, with respect to a particular interaction or
2 occurrence, a person, public authority, agency, or body other than the
3 consumer, the controller, or processor of the controller. A third party
4 may also be a controller if the third party, alone or jointly with
5 others, determines the purposes and means of the processing of personal
6 data.

7 22. "Verifiable" means to use reasonable means to determine that
8 a request to exercise any of the rights afforded in this act is being
9 made by, or on behalf of, the individual who is entitled to exercise
10 such rights authorized by this article; provided that any additional
11 personal information a controller requests for the purpose of verifica-
12 tion must be strictly necessary for the purpose of confirming the
13 identity of such individual and shall not be processed or used for any
14 purpose other than verifying the identity of the individual and shall
15 be deleted immediately upon verification or failure to verify the indi-
16 vidual. Such verification shall not extend the maximum allowable time
17 within which the regulated entity may satisfy a request by a consumer.

18 § 1201. Jurisdictional scope. 1. This article applies to legal persons
19 that conduct business in New York or produce products or services that
20 are targeted to residents of New York, and satisfy one or more of the
21 following thresholds:

22 (a) have annual gross revenue of twenty-five million dollars or more;
23 (b) controls or processes personal data of one hundred thousand
24 consumers or more; or
25 (c) derives over fifty percent of gross revenue from the sale of
26 personal data.

27 2. This article does not apply to:

28 (a) local, state, or federal governments and their agencies, authori-
29 ties or public corporations as defined in section sixty-six of the
30 general construction law or data processed by or on behalf of such
31 governmental entities provided that the data is only processed for
32 governmental purposes;

33 (b) a national securities association registered pursuant to section
34 15A of the Securities Exchange Act of 1934, as amended, or regulations
35 adopted thereunder or a registered futures association so designated
36 pursuant to section 17 of the Commodity Exchange Act, as amended, or any
37 regulations adopted thereunder;

38 (c) any nonprofit entity identified in section four hundred five of
39 the financial services law to the extent such organization collects,
40 processes, uses, or shares data solely in relation to identifying,
41 investigating, or assisting (i) law enforcement agencies in connection
42 with suspected insurance-related criminal or fraudulent acts; or (ii)
43 first responders in connection with catastrophic events;

44 (d) information that meets the following criteria:

45 (i) personal data collected, processed, or disclosed pursuant to and
46 in compliance with the federal Gramm-Leach-Bliley act (P.L. 106-102),
47 and implementing regulations;

48 (ii) personal data collected, processed, or disclosed pursuant to the
49 federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et
50 seq.), if the collection, processing, sale, or disclosure is in compli-
51 ance with that law;

52 (iii) personal data regulated by the federal Family Educational Rights
53 and Privacy Act, U.S.C. Sec. 1232g and its implementing regulations;

54 (iv) personal data collected, processed, or disclosed pursuant to the
55 federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sec.
56 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et

1 seq.) if the collection, processing, sale, or disclosure is in compli-
2 ance with that law;

3 (v) personal data regulated by section two-d of the education law;

4 (vi) data processed or maintained (A) in the course of an individual
5 applying to, employed by, or acting as an agent or independent contrac-
6 tor of a controller, processor or third party, to the extent that the
7 data is collected and used within the context of that role, (B) as the
8 emergency contact information of an individual under this section used
9 for emergency contact purposes, or (C) that is necessary to retain to
10 administer benefits for another individual relating to an individual
11 under clause (A) of this subparagraph and used for the purposes of
12 administering such benefits;

13 (vii) information maintained by a financial institution that is
14 subject to the Gramm-Leach-Bliley Act (Public Law 106-103), to the
15 extent the financial institution maintains the information in the same
16 manner as personal data as described in subparagraph (i) of this para-
17 graph;

18 (viii) personal data processed only for one or more of the following
19 purposes:

20 (A) product registration and tracking consistent with applicable
21 United States Food and Drug Administration regulations and guidance;

22 (B) public health activities and purposes as described in Section
23 164.512 of Title 45 of the Code of Federal Regulations; and/or

24 (C) activities related to quality, safety, or effectiveness regulated
25 by the United States Food and Drug Administration; or

26 (ix) personal data collected, processed, or disclosed pursuant to and
27 in compliance with any opt-out program authorized by the public service
28 commission or any other opt-out community distributed generation
29 programs authorized in law; or

30 (e) (i) an activity involving the collection, maintenance, disclosure,
31 communication, or use of any personal data bearing on a consumer's cred-
32 it worthiness, credit standing, credit capacity, character, general
33 reputation, personal characteristics, or mode of living by a consumer
34 reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a
35 furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2,
36 who provides information for use in a consumer report, as defined in
37 Title 15 U.S.C. Sec. 1861a(d), and by a user of a consumer report, as
38 set forth in Title 15 U.S.C. Sec. 1681b.; and

39 (ii) this paragraph shall apply only to the extent that such activity
40 involving the collection, maintenance, disclosure, communication, or use
41 of such data by that agency, furnisher, or user is subject to regulation
42 under the Fair Credit Reporting Act, Title 15 U.S.C. Sec. 1681 et seq.,
43 and the data is not collected, maintained, used, communicated,
44 disclosed, or sold except as authorized by the Fair Credit Reporting
45 Act.

46 § 1202. Consumer rights. 1. Right to notice. (a) Notice. Each control-
47 ler that processes a consumer's personal data must make publicly and
48 consistently available, in a conspicuous and readily accessible manner,
49 a notice containing the following:

50 (i) a description of the consumer's rights under subdivisions two
51 through seven of this section and how a consumer may exercise those
52 rights, including how to withdraw consent;

53 (ii) the categories of personal data processed by the controller and
54 by any processor who processes personal data on behalf of the control-
55 ler;

56 (iii) the sources from which personal data is collected;

(iv) the purposes for processing personal data;
(v) the categories of third parties to whom the controller disclosed, shared, transferred or sold personal data and, for each category of third party, (A) the categories of personal data being shared, disclosed, transferred, or sold to the third party, (B) the purposes for which personal data is being shared, disclosed, transferred, or sold to the third party, (C) any applicable retention periods for each category of personal data processed by the third parties or processed on their behalf, or if that is not possible, the criteria used to determine the period, and (D) whether the third parties may use the personal data for targeted advertising; and

(vi) the controller's retention period for each category of personal data that they process or is processed on their behalf, or if that is not possible, the criteria used to determine that period.

(b) Notice requirements.

(i) The notice must be written in plain language and in no less than twelve point font and consistent with section two hundred two-a of the executive law.

(ii) The categories of personal data processed and purposes for which each category of personal data is processed must be described in a clear and conspicuous manner, at a level specific enough to enable a consumer to exercise meaningful control over their personal data but not so specific as to render the notice unhelpful to a consumer.

(iii) The notice must be dated with its effective date and updated at least annually. When the information required to be disclosed to a consumer pursuant to paragraph (a) of this subdivision has not changed since the immediately previous notice (whether initial, annual, or revised) provided to the consumer, a controller may issue a statement that no changes have been made.

(iv) The notice, as well as each version of the notice in effect in the preceding six years, must be easily accessible to consumers and capable of being viewed by consumers at any time.

2. Right to opt out. (a) A controller must allow consumers the right to opt out, at any time, of processing personal data concerning the consumer for the purposes of:

(i) targeted advertising;

(ii) the sale of personal data; and

(iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

(b) A controller must provide clear and conspicuous means for the consumer or their agent to opt out of processing and clearly present as the most conspicuous choice an option to simultaneously opt out of all processing purposes set forth in paragraph (a) of this subdivision.

(c) A controller must not process personal data for any purpose from which the consumer has opted out.

(d) If a consumer has opted out of the processing of personal data pursuant to paragraph (a) of this subdivision, a controller must not request that the consumer opt back in to such processing in a way that is manifestly excessive or unduly burdensome to the consumer, and in no event shall make such a request to the consumer more than twice annually.

(e) Controllers must treat user-enabled privacy controls in a browser, browser plug-in, smartphone application, operating system, device setting, or other mechanism that communicates or signals the consumer's choice to opt out of the processing of personal data in furtherance of targeted advertising, or the sale of their personal data as an opt out

under this article. To the extent that the privacy control conflicts with a consumer's consent, the controller shall comply with the privacy control but may notify the consumer of such conflict and provide to such consumer the choice to give controller specific consent to such processing.

(f) The attorney general shall publish a list of user-enabled controls that controllers must recognize on its website with enough technical information to allow controllers and processors to recognize such controls.

3. Sensitive data. (a) A controller must obtain freely given, specific, informed, and unambiguous opt-in verifiable consent from a consumer to:

(i) process the consumer's sensitive data related to that consumer for any purpose other than those in subdivision two of section twelve hundred four of this article; or

(ii) make any changes to the existing processing or processing purpose, including those regarding the method and scope of collection, of the consumer's sensitive data that may be less protective of the consumer's sensitive data than the processing to which the consumer has previously given their freely given, specific, informed, and unambiguous opt-in consent.

(b) Any request for consent to process sensitive data must be provided to the consumer, prior to processing their sensitive data, in a stand-alone disclosure that is separate and apart from any contract or privacy policy. The request for consent must:

(i) be written in a twelve point font or greater and include a clear and conspicuous description of each category of data and processing purpose for which consent is sought;

(ii) clearly identify and distinguish between categories of data and processing purposes that are necessary to provide the services or goods requested by the consumer and categories of data and processing purposes that are not necessary to provide the services or goods requested by the consumer;

(iii) enable a reasonable consumer to easily identify the categories of data and processing purposes for which consent is sought;

(iv) clearly present as the most conspicuous choice an option to provide only the consent necessary to provide the services or goods requested by the consumer;

(v) clearly present an option to deny consent; and

(vi) where the request seeks consent to sharing, disclosure, transfer, or sale of sensitive data to third parties, identify the categories of such third parties, the categories of data sold or shared with them, the processing purposes, the retention period, or if that is not possible, the criteria used to determine the period, and state if such sharing, disclosure, transfer, or sale enables or involves targeted advertising. The details of the categories of such third parties, and the categories of data, processing purposes, and the retention period, may be set forth in a different disclosure, provided that the request for consent contains a conspicuous and directly accessible link to that disclosure.

(c) Targeted advertising and sale of personal data shall not be considered processing purposes that are necessary to provide services or goods requested by a consumer.

(d) Once a consumer has provided freely given, specific, informed, and unambiguous opt-in consent to process their sensitive data for a processing purpose, a controller may rely on such consent until it is withdrawn.

1 (e) A controller must provide a mechanism for a consumer to withdraw
2 previously given consent at any time. Such mechanism shall make it as
3 easy for a consumer to withdraw their consent as it is for such consumer
4 to provide consent.

5 (f) A controller must not infer that a consumer has provided freely
6 given, specific, informed, and unambiguous opt-in consent from the
7 consumer's inaction or the consumer's continued use of a service or
8 product provided by the controller.

9 (g) Controllers must not request consent from a consumer who has
10 previously withheld or denied consent to process sensitive data, until
11 at least twelve months after a denial, unless consent is necessary to
12 provide the services or goods requested by the consumer.

13 (h) Controllers must treat user-enabled privacy controllers in a brow-
14 ser, browser plug-in, smartphone application, operating system, device
15 setting, or other mechanism that communicates or signals the consumer's
16 choices to opt out of the processing of personal data in furtherance of
17 targeted advertising, the sale of their personal data, or profiling in
18 furtherance of decisions that produce legal or similarly significant
19 effects concerning the consumer as a denial of consent to process sensi-
20 tive data under this article. To the extent that the privacy control
21 conflicts with a consumer's consent, the privacy control settings
22 govern, unless the consumer provides freely given, specific, informed,
23 and unambiguous opt-in consent to override the privacy control, however,
24 the controller may notify such consumer of such conflict and provide to
25 the consumer the choice to give controller-specific consent to such
26 processing.

27 (i) A controller must not discriminate against a consumer for exercis-
28 ing their rights under this article or withholding or denying consent,
29 including, but not limited to, by:

30 (i) denying services or goods to the consumer, unless the consumer
31 does not consent to processing necessary to provide the services or
32 goods requested by the consumer;

33 (ii) charging different prices for goods or services, including
34 through the use of discounts or other benefits, imposing penalties, or
35 providing a different level or quality of services or goods to the
36 consumer; or

37 (iii) suggesting that the consumer will receive a different price or
38 rate for goods or services or a different level or quality of services
39 or goods.

40 (j) In the event of a merger, acquisition, bankruptcy, or other trans-
41 action in which another entity assumes control or ownership of all or
42 majority of the controller's assets, any consent provided to the
43 controller by a consumer relating to sensitive data prior to such trans-
44 action other than consent to processing necessary to provide services or
45 goods requested by the consumer, shall be deemed withdrawn.

46 4. Right to access. Upon the verifiable request of a consumer, a
47 controller shall:

48 (a) confirm whether or not the controller is processing or has proc-
49 essed personal data of that consumer, and provide access to a copy of
50 any such personal data in a manner understandable to a reasonable
51 consumer when requested; and

52 (b) provide the category of each processor or third party to whom the
53 controller disclosed, transferred, or sold the consumer's personal data
54 and, for each category of processor or third party, (i) the categories
55 of the consumer's personal data disclosed, transferred, or sold to each
56 processor or third party and (ii) the purposes for which each category

1 of the consumer's personal data was disclosed, transferred, or sold to
2 each processor or third party.

3 5. Right to portable data. Upon a verifiable request, and to the
4 extent technically feasible, the controller must provide to the consumer
5 a copy of all of, or a portion of, as designated in a verifiable
6 request, the consumer's personal data in a structured, commonly used and
7 machine-readable format that allows the consumer to transmit the data to
8 another person of the consumer's or their agent's designation without
9 hindrance.

10 6. Right to correct. (a) Upon the verifiable request of a consumer or
11 their agent, a controller must conduct a reasonable investigation to
12 determine whether personal data, the accuracy of which is disputed by
13 the consumer, is inaccurate, with such investigation to be concluded
14 within the time period set forth in paragraph (a) of subdivision eight
15 of this section.

16 (b) Notwithstanding paragraph (a) of this subdivision, a controller
17 may terminate an investigation initiated pursuant to such paragraph if
18 the controller reasonably and in good faith determines that the dispute
19 by the consumer is wholly without merit, including by reason of a fail-
20 ure by a consumer to provide sufficient information to investigate the
21 disputed personal data. Upon making any determination in accordance with
22 this paragraph that a dispute is wholly without merit, a controller
23 must, within the time period set forth in paragraph (a) of subdivision
24 eight of this section, provide the affected consumer a statement in
25 writing that includes, at a minimum, the specific reasons for the deter-
26 mination, and identification of any information required to investigate
27 the disputed personal data, which may consist of a standardized form
28 describing the general nature of such information.

29 (c) If, after any investigation under paragraph (a) of this subdivi-
30 sion of any personal data disputed by a consumer, an item of the
31 personal data is found to be inaccurate or incomplete, or cannot be
32 verified, the controller must:

33 (i) correct the inaccurate or incomplete personal data of the consum-
34 er; and

35 (ii) unless it proves impossible or involves disproportionate effort,
36 communicate such request to each third party to whom the controller
37 disclosed, transferred, or sold the personal data within one year
38 preceding the consumer's request, and to require those third parties to
39 do the same for any further third parties they disclosed, transferred,
40 or sold the personal data to.

41 (d) If the investigation does not resolve the dispute, the consumer
42 may file with the controller a brief statement setting forth the nature
43 of the dispute. Whenever a statement of a dispute is filed, unless there
44 exists reasonable grounds to believe that it is wholly without merit,
45 the controller must note that it is disputed by the consumer and include
46 either the consumer's statement or a clear and accurate codification or
47 summary thereof with the disputed personal data whenever it is
48 disclosed, transferred, or sold to any processor or third party.

49 7. Right to delete. (a) Upon the verifiable request of a consumer, a
50 controller must:

51 (i) within thirty days after receiving the verifiable request, delete
52 any or all of the consumer's personal data, as directed by the consumer
53 or their agent, that the controller possesses or controls; and

54 (ii) unless it proves impossible or involves disproportionate effort
55 that is documented in writing by the controller, communicate such
56 request to each third party to whom the controller disclosed, trans-

ferred or sold the personal data within one year preceding the consumer's request and to require those third parties to do the same for any further third parties they disclosed, transferred, or sold the personal data to.

(b) For personal data that is not possessed by the controller but by a processor of the controller, the controller may choose to (i) communicate the consumer's request for deletion to the processor, or (ii) request that the processor return to the controller the personal data that is the subject of the consumer's request and delete such personal data upon receipt of the request.

(c) A consumer's deletion of their online account must be treated as a request to the controller to delete all of that consumer's personal data directly related to that account.

(d) A controller must maintain reasonable procedures designed to prevent the reappearance in its systems, and in any data it discloses, transfers, or sells to any third party, the personal data that is deleted pursuant to this subdivision.

(e) A controller is not required to comply with a consumer's request to delete personal data if:

(i) complying with the request would prevent the controller from performing accounting functions, processing refunds, effectuating a product recall pursuant to federal or state law, or fulfilling warranty claims, provided that the personal data that is the subject of the request is not processed for any purpose other than such specific activities; or

(ii) it is necessary for the controller to maintain the consumer's personal data to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided that the consumer has given informed consent and the personal data is not processed for any purpose other than such research.

(f) Where a consumer's request for deletion is denied, the controller shall provide the consumer with a written justification for such denial.

8. Responding to requests. (a) A controller must take action under subdivisions four through seven of this section and inform the consumer of any actions taken without undue delay and in any event within thirty days of receipt of the request. That period may be extended once by thirty additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within thirty days of receipt of the request, together with the reasons for the delay. When a controller denies any such request, it must within this period disclose to the consumer a statement in writing of the specific reasons for the denial and instructions for how to appeal the decision.

(b) A controller shall permit the exercise of rights and carry out its obligations set forth in subdivisions four through seven of this section free of charge, at least twice annually to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either (i) charge a reasonable fee to cover the administrative costs of complying with the request or (ii) refuse to act on the request and notify the consumer of the reason for refusing the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

1 (c) (i) A controller shall promptly attempt, using commercially
2 reasonable efforts, to verify that all requests to exercise any rights
3 set forth in any section of this article requiring a verified request
4 were made by the consumer who is the subject of the data, or by a person
5 lawfully exercising the right on behalf of the consumer who is the
6 subject of the data. Commercially reasonable efforts shall be determined
7 based on the totality of the circumstances, including the nature of the
8 data implicated by the request.

9 (ii) A controller may require the consumer to provide additional
10 information only if the request cannot reasonably be verified without
11 the provision of such additional information. A controller must not
12 transfer or process any such additional information provided pursuant to
13 this section for any other purpose and must delete any such additional
14 information without undue delay and in any event within thirty days
15 after the controller has notified the consumer that it has taken action
16 on a request under subdivisions four through seven of this section as
17 described in paragraph (a) of this subdivision.

18 (iii) If a controller discloses this additional information to any
19 processor or third party for the purpose of verifying a consumer
20 request, it must notify the receiving processor or third party at the
21 time of such disclosure, or as close in time to the disclosure as is
22 reasonably practicable, that such information was provided by the
23 consumer for the sole purpose of verification and cannot be processed
24 for any purpose other than verification.

25 9. Implementation of rights. Controllers must provide easily accessi-
26 ble and convenient means for consumers to exercise their rights under
27 this article.

28 10. Non-waiver of rights. Any provision of a contract or agreement of
29 any kind that purports to waive or limit in any way a consumer's rights
30 under this article is contrary to public policy and is void and unen-
31 forceable.

32 § 1203. Controller, processor, and third party responsibilities. 1.
33 Controller responsibilities. (a) Data protection assessments. (i) A
34 controller shall regularly conduct and document a data protection
35 assessment for each of the controller's processing activities that
36 presents a heightened risk of harm to a consumer. For the purposes of
37 this section, processing that presents a heightened risk of harm to a
38 consumer includes: (A) the processing of personal data for the purposes
39 of targeted advertising, (B) the sale of personal data, (C) the process-
40 ing of personal data for the purposes of profiling, where such profiling
41 presents a reasonably foreseeable risk of (I) unfair or deceptive treat-
42 ment of, or unlawful disparate impact on consumers, (II) financial,
43 physical or reputational injury to consumers, (III) a physical or other
44 intrusion upon the solitude or seclusion, or the private affairs or
45 concerns of consumers where such intrusion would be offensive to a
46 reasonable person, or (IV) other substantial injury to consumers; and
47 (D) the processing of sensitive data.

48 (ii) Data protection assessments conducted pursuant to subparagraph
49 (i) of this paragraph shall identify and weigh the benefits that may
50 flow, directly and indirectly, from the processing to the controller,
51 the consumer, other stakeholders and the public against the potential
52 risks to the rights of the consumer associated with such processing, as
53 mitigated by safeguards that can be employed by the controller to reduce
54 such risks. The controller shall factor into any such data protection
55 assessment that use of deidentified data and the reasonable expectations
56 of consumers, as well as the context of the processing and the relation-

1 ship between the controller and the consumer whose personal data will be
2 processed.

3 (iii) The attorney general may require that a controller disclose any
4 data protection assessment that is relevant to an investigation
5 conducted by the attorney general, and the controller shall make the
6 data protection assessment available to the attorney general. The attor-
7 ney general may evaluate the data protection assessment to assess
8 compliance with the provisions of this article. Data protection assess-
9 ments shall be confidential and shall be exempt from disclosure under
10 the freedom of information law. To the extent any information contained
11 in a data protection assessment disclosure to the attorney general
12 includes information subject to attorney-client privilege or work prod-
13 uct protection, such disclosure shall not constitute a waiver of such
14 privilege or protection.

15 (iv) A single data protection assessment may address a comparable set
16 of processing operations that include similar activities.

17 (v) If a controller conducts a data protection assessment for the
18 purpose of complying with another applicable law or regulation, the data
19 protection assessment shall be deemed to satisfy the requirements estab-
20 lished in this section if such data protection assessment is reasonably
21 similar in scope and effect to the data protection assessment that would
22 otherwise be conducted pursuant to this section.

23 (vi) Data protection assessment requirements shall apply to processing
24 activities created or generated after the effective date of this arti-
25 cle.

26 (b) Controllers must not engage in unfair, deceptive, or abusive acts
27 or practices with respect to obtaining consumer consent, the processing
28 of personal data, and a consumer's exercise of any rights under this
29 article, including without limitation:

30 (i) designing a user interface with the purpose or substantial effect
31 of deceiving consumers, obscuring consumers' rights under this article,
32 or subverting or impairing user autonomy, decision-making, or choice; or

33 (ii) obtaining consent in a manner designed to overpower a consumer's
34 resistance; for example, by making excessive requests for consent.

35 (c) Controllers must develop, implement, and maintain reasonable safe-
36 guards to protect the security, confidentiality and integrity of the
37 personal data of consumers including adopting reasonable administrative,
38 technical and physical safeguards appropriate to the volume and nature
39 of the personal data at issue.

40 (d) (i) A controller shall limit the use and retention of a consumer's
41 personal data to what is (A) necessary to provide the services or goods
42 requested by the consumer, (B) necessary for the internal business oper-
43 ations of the controller and consistent with the disclosures made to the
44 consumer pursuant to section twelve hundred two of this article, or (C)
45 necessary to comply with the legal obligations of the controller.

46 (ii) At least annually, a controller shall review its retention prac-
47 tices for the purpose of ensuring that it is maintaining the minimum
48 amount of personal data as is necessary for the operation of its busi-
49 ness. A controller must securely dispose of all personal data that is no
50 longer (A) necessary to provide the services or goods requested by the
51 consumer, (B) necessary for the internal business operations of the
52 controller and consistent with the disclosures made to the consumer
53 pursuant to section twelve hundred two of this article, or (C) necessary
54 to comply with the legal obligations of the controller.

1 (e) Non-discrimination. A controller must not discriminate against a
2 consumer for exercising rights under this article, including but not
3 limited to, by:

4 (i) denying services or goods to consumers;

5 (ii) charging different prices for services or goods, including
6 through the use of discounts or other benefits; imposing penalties; or
7 providing a different level or quality of services or goods to the
8 consumer; or

9 (iii) suggesting that the consumer will receive a different price or
10 rate for services or goods or a different level or quality of services
11 or goods.

12 (f) Agreements with processors. (i) Before making any disclosure,
13 transfer, or sale of personal data to any processor, the controller must
14 enter into a written, signed contract with that processor. Such contract
15 must be binding and clearly set forth instructions for processing data,
16 the nature and purpose of processing, the type of data subject to proc-
17 essing, the duration of processing, and the rights and obligations of
18 both parties. The contract must also include requirements that the
19 processor must:

20 (A) ensure that each person processing personal data is subject to a
21 duty of confidentiality with respect to the data;

22 (B) protect the data in a manner consistent with the requirements of
23 this article and at least equal to the security requirements of the
24 controller set forth in their publicly available policies, notices, or
25 similar statements;

26 (C) process the data only when and to the extent necessary to comply
27 with its legal obligations to the controller unless otherwise explicitly
28 authorized by the controller;

29 (D) not combine the personal data which the processor receives from or
30 on behalf of the controller with personal data which the processor
31 receives from or on behalf of another person or collects from its own
32 interaction with consumers;

33 (E) comply with any exercises of a consumer's rights under section
34 twelve hundred two of this article upon the request of the controller,
35 subject to the limitations set forth in section twelve hundred four of
36 this article;

37 (F) at the controller's direction, delete or return all personal data
38 to the controller as requested at the end of the provision of services,
39 unless retention of the personal data is required by law;

40 (G) upon the reasonable request of the controller, make available to
41 the controller all data in its possession necessary to demonstrate the
42 processor's compliance with the obligations in this article;

43 (H) allow, and cooperate with, reasonable assessments by the control-
44 ler or the controller's designated assessor; alternatively, the process-
45 or may arrange for a qualified and independent assessor to conduct an
46 assessment of the processor's policies and technical and organizational
47 measures in support of the obligations under this article using an
48 appropriate and accepted control standard or framework and assessment
49 procedure for such assessments. The processor shall provide a report of
50 such assessment to the controller upon request;

51 (I) a reasonable time in advance before disclosing or transferring the
52 data to any further processors, notify the controller of such a proposed
53 disclosure or transfer and provide the controller an opportunity to
54 approve or reject the proposal; and

55 (J) engage any further processor pursuant to a written, signed
56 contract that includes the contractual requirements provided in this

1 paragraph, containing at minimum the same obligations that the processor
2 has entered into with regard to the data.

3 (ii) A controller must not agree to indemnify, defend, or hold a
4 processor harmless, or agree to a provision that has the effect of
5 indemnifying, defending, or holding the processor harmless, from claims
6 or liability arising from the processor's breach of the contract
7 required by clause (A) of subparagraph (i) of this paragraph or a
8 violation of this article. Any provision of an agreement that violates
9 this subparagraph is contrary to public policy and is void and unen-
10 forceable.

11 (iii) Nothing in this paragraph relieves a controller or a processor
12 from the liabilities imposed on it by virtue of its role in the process-
13 ing relationship as defined by this article.

14 (iv) Determining whether a person is acting as a controller or proces-
15 sor with respect to a specific processing of data is a fact-based deter-
16 mination that depends upon the context in which personal data is to be
17 processed. A processor that continues to adhere to a controller's
18 instructions with respect to a specific processing of personal data
19 remains a processor.

20 (g) Third parties. (i) A controller must not share, disclose, trans-
21 fer, or sell personal data, or facilitate or enable the processing,
22 disclosure, transfer, or sale to a third party of personal data for
23 which a consumer has exercised their opt-out rights pursuant to subdivi-
24 sion two of section twelve hundred two of this article, or for which
25 consent of the consumer pursuant to subdivision three of section twelve
26 hundred two of this article, has not been obtained or is not currently
27 in effect. Any request for consent to share, disclose, transfer, or sell
28 personal data, or to facilitate or enable the processing, disclosure,
29 transfer, or sale of personal data to a third party of personal data to
30 a third party must clearly include the category of the third party and
31 the processing purposes for which the third party may use the personal
32 data.

33 (ii) A controller must not share, disclose, transfer, or sell personal
34 data, or facilitate or enable the processing, disclosure, transfer, or
35 sale to a third party of personal data if it can reasonably expect the
36 personal data of a consumer to be used for purposes for which a consumer
37 has exercised their opt-out rights pursuant to subdivision two of
38 section twelve hundred two of this article, or for which the consumer
39 has not consented to pursuant to subdivision three of section twelve
40 hundred two of this article, or if it can reasonably expect that any
41 rights of the consumer provided in this article would be compromised as
42 a result of such transaction.

43 (iii) Before making any disclosure, transfer, or sale of personal data
44 to any third party, the controller must enter into a written, signed
45 contract. Such contract must be binding and the scope, nature, and
46 purpose of processing, the type of data subject to processing, the dura-
47 tion of processing, and the rights and obligations of both parties.
48 Such contract must include requirements that the third party:

49 (A) Process that data only to the extent permitted by the agreement
50 entered into with the controller; and

51 (B) Provide a mechanism to comply with any exercises of a consumer's
52 rights under section twelve hundred two of this article upon the request
53 of the controller, subject to any limitations thereon as authorized by
54 this article; and

1 (C) To the extent the disclosure, transfer, or sale of the personal
2 data causes the third party to become a controller, comply with all
3 obligations imposed on controllers under this article.

4 2. Processor responsibilities. (a) For any personal data that is
5 obtained, received, purchased, or otherwise acquired by a processor,
6 whether directly from a controller or indirectly from another processor,
7 the processor must comply with the requirements set forth in clauses (A)
8 through (J) of subparagraph (i) of paragraph (f) of subdivision one of
9 this section in its role as a processor.

10 (b) A processor is not required to comply with a request submitted
11 pursuant to this article if (i) the consumer submits the request direct-
12 ly to the processor; and (ii) the processor has processed the consumer's
13 personal data solely in its role as a processor for a controller.

14 (c) Processors shall be under a continuing obligation to engage in
15 reasonable measures to review their activities for circumstances that
16 may have altered their ability to identify a specific natural person and
17 to update their classifications of data as identified or identifiable
18 accordingly.

19 (d) A processor shall not engage in any sale of personal data other
20 than on behalf of the controller pursuant to any agreement entered into
21 with the controller.

22 (e) A processor must adopt appropriate technical and organizational
23 measures to assist a controller in fulfilling the controller's obli-
24 gation to respond to consumer requests to exercise their rights pursuant
25 to section twelve hundred two of this article, taking into account the
26 nature of the processing and the information available to the processor.

27 3. Third party responsibilities. For any personal data that is
28 obtained, received, purchased, or otherwise acquired or accessed by a
29 third party from a controller or processor, the third party must:

30 (a) Process that data only to the extent permitted by any agreements
31 entered into with the controller;

32 (b) Comply with any exercises of a consumer's rights under section
33 twelve hundred two of this article upon the request of the controller or
34 processor, subject to any limitations thereon as authorized by this
35 article; and

36 (c) To the extent the third party becomes a controller for personal
37 data, comply with all obligations imposed on controllers under this
38 article.

39 4. Exceptions. The requirements of this section shall not apply where:

40 (a) The processing is required by law;

41 (b) The processing is made pursuant to a request by a federal, state,
42 or local government or government entity; or

43 (c) The processing significantly advances protection against criminal
44 or tortious activity.

45 § 1204. Limitations. 1. This article does not require a controller or
46 processor to do any of the following solely for purposes of complying
47 with this article:

48 (a) Reidentify deidentified data;

49 (b) Comply with a verified consumer request to access, correct, or
50 delete personal data pursuant to this article if all of the following
51 are true:

52 (i) The controller is not reasonably capable of associating the
53 request with the personal data;

54 (ii) The controller does not associate the personal data with other
55 personal data about the same specific consumer as part of its normal
56 business practice; and

1 (iii) The controller does not sell the personal data to any third
2 party or otherwise voluntarily disclose or transfer the personal data to
3 any processor or third party, except as otherwise permitted in this
4 article; or

5 (c) Maintain personal data in identifiable form, or collect, obtain,
6 retain, or access any personal data or technology, in order to be capa-
7 ble of associating a verified consumer request with personal data.

8 2. The obligations imposed on controllers and processors under this
9 article do not restrict a controller's or processor's ability to do any
10 of the following, to the extent that the use of the consumer's personal
11 data is reasonably necessary and proportionate for these purposes:

12 (a) Comply with federal, state, or local laws, rules, or regulations,
13 provided that no law enforcement agency or officer thereof shall access
14 personal data without a subpoena or a lawfully executed search warrant,
15 except for the attorney general for the purposes of enforcing this
16 article, except where otherwise provided specifically in federal law;

17 (b) Investigate, establish, exercise, prepare for, or defend legal
18 claims;

19 (c) Process personal data necessary to provide the services or goods
20 requested by a consumer; perform a contract to which the consumer is a
21 party; or take steps at the request of the consumer prior to entering
22 into a contract;

23 (d) Take immediate steps to protect the life or physical safety of the
24 consumer or of another natural person, and where the processing cannot
25 be manifestly based on another legal basis;

26 (e) Prevent, detect, protect against, or respond to security inci-
27 dents, identity theft, fraud, harassment, malicious or deceptive activ-
28 ities, or any illegal activity; preserve the integrity or security of
29 systems; or investigate, report, or prosecute those responsible for any
30 such action;

31 (f) Identify and repair technical errors that impair existing or
32 intended functionality; or

33 (g) Process business contact information, including a natural person's
34 name, position name or title, business telephone number, business
35 address, business electronic mail address, business fax number, or qual-
36 ifications and any other similar information about the natural person.

37 3. The obligations imposed on controllers or processors under this
38 article do not apply where compliance by the controller or processor
39 with this article would violate an evidentiary privilege under New York
40 law and do not prevent a controller or processor from providing personal
41 data concerning a consumer to a person covered by an evidentiary privi-
42 lege under New York law as part of a privileged communication.

43 4. A controller that receives a request pursuant to subdivisions four
44 through seven of section twelve hundred two of this article, or a
45 processor or third party to whom a controller communicates such a
46 request, may decline to fulfill the relevant part of such request if:

47 (a) the controller, processor, or third party is unable to verify the
48 request using commercially reasonable efforts, as described in paragraph
49 (c) of subdivision eight of section twelve hundred two of this article;

50 (b) complying with the request would be demonstrably impossible (for
51 purposes of this paragraph, the receipt of a large number of verified
52 requests, on its own, is not sufficient to render compliance with a
53 request demonstrably impossible);

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

1 (d) the personal data was created by a natural person other than the
2 consumer making the request and is being processed for the purpose of
3 facilitating interpersonal relationships or public discussion.

4 § 1205. Enforcement. 1. (a) Whenever it appears to the attorney gener-
5 al, either upon complaint or otherwise, that any person or persons has
6 engaged in or is about to engage in any of the acts or practices stated
7 to be unlawful under this article, the attorney general may bring an
8 action or special proceeding in the name and on behalf of the people of
9 the state of New York to enjoin any violation of this article, to obtain
10 restitution of any moneys or property obtained directly or indirectly by
11 any such violation, to obtain disgorgement of any profits obtained
12 directly or indirectly by any such violation, to obtain civil penalties
13 of not more than twenty thousand dollars per violation, and to obtain
14 any such other and further relief as the court may deem proper, includ-
15 ing preliminary relief.

16 (b) Any action or special proceeding brought by the attorney general
17 pursuant to this section must be commenced within six years.

18 (c) Each instance of unlawful processing counts as a separate
19 violation. Unlawful processing of the personal data of more than one
20 consumer counts as a separate violation as to each consumer. Each
21 provision of this article that is violated counts as a separate
22 violation.

23 (d) In assessing the amount of penalties, the court must consider any
24 one or more of the relevant circumstances presented by any of the
25 parties, including, but not limited to, the nature and seriousness of
26 the misconduct, the number of violations, the persistence of the miscon-
27 duct, the length of time over which the misconduct occurred, the will-
28 fulness of the violator's misconduct, and the violator's financial
29 condition.

30 2. In connection with any proposed action or special proceeding under
31 this section, the attorney general is authorized to take proof and make
32 a determination of the relevant facts, and to issue subpoenas in accord-
33 ance with the civil practice law and rules. The attorney general may
34 also require such other data and information as such attorney general
35 may deem relevant and may require written responses to questions under
36 oath. Such power of subpoena and examination shall not abate or termi-
37 nate by reason of any action or special proceeding brought by the attor-
38 ney general under this article.

39 3. Any person, within or outside the state, who the attorney general
40 believes may be in possession, custody, or control of any books, papers,
41 or other things, or may have information, relevant to acts or practices
42 stated to be unlawful in this article is subject to the service of a
43 subpoena issued by the attorney general pursuant to this section.
44 Service may be made in any manner that is authorized for service of a
45 subpoena or a summons by the state in which service is made.

46 4. (a) Failure to comply with a subpoena issued pursuant to this
47 section without reasonable cause tolls the applicable statutes of limi-
48 tations in any action or special proceeding brought by the attorney
49 general against the noncompliant person that arises out of the attorney
50 general's investigation.

51 (b) If a person fails to comply with a subpoena issued pursuant to
52 this section, the attorney general may move in the supreme court to
53 compel compliance. If the court finds that the subpoena was authorized,
54 it shall order compliance and may impose a civil penalty of up to one
55 thousand dollars per day of noncompliance.

1 (c) Such tolling and civil penalty shall be in addition to any other
2 penalties or remedies provided by law for noncompliance with a subpoena.

3 5. This section shall apply to all acts declared to be unlawful under
4 this article, whether or not subject to any other law of this state, and
5 shall not supersede, amend or repeal any other law of this state under
6 which the attorney general is authorized to take any action or conduct
7 any inquiry.

8 § 1206. Miscellaneous. 1. Preemption: This article preempts the laws,
9 ordinances, regulations, or the equivalent adopted by any local entity
10 regarding the processing, collection, transfer, disclosure, and sale of
11 consumers' personal data by a controller or processor subject to this
12 article.

13 2. Impact report: The attorney general shall issue a report evaluating
14 this article, its scope, any complaints from consumers or persons, the
15 liability and enforcement provisions of this article including, but not
16 limited to, the effectiveness of its efforts to enforce this article,
17 and any recommendations for changes to such provisions. The attorney
18 general shall submit the report to the governor, the temporary president
19 of the senate, the speaker of the assembly, and the appropriate commit-
20 tees of the legislature within two years of the effective date of this
21 section.

22 3. Regulatory authority: (a) The attorney general is hereby authorized
23 and empowered to adopt, promulgate, amend and rescind suitable rules and
24 regulations to carry out the provisions of this article, including rules
25 governing the form and content of any disclosures or communications
26 required by this article.

27 (b) The attorney general may request, and shall receive, data and
28 information from controllers conducting business in New York state,
29 other New York state government entities administering notice and
30 consent regimes, consumer protection and privacy advocates and research-
31 ers, internet standards setting bodies, such as the internet engineering
32 taskforce and the institute of electrical and electronics engineers, and
33 other relevant sources, to conduct studies to inform suitable rules and
34 regulations. The attorney general shall receive, upon request, data
35 from other New York state governmental entities.

36 4. Exercise of rights: Any consumer right set forth in this article
37 may be exercised at any time by the consumer who is the subject of the
38 data or by a parent or guardian authorized by law to take actions of
39 legal consequence on behalf of the consumer who is the subject of the
40 data. An agent authorized by a consumer may exercise the consumer rights
41 set forth in subdivisions four through seven of section twelve hundred
42 two of this article on the consumer's behalf.

43 § 4. Severability. If any provision of this act, or any application of
44 any provision of this act, is held to be invalid, that shall not affect
45 the validity or effectiveness of any other provision of this act, or of
46 any other application of any provision of this act, which can be given
47 effect without that provision or application; and to that end, the
48 provisions and applications of this act are severable.

49 § 5. This act shall take effect immediately; provided, however, that
50 sections 1201, 1202, 1203, 1204, 1205 and 1206 of the general business
51 law, as added by section three of this act, shall take effect two years
52 after it shall have become a law.