

STATE OF NEW YORK

2277

2023-2024 Regular Sessions

IN SENATE

January 19, 2023

Introduced by Sen. KAVANAGH -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the general business law, the executive law, the state finance law and the education law, in relation to enacting the "digital fairness act"

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 "digital fairness act".

3 § 2. Legislative findings. The legislature finds that privacy
4 violations and misuse of personal information in the digital age can
5 lead to a range of harms, including discrimination in employment,
6 healthcare, housing, access to credit, and other areas; unfair price
7 discrimination; and financial, emotional, or reputational harms. Misuse
8 of personal information can limit awareness of and access to opportu-
9 nities, exacerbate information disparities, erode public trust and free
10 expression, disincentivize individuals from participating fully in
11 digital life and utilizing online services, and increase the risk of
12 future harms.

13 The legislature additionally finds that individuals in New York state,
14 like individuals across the nation, do not know or consent to the manner
15 in which entities collect, use, retain, share, and monetize their
16 personal information. This misunderstanding is, at least in part, due to
17 obfuscation on the part of the entities leveraging individuals' personal
18 information. Researchers at Carnegie Mellon found that it would take
19 seventy-six work days for individuals to read all of the privacy poli-
20 cies they encounter in a year. Although the advertising industry devel-
21 oped a common logo and slogan to notify individuals of the opportunity
22 to opt-out of targeted advertising, following market research, the
23 industry selected the slogan and logo that few individuals understood,
24 seemingly to discourage opt-out.

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

LBD06719-01-3

1 The legislature further finds that entities that collect, use, retain,
2 share, and monetize personal information have specialized knowledge
3 about the algorithms and data security measures they use, as well as
4 about how they collect, use, retain, share, and monetize personal infor-
5 mation, that the average individual is unlikely to understand. Just as
6 banks, lawyers, and medical providers, given their specialized know-
7 ledge, have special obligations to individuals, entities collecting
8 intimate personal information in the digital age and benefiting from
9 similarly specialized knowledge should have similar obligations.

10 The legislature also finds that individuals in New York state, like
11 individuals across the country, value privacy and wish to control who
12 has access to their personal information. Ninety-two percent of Face-
13 book users alter the social network's default privacy settings, demon-
14 strating that they wish to choose with whom they share personal informa-
15 tion. Similarly, ninety-two percent of Americans believe companies
16 should obtain individuals' permission before sharing or selling their
17 personal information.

18 The legislature additionally finds that biometric information is
19 unlike other unique identifiers, because biometric information is
20 biologically unique to an individual and cannot be changed if compro-
21 mised. As a result, biometric information merits special protections.

22 The legislature also finds that it has had a decades long interest in
23 protecting New Yorkers' privacy. For example, since 1996, section 79-1
24 of the New York civil rights law has protected the privacy of genetic
25 information, requiring an individual's informed, written consent prior
26 to genetic testing and restricting the disclosure and retention of
27 genetic information.

28 The legislature further finds that the use of automated decision
29 systems to make core government and business decisions raises concerns
30 around due process, fairness, accountability, and transparency, as well
31 as other civil rights and liberties. Reliance on automated decision
32 systems without adequate transparency, oversight, or safeguards can
33 undermine market predictability, harm consumers, and deny historically
34 disadvantaged or vulnerable groups the full measure of their civil
35 rights and liberties.

36 The legislature finally finds that New York has the longest standing
37 human rights law in the nation and that the state has prioritized root-
38 ing out discrimination in employment, housing, credit, public accommo-
39 dations, and educational institutions based on age, race, national
40 origin, sex, sexual orientation, gender identity, disability, and other
41 protected classes. Ensuring that sophisticated algorithms cannot be used
42 to circumvent the state's civil and human rights laws is an important
43 exercise of the legislature's authority.

44 § 3. The general business law is amended by adding a new article 39-FF
45 to read as follows:

46 ARTICLE 39-FF

47 DIGITAL FAIRNESS ACT

48 Section 899-cc. Definitions.

49 899-dd. Meaningful notice.

50 899-ee. Opt-in consent.

51 899-ff. Affirmative obligations.

52 899-gg. Biometric information; retention, collection, disclosure
53 and destruction.

54 899-hh. Surreptitious surveillance.

55 899-ii. Enforcement.

1 § 899-cc. Definitions. For the purposes of this article, the following
2 terms shall have the following meanings:

3 1. "Biometric information" shall mean a record of one or more measur-
4 able biological or behavioral characteristics that can be used singular-
5 ly or in combination with other characteristics, or with other informa-
6 tion, for automated recognition of a known or unknown individual.
7 Examples of such term shall include, but not be limited to: finger-
8 prints, retina and iris patterns, voiceprints, DNA sequence, facial
9 characteristics, gait, handwriting, key stroke dynamics, and mouse move-
10 ments.

11 2. "Collect" shall mean to buy, rent, gather, obtain, receive, or
12 access any personal information pertaining to an individual by any
13 means, online or offline, including but not limited to, receiving infor-
14 mation from the individual or from a third party, actively or passively,
15 or obtaining information by observing such individual's behavior.

16 3. "Conduct business in New York" shall mean to produce, solicit, or
17 offer for use or sale any product or service in a manner that inten-
18 tionally targets, or may reasonably be expected to contact, New York
19 residents, or to engage in any activity that would subject the actor to
20 personal jurisdiction under section three hundred one or section three
21 hundred two of the civil practice law and rules, whether or not for
22 profit.

23 4. "Covered entity" shall mean a legal entity that conducts business
24 in New York state and as part of such business, processes and maintains
25 the personal information of five hundred or more unique individuals.

26 5. "Data processor" shall mean a person that processes personal infor-
27 mation on behalf of a covered entity.

28 6. "De-identified information" shall mean information that cannot
29 reasonably identify, relate to, describe, be capable of being associated
30 with, or be linked, directly or indirectly, to a particular individual;
31 provided that a covered entity that uses de-identified information:

32 (a) Has implemented technical safeguards that prohibit reidentifica-
33 tion of the individual to whom such information may pertain;

34 (b) Has implemented business processes that specifically prohibit
35 reidentification of such information;

36 (c) Has implemented business processes that prevent inadvertent
37 release of such de-identified information; and

38 (d) Makes no attempt to reidentify such information.

39 7. "Device" shall mean a product that is capable of sending, routing,
40 or receiving communications to or from another device and intended for
41 use by a single individual or single household or, if used outside of a
42 home, for use by the general public.

43 8. "Device fingerprinting" shall mean information passively collected
44 for the purpose of identifying a device through a combination of device
45 identifiers, wireless or cellular networks, language settings, software
46 versions, time zone, frequently visited sites, drivers, or other spec-
47 ifications.

48 9. "Device indicator" shall mean any identifier tied to an individual,
49 household, or device, including but not limited to a combinatory method
50 such as device fingerprinting or a technical identifier such as internet
51 protocol address, device advertisement identifier, serial number, inter-
52 national mobile equipment identity, media access control address, cookie
53 identifier, or subscriber identification module card serial number,
54 whether resettable or persistent.

55 10. "Disclose" shall mean any action, set of actions, or omission in
56 which a covered entity, data processor, or third party makes personal

1 information available to another person, intentionally or uninten-
2 tionally, including but not limited to, sharing, publishing, releasing,
3 transferring, disseminating, making available, selling, leasing, provid-
4 ing access to, failing to restrict access to, or otherwise communicating
5 orally, in writing, electronically, or by any other means.

6 11. "Division" shall mean the consumer protection division, unless
7 context clearly indicates otherwise.

8 12. "Governmental entity" shall mean a department or agency of the
9 state or a political subdivision thereof, or an individual acting for or
10 on behalf of the state or a political subdivision thereof.

11 13. "Harm" shall mean potential or realized adverse consequences to an
12 individual or to society, including but not limited to:

13 (a) Direct or indirect financial harm.

14 (b) Physical harm or threats to persons or property, including but not
15 limited to bias-related crimes and threats, harassment, and sexual
16 harassment.

17 (c) Discrimination in goods, services, or economic opportunity,
18 including but not limited to housing, employment, credit, insurance,
19 education, or health care on the basis of an individual or class of
20 individuals' actual or perceived age, race, national origin, sex, sexual
21 orientation, gender identity, marital status, disability, military
22 status, and/or membership in another protected class.

23 (d) Interference with or surveillance of first amendment-protected
24 activities by state actors.

25 (e) Interference with the right to vote or with free and fair
26 elections.

27 (f) Interference with due process or equal protection under law.

28 (g) Loss of individual control over personal information, nonconsensu-
29 al sharing of private information, and data breach.

30 (h) The nonconsensual capture of information or communications within
31 an individual's home or where an individual has a reasonable expectation
32 of seclusion or access control.

33 (i) Other effects on an individual that may not be reasonably foresee-
34 able to, contemplated by, or expected by the individual to whom the
35 personal information relates, that are nevertheless reasonably foreseea-
36 ble, contemplated by, or expected by the covered entity that alter or
37 limit such individual's choices or predetermine results.

38 14. "Individual" shall mean a natural person whom a covered entity
39 knows or has reason to know is located within New York state.

40 15. "Personal information" shall mean information that is captured in
41 exchange for any kind of value provided to the individual to whom the
42 information pertains, including but not limited to a good or service,
43 the placement of targeted advertisements, or a membership; as a result
44 of an individual, household, or device's establishment or maintenance of
45 an account with a covered entity; or as a result of an individual,
46 household, or device's interaction with a covered entity. Such term
47 shall also include information that directly or indirectly identifies,
48 relates to, describes, is capable of being associated with, or could
49 reasonably be linked to a particular individual, household, or device
50 that provides or provided information to a covered entity in exchange
51 for any kind of value provided to the individual to whom such informa-
52 tion pertains or that established, maintained, establishes or maintains
53 an account with a covered entity. Information is reasonably linkable to
54 an individual, household, or device if it can be used on its own or in
55 combination with other reasonably available information, regardless of

1 whether such other information is held by the covered entity, to identi-
2 fy an individual, household, or device.

3 16. "Monetize" shall mean to sell, rent, release, disclose, dissem-
4 inate, make available, transfer, or otherwise communicate orally, in
5 writing, or by electronic or other means, an individual's personal
6 information by a covered entity, a third party, or a data processor in
7 exchange for monetary or other consideration, as well as to leverage or
8 use an individual's personal information to place a targeted advertise-
9 ment or to otherwise profit, regardless of whether such individual's
10 personal information changes hands.

11 17. "Process" or "processing" shall mean any action or set of actions
12 performed on or with personal information, including but not limited to,
13 collection, access, use, retention, sharing, monetizing, analysis,
14 creation, generation, derivation, decision-making, recording, alter-
15 nation, organization, structuring, storage, disclosure, transmission,
16 sale, licensing, disposal, destruction, de-identifying, or other handl-
17 ing of personal information.

18 18. "Reasonably understandable" shall mean of a length and complexity
19 such that an individual with a fourth-grade reading level, as estab-
20 lished by the New York department of education's fourth grade English
21 language arts learning standards, can read and comprehend the contents
22 in two minutes or less.

23 19. "Targeted advertisement" shall mean an advertisement directed to
24 an individual where the advertisement is selected based on personal
25 information obtained or inferred over time from such individual's or the
26 individual's device's activities, communications, or associations across
27 websites, applications, services, or covered entities. Such term shall
28 not include advertisements directed to an individual solely based upon
29 the individual's current visit to a website, application, service, or
30 covered entity, or in response to the individual's request for informa-
31 tion or feedback.

32 20. "Third party" shall mean, with respect to an individual's personal
33 information, any person that is not the covered entity or a data proces-
34 sor.

35 21. "Use model" shall mean a discrete purpose for which collected
36 personal information is to be processed, including but not limited to,
37 first party marketing, third party marketing, first party research and
38 development, third party research and development, and product improve-
39 ment.

40 § 899-dd. Meaningful notice. 1. In addition to any long form privacy
41 policy, each covered entity shall make persistently and conspicuously
42 available a short-form privacy notice--

43 (a) That an individual must interact with upon the individual's first
44 visit to the covered entity's website or first use of the covered enti-
45 ty's mobile application;

46 (b) Persistently available and readily accessible on a covered enti-
47 ty's website or mobile application;

48 (c) At the physical place of business or any offline equivalent main-
49 tained by the covered entity; and

50 (d) At or prior to the point of sale of a product or service,
51 subscription to a service, or establishment of an account with, the
52 covered entity or if there is no such sale, subscription, or establish-
53 ment, before the individual uses such product or service of the covered
54 entity.

55 2. The short-form privacy notice required by subdivision one of this
56 section shall:

- (a) Be clear, concise, well-organized, and complete;
- (b) Be clear and prominent in appearance;
- (c) Use clear and plain language;
- (d) Use visualizations where appropriate to make complex information understandable by the ordinary user;
- (e) Be reasonably understandable;
- (f) Be clearly distinguishable from other matters;
- (g) Not contain any unrelated, confusing, or contradictory information;
- (h) Be no more than five hundred words, excluding the list of third parties required under paragraph (f) of subdivision three of this section; and
- (i) Be provided free of charge.

3. The short-form privacy notice required by subdivision one of this section shall include:

- (a) What personal information is being processed;
- (b) The manner in which personal information is processed;
- (c) How and for what purpose the covered entity processes personal information;
- (d) How long personal information will be retained;
- (e) Whether and how the covered entity monetizes personal information;
- (f) To which third parties the covered entity discloses personal information and for what purposes; and
- (g) How the covered entity collects personal information, including offline practices, when the individual is not directly interacting with such covered entity.

4. The list of third parties required under paragraph (f) of subdivision three of this section, shall be offset by at least two line breaks from the rest of the short-form privacy notice required under subdivision one of this section.

5. Within one year of the enactment of this article, the consumer protection division shall establish standardized short-form privacy notices that comply with this section. A covered entity may satisfy the short-form privacy notice requirements by adopting the standardized short-form privacy notice established by the division.

6. Within one year of the enactment of this article, the consumer protection division shall develop a recognizable and uniform logo or button to promote individual awareness of the short-form privacy notice that may be used by covered entities.

7. The consumer protection division may promulgate rules and regulations specifying additional requirements for the format and substance of such short-form privacy notices.

§ 899-ee. Opt-in consent. 1. A covered entity shall obtain freely given, specific, informed, and unambiguous opt-in consent from an individual to:

- (a) Process such individual's personal information; and
- (b) Make any changes in the processing of such individual's information that necessitate a change to the entity's short-form privacy notice required under section eight hundred ninety-nine-dd of this article.

2. Within one year of the enactment of this article, the division shall promulgate rules and regulations grouping different types of processing of personal information by use model and permitting a covered entity to simultaneously obtain freely given, specific, informed, and unambiguous opt-in consent from an individual for multiple transactions of the same use model.

1 3. A covered entity shall ensure that the option to withhold consent
2 is displayed as clearly and prominently as the option to provide
3 consent.

4 4. A covered entity shall provide a mechanism for an individual to
5 withdraw previously-given consent at any time. Such mechanism shall make
6 it as easy for an individual to withdraw their consent as it is for such
7 individual to provide consent.

8 5. A covered entity shall not be required to obtain freely given,
9 specific, informed, and unambiguous opt-in consent from an individual
10 under subdivision one of this section if:

11 (a) The processing is necessary for the primary purpose of the trans-
12 action for which personal information is provided, such as the provision
13 of financial information to complete a purchase or the provision of a
14 mailing address for package delivery; provided that the personal infor-
15 mation shall not be processed or monetized for any other purpose without
16 the freely given, specific, informed, and unambiguous opt-in consent
17 from the individual to whom the personal information pertains.

18 (b) The covered entity, in good faith, believes that an emergency
19 presenting the risk of death or serious physical injury to any individ-
20 ual requires disclosure, without delay, of personal information relating
21 to such emergency, the covered entity may disclose the personal informa-
22 tion relating to such emergency to a governmental entity. A covered
23 entity that discloses the personal information of an individual without
24 obtaining opt-in approval shall, within twenty-four hours, inform the
25 individual of the personal information that the covered entity
26 disclosed, the details of the emergency, and the reasons why the covered
27 entity needed to use, access, or disclose the personal information.

28 (c) Processing the personal information is necessary for engaging in
29 public or peer-reviewed scientific, medical, historical, social science,
30 or statistical research in the public interest that adheres to all other
31 applicable ethical standards or laws, with informed consent.

32 (d) Processing the personal information is necessary for clinical,
33 treatment, public health, medical educational, medical training, or
34 insurance purposes, provided that the personal information shall not be
35 processed or monetized for any other purpose without the freely given,
36 specific, informed, and unambiguous opt-in consent from such individual
37 to whom the personal information pertains.

38 (e) The processing involves only de-identified information.

39 (f) In response to a warrant issued by a court of competent jurisdic-
40 tion under the procedures described in the federal rules of criminal
41 procedure or article six hundred ninety of the criminal procedure law.

42 (g) If required by state or federal law.

43 6. The division is hereby authorized and directed to conduct a study
44 to determine the most effective way for entities to obtain individuals'
45 freely given, specific, informed, and unambiguous opt-in consent for
46 each type of personal information processing and, to the extent possi-
47 ble, to avoid notice fatigue.

48 7. The division may request data and information from covered entities
49 conducting business in New York state, other New York state government
50 entities administering notice and consent regimes, consumer protection
51 and privacy advocates and researchers, internet standards setting
52 bodies, such as the internet engineering taskforce and the institute of
53 electrical and electronics engineers, and other relevant sources to
54 effectuate the purpose of such study. The division shall receive, upon
55 request, data from other New York state governmental entities.

1 8. Within one year of the enactment of this article, the division
2 shall promulgate rules and regulations specifying the manner in which
3 covered entities shall obtain individuals' freely given, specific,
4 informed, and unambiguous opt-in consent for each type of personal
5 information processing, as well as the manner in which individuals may
6 withdraw their consent at any time. Such rules and regulations shall
7 require covered entities to make it as easy for an individual to with-
8 draw their consent as it is for the individual to provide consent.

9 9. Under no circumstances shall an individual's interaction with a
10 covered entity or use of a covered entity's product or service, when the
11 covered entity has a terms of service or a privacy policy, including the
12 short-form privacy notice required under section eight hundred ninety-
13 nine-dd of this article, in and of itself constitute freely given,
14 specific, informed, and unambiguous consent.

15 10. To the extent that a covered entity must process internet protocol
16 addresses, system configuration information, URLs of referring pages,
17 locale and language preferences, keystrokes, and other personal informa-
18 tion in order to obtain individuals' freely given, specific, informed,
19 and unambiguous opt-in consent, the covered entity shall:

20 (a) Only process the personal information necessary to request freely
21 given, specific, informed, and unambiguous opt-in consent;

22 (b) Process the personal information solely to request freely given,
23 specific, informed, and unambiguous opt-in consent; and

24 (c) Immediately delete the personal information if consent is withheld
25 or withdrawn.

26 11. A covered entity shall not refuse to serve an individual who does
27 not approve the processing of such individual's personal information
28 under this section, unless the processing is necessary for the primary
29 purpose of the transaction such individual has requested.

30 12. A covered entity shall not offer an individual a program that
31 relates the price or quality of a product or service to the privacy
32 protections afforded to the individual, including by providing a
33 discount or other incentive in exchange for the opt-in approval of such
34 individual to the processing of such individual's personal information,
35 or because an individual declines to exercise the opportunities provided
36 under subdivision two of section eight hundred ninety-nine-ff of this
37 article.

38 13. Notwithstanding subdivision twelve of this section, a covered
39 entity may, with the individual's freely given, specific, informed, and
40 unambiguous opt-in consent given pursuant to this section, operate a
41 program in which information, products, or services sold to the individ-
42 ual are discounted based on such individual's prior purchases from the
43 covered entity; provided that the captured personal information shall be
44 processed solely for the purpose of operating such program.

45 § 899-ff. Affirmative obligations. 1. Care. (a) A covered entity shall
46 store, transmit, and protect from disclosure all personal information
47 using the reasonable standard of care within the covered entity's indus-
48 try; and such covered entity shall store, transmit, and protect from
49 disclosure all personal information in a manner that is the same as or
50 more protective than the manner in which the covered entity stores,
51 transmits, and protects other confidential information.

52 (b) The division, in consultation with the office of information tech-
53 nology services and the department of financial services, may develop
54 appropriate security standards for personal information. This paragraph
55 shall preempt paragraph (a) of this subdivision only to the extent that

1 the security standards developed are more protective of personal infor-
2 mation than the industry standard of care.

3 2. Loyalty. (a) Absent freely given, specific, informed, and unambig-
4 uous opt-in consent from the individual engaging in a transaction with a
5 covered entity, a covered entity shall not process personal information
6 beyond what is adequate, relevant, and necessary for the completion of
7 the transaction requested by such individual.

8 (b) A covered entity that maintains an individual's personal informa-
9 tion shall provide such individual with a reasonable means to access
10 their personal information, including any information obtained about
11 that individual from a third-party, whether online or offline, as well
12 as information about where or from whom the covered entity obtained the
13 personal information and the names of the third parties to which the
14 covered entity has disclosed or will disclose the personal information.

15 (c) A covered entity that maintains an individual's personal informa-
16 tion shall provide the access to such personal information under para-
17 graph (b) of this subdivision, in a usable and searchable format that
18 allows the individual to transfer the personal information from one
19 entity to another entity without hindrance.

20 (d) A covered entity that maintains an individual's personal informa-
21 tion in a non-public profile or account shall delete such personal
22 information, and any information derived therefrom, pertaining to an
23 individual upon such individual's request.

24 (e) A covered entity shall provide the opportunities required under
25 paragraphs (b), (c) and (d) of this subdivision, in a form that is:

26 (i) Clear and conspicuous;

27 (ii) Made available at no additional cost to the individual to whom
28 the information pertains; and

29 (iii) In a language other than English if the covered entity communi-
30 cates with the individual to whom the information pertains in such other
31 language.

32 (f) A covered entity shall comply with an individual's request under
33 paragraphs (b), (c) and (d) of this subdivision, not later than ninety
34 days after receiving a verifiable request from the individual; or, if
35 the individual is a minor under the age of thirteen, the individual's
36 parent or guardian; or, if the individual is a minor between the ages of
37 thirteen and eighteen, either the individual or the individual's parent
38 or guardian.

39 (i) Where the covered entity has reasonable doubts or cannot verify
40 the identity of the individual making a request under paragraphs (b),
41 (c) or (d) of this subdivision, the covered entity may request addi-
42 tional personal information necessary for the specific purpose of
43 confirming the identity of such individual. In such cases, the addi-
44 tional personal information shall not be processed for any purpose other
45 than verifying the identity of the individual and shall be deleted imme-
46 diately upon verification or failure to verify the individual.

47 (ii) A covered entity may not de-identify an individual's personal
48 information during the ninety-day period beginning on the date on which
49 the covered entity receives a request from the individual pursuant to
50 paragraphs (b), (c) and (d) of this subdivision.

51 (iii) The division may promulgate rules and regulations specifying
52 additional requirements for a covered entity's response to requests
53 pursuant to paragraphs (b), (c) and (d) of this subdivision.

54 (g) Where an individual has taken steps by the online selection of
55 options related to the processing of personal information, a covered
56 entity shall adhere to such selections.

1 (h) A covered entity shall not share an individual's device identi-
2 fers with any third party without the individual's freely given, specif-
3 ic, informed, and unambiguous opt-in written consent.

4 3. Confidentiality. (a) A covered entity shall not disclose personal
5 information to a third party unless that third party is contractually
6 bound to the covered entity to meet the same privacy and security obli-
7 gations as the covered entity. A covered entity shall exercise reason-
8 able oversight and take reasonable actions, including by auditing the
9 data security and processing practices of the third party no less than
10 once annually, to ensure the third party's compliance. The covered enti-
11 ty shall publish the results of such audit publicly on its website.

12 (i) A covered entity shall not process personal information it has
13 acquired from a third party, without the freely given, specific,
14 informed, and unambiguous opt-in consent from the individual to whom
15 that personal information pertains unless the processing is necessary to
16 obtain such individuals' freely given, specific, informed, and unambig-
17 uous opt-in consent, in which the covered entity shall only process the
18 personal information necessary to request freely given, specific,
19 informed, and unambiguous opt-in consent and shall immediately delete
20 such personal information if consent is withheld or withdrawn.

21 (ii) A covered entity that facilitates access to personal information
22 by other covered entities shall limit access to and seek proof of
23 destruction of such personal information if the first covered entity has
24 actual knowledge that another covered entity has violated this section.

25 (b) A covered entity shall not disclose personal information to a data
26 processor unless the covered entity enters into a contractual agreement
27 with such data processor that prohibits the data processor from process-
28 ing such personal information for any purpose other than the purposes
29 for which the individual provided the personal information to the
30 covered entity, and that requires the data processor to meet the same
31 privacy and security obligations as the covered entity. Such data
32 processor shall not further disclose or process personal information it
33 has acquired from the covered entity except as explicitly authorized by
34 the contract. A covered entity shall exercise reasonable oversight and
35 take reasonable actions, including but not limited to, auditing the data
36 security and processing practices of the data processor no less than
37 once annually, to ensure its data processor's compliance. The covered
38 entity shall publish the results of such audit publicly on its website.

39 4. Duty. A covered entity that collects personal information directly
40 from an individual has a duty, when processing such personal informa-
41 tion, to put the interests of the individual ahead of the interests of
42 the covered entity's business.

43 § 899-gg. Biometric information; retention, collection, disclosure and
44 destruction. 1. A covered entity or governmental entity in possession
45 of biometric information shall develop a written policy, made available
46 to the public, establishing a retention schedule and guidelines for
47 permanently destroying biometric information when the initial purpose
48 for collecting or obtaining such information has been satisfied, or
49 within one year of the individual's last interaction with the covered
50 entity or governmental entity, whichever occurs first. Absent a valid
51 warrant issued by a court of competent jurisdiction, a covered entity or
52 governmental entity in possession of biometric information shall comply
53 with its established retention schedule and destruction guidelines.

54 2. No covered entity shall collect, capture, purchase, receive through
55 trade, or otherwise obtain an individual's biometric information, unless
56 it first:

1 (a) Informs the subject or the subject's legally authorized represen-
2 tative in writing that biometric information is being collected or
3 stored;

4 (b) Informs the subject or the subject's legally authorized represen-
5 tative in writing of the specific purpose and length of term for which
6 such biometric information is being collected, stored, and used; and

7 (c) Receives a written release executed by the subject of the biome-
8 tric information or the subject's legally authorized representative.

9 3. Absent a law enforcement investigation pursuant to a criminal inci-
10 dent, no governmental entity shall collect, capture, purchase, receive
11 through trade, or otherwise obtain an individual's biometric informa-
12 tion, unless:

13 (a) It first obtains a valid warrant issued by a court of competent
14 jurisdiction under the procedures described in the federal rules of
15 criminal procedure or article six hundred ninety of the criminal proce-
16 dure law.

17 (b) It believes that an emergency involving immediate danger of death
18 or serious physical injury to any individual requires obtaining, without
19 delay, biometric information related to such emergency and the request
20 is narrowly tailored to address such emergency, subject to the following
21 limitations:

22 (i) The request shall document the factual basis for believing that an
23 emergency involving immediate danger of death or serious physical injury
24 to an individual requires obtaining, without delay, biometric informa-
25 tion relating to such emergency; and

26 (ii) Not later than forty-eight hours after the date on which a
27 governmental entity obtains biometric information under this paragraph,
28 the governmental entity shall file with the appropriate court a signed,
29 sworn statement of a supervisory official of a rank designated by the
30 head of such governmental entity setting forth the grounds for the emer-
31 gency access; or

32 (c) It first informs the subject or the subject's legally authorized
33 representative in writing that biometric information is being collected
34 or stored, the specific purpose and length of term for which such biome-
35 tric information is being collected, stored, and used, and it receives a
36 written release executed by the subject of the biometric information or
37 the subject's legally authorized representative.

38 4. No covered entity or governmental entity in possession of biometric
39 information shall sell, lease, trade, monetize, or otherwise profit from
40 such biometric information.

41 5. No covered entity or governmental entity in possession of an indi-
42 vidual's biometric information shall disclose, redisclose, or otherwise
43 disseminate such individual's biometric information unless:

44 (a) The subject of the biometric information or the subject's legally
45 authorized representative consents in writing to the disclosure or
46 redisclosure of such information;

47 (b) The disclosure or redisclosure of such information completes a
48 financial transaction requested or authorized by the subject of the
49 biometric identifier or the biometric information or the subject's
50 legally authorized representative;

51 (c) The disclosure or redisclosure is required by state or federal
52 law; or

53 (d) The disclosure is required pursuant to a valid warrant issued by a
54 court of competent jurisdiction under the procedures described in the
55 federal rules of criminal procedure or article six hundred ninety of the
56 criminal procedure law.

1 6. The requirements of this section are in addition to those imposed
2 by sections eight hundred ninety-nine-dd through eight hundred ninety-
3 nine-ff of this article.

4 7. (a) Subdivisions one through six of this section shall not apply to
5 biometric information captured from a patient by a health care provider
6 or health care facility, as defined in section eighteen of the public
7 health law, or biometric information collected, used, or stored for
8 medical education or research, public health or epidemiological
9 purposes, health care treatment, payment, or operations under the feder-
10 al health insurance portability and accountability act of 1996, or to
11 X-ray, roentgen process, computed tomography, MRI, PET scan, mammogra-
12 phy, or other image or film of the human anatomy used to diagnose, prog-
13 nose, or treat an illness or other medical condition or to further vali-
14 date scientific testing or screening.

15 (b) Biometric information captured, collected, used, or stored pursu-
16 ant to paragraph (a) of this subdivision, including information that has
17 been de-identified or aggregated, shall not be used, disclosed, or
18 otherwise disseminated except for:

19 (i) Clinical, treatment, scientific, public health, medical educa-
20 tional, medical training, research, or insurance purposes;

21 (ii) If required by state or federal law;

22 (iii) To respond to a warrant issued by a court of competent jurisdic-
23 tion under the procedures described in the federal rules of criminal
24 procedure or article six hundred ninety of the criminal procedure law;
25 or

26 (iv) If the subject of the biometric information or the subject's
27 legally authorized representative consents in writing to the disclosure
28 or redisclosure.

29 8. Nothing in subdivision seven of this section shall affect any
30 person or covered entity's rights or obligations under section eighteen
31 of the public health law.

32 § 899-hh. Surreptitious surveillance. A covered entity shall not acti-
33 vate the microphone, camera, or other sensor on a device in the lawful
34 possession of an individual that is capable of collecting or transmit-
35 ting audio, video, or image data or data that can be directly used to
36 measure biometric information, human movement, location, chemicals,
37 light, radiation, air pressure, speed, weight or mass, positional or
38 physical orientation, magnetic fields, temperature, or sound without
39 providing the notice required by section eight hundred ninety-nine-dd of
40 this article and obtaining the individual's freely given, specific,
41 informed, and unambiguous opt-in consent pursuant to section eight
42 hundred ninety-nine-ee of this article.

43 § 899-ii. Enforcement. 1. Any individual may bring a civil action in
44 any court of competent jurisdiction alleging a violation of this arti-
45 cle, or a violation of a rule or regulation promulgated to effectuate
46 the provisions of this article.

47 (a) A violation of this article, or a violation of a rule or regu-
48 lation promulgated to effectuate the provisions of this article, with
49 respect to the personal information of an individual constitutes a
50 rebuttable presumption of harm to such individual.

51 (b) In a civil action in which the plaintiff prevails, the court may
52 award:

53 (i) Liquidated damages of ten thousand dollars or actual damages,
54 whichever is greater;

55 (ii) Punitive damages; and

1 (iii) Any other relief, including an injunction, that the court deems
2 appropriate.

3 (c) In addition to any relief awarded under paragraph (b) of this
4 subdivision, the court shall award reasonable attorney's fees and costs
5 to any prevailing plaintiff.

6 2. The attorney general may bring an action in the name of the state,
7 or as a parens patriae proceeding on behalf of persons residing in the
8 state, to enforce this article. In such action, the court may award:

9 (a) Injunctive relief, including preliminary injunctions, to prevent
10 further violations of and compel compliance with the provisions of this
11 article;

12 (b) Civil penalties of up to twenty-five thousand dollars per
13 violation, or up to four percent of annual revenue of the covered enti-
14 ty, data processor, or third party;

15 (c) Other appropriate relief, including restitution, to redress harms
16 to individuals or to mitigate all substantial risk of harm; and

17 (d) Any other relief the court deems appropriate.

18 3. A district attorney, or a city attorney in a city having a popu-
19 lation in excess of seven hundred fifty thousand people, may bring an
20 action to enforce this article. In such action, the court may award:

21 (a) Injunctive relief, including preliminary injunctions, to prevent
22 further violations of and compel compliance with the provisions of this
23 article;

24 (b) Civil penalties of up to twenty-five thousand dollars per
25 violation, or up to four percent of annual revenue of the covered enti-
26 ty, data processor, or third party;

27 (c) Other appropriate relief, including restitution, to redress harms
28 to individuals or to mitigate all substantial risk of harm; and

29 (d) Any other relief the court deems appropriate.

30 4. When calculating damages and civil penalties, the court shall
31 consider the number of affected individuals, the severity of the
32 violation, and the size and revenues of the covered entity.

33 5. Each individual whose personal information is unlawfully processed,
34 and each instance of processing counts as a separate violation. Each
35 provision of this article that is violated counts as a separate
36 violation.

37 6. It is a violation of this article for a covered entity, govern-
38 mental entity, or anyone else acting on behalf of a covered entity or
39 governmental entity to retaliate against an individual who makes a good-
40 faith complaint that there has been a failure to comply with any
41 provision of this article. An individual who is injured by a violation
42 of this subdivision may bring a civil action for monetary damages and
43 injunctive relief in any court of competent jurisdiction.

44 7. If a series of steps or transactions were component parts of a
45 single transaction intended to be taken with the intention of avoiding
46 the reach of this article, a court shall disregard the intermediate
47 steps or transactions for purposes of effectuating the purposes of this
48 article.

49 8. Any provision of a contract or agreement of any kind, including a
50 covered entity's terms of service or a privacy policy, including the
51 short-form privacy notice required under section eight hundred ninety-
52 nine-dd of this article, that purports to waive or limit in any way an
53 individual's rights under this article, including but not limited to,
54 any right to a remedy or means of enforcement, shall be deemed contrary
55 to public policy and shall be void and unenforceable.

1 9. No covered entity, that is a provider of an interactive computer
2 service as defined in 47 U.S.C. § 230, shall be liable for any personal
3 information or biometric information posted by another information
4 content provider, as defined in 47 U.S.C. § 230.

5 10. No private or government action brought pursuant to this section
6 shall preclude any other action under this article.

7 § 4. Section 292 of the executive law is amended by adding nine new
8 subdivisions 42, 43, 44, 45, 46, 47, 48, 49 and 50 to read as follows:

9 42. The term "advertiser" shall mean a person who proposes a commer-
10 cial transaction or disseminates a public or private communication of
11 which the primary purpose is to solicit for an opportunity.

12 43. The term "conduct business in New York" shall mean to produce,
13 solicit, or offer for use or sale any product or service in a manner
14 that intentionally targets, or may reasonably be expected to contact,
15 New York residents, or to engage in any activity that would subject the
16 actor to personal jurisdiction under section three hundred one or three
17 hundred two of the civil practice law and rules, whether or not for
18 profit.

19 44. The term "covered entity" shall mean a legal entity that conducts
20 business in New York state and as part of such business, processes and
21 maintains the data of five hundred or more unique individuals.

22 45. The term "governmental entity" shall mean a department or agency
23 of the state or a political subdivision thereof, or an individual acting
24 for or on behalf of the state or a political subdivision thereof.

25 46. The term "individual" shall mean a natural person whom a covered
26 entity knows or has reason to know is located within New York state.

27 47. The term "personal information" shall mean information that
28 directly or indirectly identifies, relates to, describes, is capable of
29 being associated with, or could reasonably be linked to a particular
30 individual, household, or device. Information is reasonably linkable to
31 an individual, household, or device if it can be used on its own or in
32 combination with other reasonably available information, regardless of
33 whether such other information is held by the covered entity, to identi-
34 fy an individual, household, or device.

35 48. The term "process" or "processing" shall mean any action or set of
36 actions performed on or with personal information, including but not
37 limited to, collection, access, use, retention, sharing, monetizing,
38 analysis, creation, generation, derivation, decision-making, recording,
39 alternation, organization, structuring, storage, disclosure, trans-
40 mission, sale, licensing, disposal, destruction, de-identifying, or
41 other handling of personal information.

42 49. The term "proxy" or "proxies" shall mean information that, by
43 itself or in combination with other information, is used by a covered
44 entity in a way that discriminates based on actual or perceived personal
45 characteristics or classes protected under section two hundred ninety-
46 six of this article.

47 50. The term "targeted advertisement" shall mean an advertisement
48 directed to an individual where the advertisement is selected based on
49 personal information obtained or inferred over time from such individ-
50 ual's or the individual's device's activities, communications, or asso-
51 ciations across websites, applications, services, or covered entities.
52 Such term shall not include advertisements directed to an individual
53 solely based upon the individual's current visit to a website, applica-
54 tion, service, or covered entity, or in response to the individual's
55 request for information or feedback.

§ 5. The executive law is amended by adding a new section 296-e to read as follows:

§ 296-e. Unlawful discriminatory practices relating to targeted advertising. 1. It shall be an unlawful discriminatory practice:

(a) For a covered entity to process personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, health care, credit, insurance, housing, or education opportunities, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of an individual's or class of individuals' actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status.

(b) For a covered entity or governmental entity to process personal information in a manner that discriminates in or otherwise makes unavailable, on the basis of an individual's or class of individuals' actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status, any of the following:

(i) The goods, services, facilities, privileges, advantages, or accommodations of any inn, hotel, motel, or other place of lodging, except for an establishment located within a building that contains not more than five rooms for rent or hire and that is actually occupied by the proprietor of such establishment as the residence of such proprietor;

(ii) Any restaurant, bar, or other establishment serving food or drink to the public;

(iii) Any motion picture house, theater, concert hall, stadium, auditorium, convention center, or lecture hall;

(iv) Any sales or rental establishment;

(v) Any laundromat, dry-cleaner, bank, barber shop, beauty shop, travel service, shoe repair service, funeral parlor, gas station, office of an accountant or lawyer, pharmacy, insurance office, professional office of a health care provider, hospital, or other service establishment;

(vi) Any terminal, depot, or other station used for specified public transportation;

(vii) Any museum, library, or gallery;

(viii) Any park, zoo, or amusement park;

(ix) A nursery, elementary, secondary, undergraduate, or postgraduate school, or other place of education;

(x) Any day care center, senior citizen center, homeless shelter, food bank, adoption agency, or other social service center establishment; or

(xi) Any gymnasium, health spa, bowling alley, golf course, or other place of exercise.

(c) For a covered entity or governmental entity that offers, facilitates, sells, places, displays, or provides individual level information to enable targeted advertisements for employment, finance, health care, credit, insurance, housing, education opportunities, or places of public accommodation, resort or amusement, as described in paragraph (b) of this subdivision, to enable advertisers to target such advertisements based on actual or perceived personal characteristics or classes, or proxies therefor, protected under section two hundred ninety-six of this article, including actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disabili-

1 ity, predisposing genetic characteristics, or domestic violence victim
2 status.

3 2. A covered entity or governmental entity that sells or places
4 targeted advertisements for employment, finance, health care, credit,
5 insurance, housing, education opportunities or places of public accommo-
6 dation, resort or amusement, as described in paragraph (b) of this
7 subdivision, shall require advertisers to certify that they are in
8 compliance with section two hundred ninety-six of this article.

9 3. Nothing in this section shall limit a covered entity from process-
10 ing personal information for legitimate testing for the purpose of
11 preventing unlawful discrimination or otherwise determining the extent
12 or effectiveness of such covered entity's or governmental entity's
13 compliance with this section.

14 § 6. The general business law is amended by adding a new section 350-
15 a-1 to read as follows:

16 § 350-a-1. Targeted advertising. 1. For the purposes of this section,
17 the following terms shall have the following meanings:

18 (a) "Advertiser" shall mean a person who proposes a commercial trans-
19 action or disseminates a public or private communication of which the
20 primary purpose is to solicit for an opportunity.

21 (b) "Conduct business in New York" shall mean to produce, solicit, or
22 offer for use or sale any product or service in a manner that inten-
23 tionally targets, or may reasonably be expected to contact, New York
24 residents, or to engage in any activity that would subject the actor to
25 personal jurisdiction under section three hundred one or section three
26 hundred two of the civil practice law and rules, whether or not for
27 profit.

28 (c) "Covered entity" shall mean a legal entity that conducts business
29 in New York state and as part of such business, processes and maintains
30 the data of five hundred or more unique individuals.

31 (d) "Individual" shall mean a natural person whom a covered entity
32 knows or has reason to know is located within New York state.

33 (e) "Personal information" shall mean information that directly or
34 indirectly identifies, relates to, describes, is capable of being asso-
35 ciated with, or could reasonably be linked to a particular individual,
36 household, or device. Information is reasonably linkable to an individ-
37 ual, household, or device if it can be used on its own or in combination
38 with other reasonably available information, regardless of whether such
39 other information is held by the covered entity, to identify an individ-
40 ual, household, or device.

41 (f) "Process" or "processing" shall mean any action or set of actions
42 performed on or with personal information, including but not limited to,
43 collection, access, use, retention, sharing, monetizing, analysis,
44 creation, generation, derivation, decision-making, recording, alter-
45 nation, organization, structuring, storage, disclosure, transmission,
46 sale, licensing, disposal, destruction, de-identifying, or other handl-
47 ing of personal information.

48 (g) "Proxy" or "proxies" shall mean information that, by itself or in
49 combination with other information, is used by a covered entity in a way
50 that discriminates based on actual or perceived personal characteristics
51 or classes protected under section two hundred ninety-six of the execu-
52 tive law.

53 (h) "Targeted advertisement" shall mean an advertisement directed to
54 an individual where the advertisement is selected based on personal
55 information obtained or inferred over time from such individual's or the
56 individual's device's activities, communications, or associations across

websites, applications, services, or covered entities. Such term shall not include advertisements directed to an individual solely based upon the individual's current visit to a website, application, service, or covered entity, or in response to the individual's request for information or feedback.

2. It shall be unlawful:

(a) For a covered entity to process personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, health care, credit, insurance, housing, or education opportunities, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of an individual's or class of individuals' actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status.

(b) For a covered entity or governmental entity to process personal information in a manner that discriminates in or otherwise makes unavailable, on the basis of an individual's or class of individuals' actual or perceived age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status, any of the following:

(i) The goods, services, facilities, privileges, advantages, or accommodations of any inn, hotel, motel, or other place of lodging, except for an establishment located within a building that contains not more than five rooms for rent or hire and that is actually occupied by the proprietor of such establishment as the residence of such proprietor;

(ii) Any restaurant, bar, or other establishment serving food or drink to the public;

(iii) Any motion picture house, theater, concert hall, stadium, auditorium, convention center, or lecture hall;

(iv) Any sales or rental establishment;

(v) Any laundromat, dry-cleaner, bank, barber shop, beauty shop, travel service, shoe repair service, funeral parlor, gas station, office of an accountant or lawyer, pharmacy, insurance office, professional office of a health care provider, hospital, or other service establishment;

(vi) Any terminal, depot, or other station used for specified public transportation;

(vii) Any museum, library, or gallery;

(viii) Any park, zoo, or amusement park;

(ix) A nursery, elementary, secondary, undergraduate, or postgraduate school, or other place of education;

(x) Any day care center, senior citizen center, homeless shelter, food bank, adoption agency, or other social service center establishment; or

(xi) Any gymnasium, health spa, bowling alley, golf course, or other place of exercise.

(c) For a covered entity that offers, facilitates, sells, places, displays, or provides individual level information to enable targeted advertisements for employment, finance, health care, credit, insurance, housing, education opportunities, or places of public accommodation, resort or amusement, as described in paragraph (b) of this subdivision, to enable advertisers to target such advertisements based on actual or perceived personal characteristics or classes, or proxies therefor, protected under section two hundred ninety-six of the executive law, including actual or perceived age, race, creed, color, national origin,

sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status.

3. A covered entity that sells or places targeted advertisements for employment, finance, health care, credit, insurance, housing, education opportunities or places of public accommodation, resort or amusement, as described in paragraph (b) of subdivision two of this section, shall require advertisers to certify that they are in compliance with section two hundred ninety-six of the executive law.

4. Nothing in this section shall limit a covered entity from processing personal information for legitimate testing for the purpose of preventing unlawful discrimination or otherwise determining the extent or effectiveness of such covered entity's compliance with this section.

§ 7. Section 165 of the state finance law is amended by adding two new subdivisions 9 and 10 to read as follows:

9. Automated decision system impact assessments.

a. For the purpose of this subdivision, the following terms shall have the following meanings:

(i) "Automated decision system" shall mean any software, system, or process that is designed to aid or replace human decision making. Such term may include analyzing complex datasets to generate scores, predictions, classifications, or some recommended action or actions, which are used by agencies to make decisions that impact human welfare.

(ii) "Automated decision system impact assessment" shall mean a study evaluating an automated decision system and the automated decision system's development processes, including the design and training data of the automated decision system, for statistical impacts on classes protected under section two hundred ninety-six of the executive law, as well as for impacts on privacy, and security that includes at a minimum:

(A) A detailed description of the automated decision system, its design, its training, its data, and its purpose;

(B) An assessment of the relative benefits and costs of the automated decision system in light of its purpose, taking into account relevant factors, including data minimization practices, the duration for which personal information and the results of the automated decision system are stored, what information about the automated decision system are available to the public, and the recipients of the results of the automated decision system;

(C) An assessment of the risk of harm posed by the automated decision system and the risk that such automated decision system may result in or contribute to inaccurate, unfair, biased, or discriminatory decisions impacting individuals; and

(D) The measures the state agency will employ to minimize the risks described in item (C) of this subparagraph, including technological and physical safeguards.

(iii) "Harm" shall mean potential or realized adverse consequences to an individual or to society, including but not limited to:

(A) Direct or indirect financial harm.

(B) Physical harm or threats to persons or property, including but not limited to bias-related crimes and threats, harassment, and sexual harassment.

(C) Discrimination in goods, services, or economic opportunity, including but not limited to housing, employment, credit, insurance, education, or health care on the basis of an individual or class of individuals' actual or perceived age, race, national origin, sex, sexual

orientation, gender identity, marital status, disability, military status, and/or membership in another protected class.

(D) Interference with or surveillance of first amendment-protected activities by state actors.

(E) Interference with the right to vote or with free and fair elections.

(F) Interference with due process or equal protection under law.

(G) Loss of individual control over personal information, nonconsensual sharing of private information, and data breach.

(H) The nonconsensual capture of information or communications within an individual's home or where an individual has a reasonable expectation of seclusion or access control.

(I) Other effects on an individual that may not be reasonably foreseeable to, contemplated by, or expected by the individual to whom the personal information relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity that alter or limit such individual's choices or predetermine results.

(iv) "Individual" shall mean a natural person whom a covered entity knows or has reason to know is located within New York state.

(v) "Personal information" shall mean information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device. Information is reasonably linkable to an individual, household, or device if it can be used on its own or in combination with other reasonably available information, regardless of whether such other information is held by the state agency, to identify an individual, household, or device.

(vi) "Proxy" or "proxies" shall mean information that, by itself or in combination with other information, is used by a covered entity in a way that discriminates based on actual or perceived personal characteristics or classes protected under section two hundred ninety-six of the executive law.

(vii) "Training data" shall mean the datasets used to train an automated decision system, machine learning algorithm, or classifier to create and derive patterns from a prediction model.

b. The state and any governmental agency, political subdivision or public benefit corporation of the state shall not purchase, obtain, procure, acquire, employ, use, deploy, or access information from an automated decision system unless it first engages a neutral third party to conduct an automated decision system impact assessment and publishes on its public website that automated decision system impact assessment:

(i) Of existing automated decision system within one year of the effective date of this subdivision and every two years thereafter.

(ii) Of new automated decision systems prior to acquisition and every two years thereafter.

c. Upon publication of an automated decision system impact assessment, the public shall have forty-five days to submit comments on such assessment to the state and any governmental agency, political subdivision or public benefit corporation. The state and any governmental agency, political subdivision or public benefit corporation shall consider such public comments when determining whether to purchase, obtain, procure, acquire, employ, use, deploy, or access information from an automated decision system and shall post responses to such public comments to its website within forty-five days after the close of the public comment period.

d. The state procurement council shall, in consultation with the office of information technology services, the division of human rights and experts and representatives from the communities that will be directly affected by automated decision systems, promulgate rules and regulations to set the minimum standard entities shall meet to serve as neutral third parties conducting automated decision system impact assessments.

e. The state procurement council shall maintain a publicly available list of neutral third parties that meet the qualifications outlined in paragraph d of this subdivision.

f. Within two years of the effective date of this subdivision, the office of information technology services, in consultation with the division of human rights and experts and representatives from the communities that will be directly affected by automated decision systems, shall complete and publish on its website a comprehensive study of the statistical impacts of automated decision systems on classes protected under section two hundred ninety-six of the executive law, including but not limited to, evaluating the use of proxies and the types of data used in training data sets and the risks associated with particular types of training data.

(i) As part of such study, the office of information technology services shall review the automated decision system impact assessments that have been published prior to completion of the study, as well as the public comments submitted in response to such automated decision impact assessments.

(ii) The office may request data and information from: state agencies; consumer protection, civil rights, and privacy advocates; researchers and academics; private entities that develop or deploy automated decision systems; and other relevant sources to meet the purpose of such study. The office shall receive, upon request, data from other state agencies.

10. Automated decision system use policies; notice and human review requirements.

a. For the purpose of this subdivision, the following terms shall have the following meanings:

(i) "Automated decision system" shall mean any software, system, or process that is designed to aid or replace human decision making. Such term may include analyzing complex datasets to generate scores, predictions, classifications, or some recommended action or actions, which are used by agencies to make decisions that impact human welfare.

(ii) "Automated decision system use policy" shall mean:

(A) A description of the capabilities of the automated decision system, any decisions that such system is used to make or assist in making and any specific types or groups of persons protected under section two hundred ninety-six of the executive law who are likely to be affected by such decisions;

(B) Rules, processes, and guidelines issued by the state agency regulating access to or use of such automated decision system, as well as any prohibitions or restrictions on use;

(C) Safeguards or security measures designed to protect information collected by or inputted into such automated decision system, including but not limited to, the existence of encryption and access control mechanisms;

(D) Policies and practices relating to the retention, access, and use of data collected by or inputted into such automated decision system, as well as the decisions rendered by such automated decision system;

1 (E) Whether other entities outside the state agency have access to the
2 information and data used by or inputted into the automated decision
3 system or the decisions rendered by the automated decision system,
4 including whether the outside entity is local, state, federal, or
5 private, the type of information and data that may be disclosed, and any
6 safeguards or restrictions imposed by the agency on the outside entity
7 regarding the use or dissemination of the information, data, or deci-
8 sion;

9 (F) Whether any training is required by the state agency for an indi-
10 vidual to use such automated decision system or access information
11 collected by or inputted into such automated decision system or the
12 decisions rendered by the automated decision system;

13 (G) A description of the internal and external audit and oversight
14 mechanisms, including the mechanism for human review required under
15 paragraph g of this subdivision, to ensure compliance with the automated
16 decision use policy and that the automated decision system does not
17 result in harm to an individual;

18 (H) Relevant technical information about the automated decision
19 system, including the system's name, vendor, and version, as well as a
20 description of the automated decision system's general capabilities,
21 including reasonably foreseeable capabilities outside the scope of the
22 agency's proposed use;

23 (I) The type or types of data inputs that the automated decision
24 system uses, how that data is generated, collected, and processed, and
25 the types of data the system is reasonably likely to generate;

26 (J) How and when the automated decision system will be deployed or
27 used and by whom, including but not limited to, the factors that will be
28 used to determine where, when, and how the technology is deployed;

29 (K) A description of any public or community engagement held and any
30 future public or community engagement plans in connection with the auto-
31 mated decision system; and

32 (L) A description of the fiscal impact of the automated decision
33 system, including initial acquisition costs, ongoing operating costs,
34 such as maintenance, licensing, personnel, legal compliance, use audit-
35 ing, data retention, and security costs, and any current or potential
36 sources of funding, including any subsidies or free products offered by
37 vendors or governmental entities.

38 (iii) "De-identified information" shall mean information that cannot
39 reasonably identify, relate to, describe, be capable of being associated
40 with, or be linked, directly or indirectly, to a particular individual;
41 provided that a covered entity that uses de-identified information:

42 (A) Has implemented technical safeguards that prohibit reidentifica-
43 tion of the individual to whom such information may pertain;

44 (B) Has implemented business processes that specifically prohibit
45 reidentification of such information;

46 (C) Has implemented business processes that prevent inadvertent
47 release of such de-identified information; and

48 (D) Makes no attempt to reidentify such information.

49 (iv) "Harm" shall mean potential or realized adverse consequences to
50 an individual or to society, including but not limited to:

51 (A) Direct or indirect financial harm.

52 (B) Physical harm or threats to persons or property, including but not
53 limited to bias-related crimes and threats, harassment, and sexual
54 harassment.

55 (C) Discrimination in goods, services, or economic opportunity,
56 including but not limited to housing, employment, credit, insurance,

1 education, or health care on the basis of an individual or class of
2 individuals' actual or perceived age, race, national origin, sex, sexual
3 orientation, gender identity, marital status, disability, military
4 status, and/or membership in another protected class.

5 (D) Interference with or surveillance of first amendment-protected
6 activities by state actors.

7 (E) Interference with the right to vote or with free and fair
8 elections.

9 (F) Interference with due process or equal protection under law.

10 (G) Loss of individual control over personal information, nonconsensu-
11 al sharing of private information, and data breach.

12 (H) The nonconsensual capture of information or communications within
13 an individual's home or where an individual has a reasonable expectation
14 of seclusion or access control.

15 (I) Other effects on an individual that may not be reasonably foresee-
16 able to, contemplated by, or expected by the individual to whom the
17 personal information relates, that are nevertheless reasonably foreseea-
18 ble, contemplated by, or expected by the covered entity that alter or
19 limit such individual's choices or predetermine results.

20 (v) "Individual" shall mean a natural person whom a covered entity
21 knows or has reason to know is located within New York state.

22 (vi) "Personal information" shall mean information that directly or
23 indirectly identifies, relates to, describes, is capable of being asso-
24 ciated with, or could reasonably be linked to a particular individual,
25 household, or device. Information is reasonably linkable to an individ-
26 ual, household, or device if it can be used on its own or in combination
27 with other reasonably available information, regardless of whether such
28 other information is held by the state agency, to identify an individ-
29 ual, household, or device.

30 (vii) "Relevant technical information" shall include, but not be
31 limited to, source code, models, documentation on the algorithms used,
32 design documentation and information about technical architecture,
33 training data, data provenance information, justification for the valid-
34 ity of the model, any records of bias, and any validation testing
35 performed on the system.

36 b. The state and any governmental agency, political subdivision or
37 public benefit corporation of the state that purchases, obtains,
38 procures, acquires, employs, uses, deploys, or accesses information from
39 an automated decision system shall publish on its website at least nine-
40 ty days prior to the purchase, obtaining, use, acquisition, or deploy-
41 ment of new automated decision systems and, for existing automated deci-
42 sion systems, within one hundred eighty days of the effective date of
43 this subdivision, an automated decision system use policy.

44 (i) When the state and any governmental agency, political subdivision
45 or public benefit corporation of the state seeks to change or changes an
46 automated decision system in a way that affects the results or outcomes
47 of the automated decision system or uses such automated decision system
48 for a purpose or manner not previously disclosed through an automated
49 decision system use policy, it shall provide an addendum to the existing
50 automated decision system use policy describing such change or addi-
51 tional use and retain an archived copy of the previous automated deci-
52 sion system so that decisions made under the old system use policy may
53 be challenged under paragraph g of this subdivision.

54 (ii) Upon publication of, or addendum to, any proposed automated deci-
55 sion system policy, the public shall have forty-five days to submit

1 comments on such policy to the state and any governmental agency or
2 political subdivision or public benefit corporation.

3 (iii) The state and any governmental agency, political subdivision or
4 public benefit corporation shall consider public comments and provide
5 the final automated decision system use policy to the office of informa-
6 tion technology services, the committee on open government, and the
7 state procurement council, and shall post such decision to its website
8 no later than forty-five days after the close of the public comment
9 period.

10 c. The state and any governmental agency, political subdivision or
11 public benefit corporation shall obtain approval from the city or county
12 council with appropriate jurisdiction or the state legislature, follow-
13 ing the public comment period required in paragraph b of this subdivi-
14 sion, and a properly-noticed, germane, public hearing at which the
15 public is afforded a fair and adequate opportunity to provide online,
16 written, and oral testimony, prior to:

17 (i) Seeking funds for an automated decision system that assigns or
18 contributes to the determination of rights, benefits, opportunities, or
19 services for an individual, including but not limited to, applying for a
20 grant, or soliciting or accepting state or federal funds or in-kind or
21 other donations;

22 (ii) Acquiring or borrowing an automated decision system that assigns
23 or contributes to the determination of rights, benefits, opportunities,
24 or services for an individual, whether or not such acquisition is made
25 through the exchange of monies or other consideration;

26 (iii) Using a new or existing automated decision system that assigns
27 or contributes to the determination of rights, benefits, opportunities,
28 or services for an individual, or data derived therefrom, for a purpose
29 or in a manner not previously approved by the city or county council
30 with appropriate jurisdiction or the state legislature; or

31 (iv) Soliciting proposals for or entering into an agreement with any
32 other person or entity to acquire, share, or otherwise use an automated
33 decision system that assigns or contributes to the determination of
34 rights, benefits, opportunities, or services for an individual or auto-
35 mated decision system data.

36 d. The committee on open government shall conduct annual audits of
37 automated decision system use policies that shall:

38 (i) Assess whether each state agency that purchases, obtains,
39 procures, acquires, employs, uses, deploys, or accesses information from
40 an automated decision system complies with the terms of the automated
41 decision system use policy;

42 (ii) Describes any known or reasonably suspected violations of any
43 automated decision system use policies; and

44 (iii) Publish recommendations, if any, relating to revision of the
45 relevant automated decision system use policies.

46 e. The state and any governmental agency, political subdivision or
47 public benefit corporation of the state shall not purchase, obtain,
48 procure, acquire, employ, use, deploy, or access information from an
49 automated decision system that assigns or contributes to the determi-
50 nation of rights, benefits, opportunities, or services for an individual
51 unless it first implements a process to provide a plain-language notifi-
52 cation to any individual whose personal information is processed by the
53 automated decision system and whom the automated decision system's deci-
54 sion affects of the fact that such system is in use, the system's name,
55 vendor, and version, what decision or decisions will be used to make or
56 support; and what policies and guidelines apply to its deployment.

1 f. The state and any governmental agency, political subdivision or
2 public benefit corporation of the state shall not purchase, obtain,
3 procure, acquire, employ, use, deploy, or access information from an
4 automated decision system that assigns or contributes to the determi-
5 nation of rights, benefits, opportunities, or services for an individual
6 unless it first implements a process to provide a plain-language notifi-
7 cation to any individual whose personal information is processed by such
8 automated decision system and whom such automated decision system's
9 decision affects, of the involvement of an automated decision system in
10 making the decision, the degree of human intervention in the system, how
11 the automated decision system made the decision, the justification for
12 the decision, the variables considered in rendering the decision, wheth-
13 er and how the decision deviated from the automated decision's system's
14 recommendation, how the individual may contest the decision pursuant to
15 paragraph g of this subdivision, and the process for requesting human
16 review of the decision pursuant to paragraph g of this subdivision.

17 (i) The state and any governmental agency, political subdivision or
18 public benefit corporation of the state shall ensure that it can explain
19 the basis for its decision to any impacted individual in terms under-
20 standable to a layperson including, without limitation, by requiring the
21 vendor to create such explanation.

22 (ii) The committee on open government, in consultation with the divi-
23 sion of human rights, the office of information technology services, and
24 experts and representatives from the communities that will be directly
25 affected by automated decision systems, may promulgate rules and regu-
26 lations specifying the requirements for such notice.

27 g. The state and any governmental agency, political subdivision or
28 public benefit corporation of the state shall not purchase, obtain,
29 procure, acquire, employ, use, deploy, or access information from an
30 automated decision system that assigns or contributes to the determi-
31 nation of rights, benefits, opportunities, or services for an individual
32 unless it first develops a process for human review.

33 (i) The office of information technology services, in consultation
34 with the division of human rights, the committee on open government and
35 experts and representatives from the communities that will be directly
36 affected by automated decision systems, may promulgate rules and regu-
37 lations specifying the requirements for human review of decisions
38 rendered by automated decision systems.

39 (ii) An individual who was denied or assigned a right, benefit, oppor-
40 tunity or service, may request human review of the decision rendered by
41 the automated decision system.

42 (iii) Where the human review overturns a decision rendered by an auto-
43 mated decision system, the affected individual experiences harm as a
44 result of the overturned decision, and the state or any governmental
45 agency, political subdivision or public benefit corporation of the state
46 cannot or will not provide a remedy, or where the human review does not
47 overturn a decision rendered by an automated decision system, the
48 affected individual, or their heirs, assigns, estate, or successors in
49 interest, may bring in any court of competent jurisdiction an action
50 alleging a violation of this subdivision.

51 (iv) The court shall award to the prevailing plaintiff in such action,
52 the following relief:

53 (A) Any injunctive or other equitable relief the court deems appropri-
54 ate;

1 (B) Any actual damages resulting from any violation of this subdivi-
2 sion, or ten thousand dollars in damages for each such violation, which-
3 ever is greater;

4 (C) Reasonable attorney's fees and costs; and

5 (D) Any other relief the court deems appropriate.

6 h. The state and any governmental agency, political subdivision or
7 public benefit corporation of the state that purchases, obtains,
8 procures, acquires, employs, uses, deploys, or accesses information from
9 an automated decision system that assigns or contributes to the determi-
10 nation of rights, benefits, opportunities, or services for an individual
11 shall annually publish publicly on its website metrics on the number of
12 requests for human review of a decision rendered by the automated deci-
13 sion system it received and the outcome of such human review. The
14 metrics may include de-identified information in the aggregate but shall
15 not include any personal information.

16 § 8. Section 8 of the state finance law is amended by adding a new
17 subdivision 21 to read as follows:

18 21. Notwithstanding any inconsistent provision of law, no payment
19 shall be made for an automated decision system, as defined in section
20 one hundred sixty-five of this chapter, that assigns or contributes to
21 the determination of rights, benefits, opportunities, or services for an
22 individual unless the automated decision system uses only open source
23 software and the acquiring agency has complied with the automated deci-
24 sion system impact assessment and automated decision system use policy
25 requirements in section one hundred sixty-five of this chapter. For the
26 purposes of this subdivision, "open source software" shall mean software
27 for which the human-readable source code is available for use, study,
28 modification, and enhancement by the users of that software.

29 § 9. Section 8 of the state finance law is amended by adding four new
30 subdivisions 22, 23, 24 and 25 to read as follows:

31 22. Notwithstanding any inconsistent provision of law, no payment
32 shall be made for an automated decision system, as defined in section
33 one hundred sixty-five of this chapter, that assigns or contributes to
34 the determination of rights, benefits, opportunities, or services for an
35 individual, prior to the approval from the city or county council with
36 appropriate jurisdiction or the state legislature as required in section
37 one hundred sixty-five of this chapter.

38 23. Notwithstanding any inconsistent provision of law, no payment
39 shall be made for an automated decision system, as defined in section
40 one hundred sixty-five of this chapter, if the vendor's contract
41 contains nondisclosure or other provisions that prohibit or impair the
42 state and any governmental agency or political subdivision or public
43 benefit corporation of the state's obligations under subdivisions nine
44 and ten of section one hundred sixty-five of this chapter.

45 24. Notwithstanding any inconsistent provision of law, no payment
46 shall be made for an automated decision system, as defined in section
47 one hundred sixty-five of this chapter, if the automated decision system
48 discriminates against an individual, or treats an individual less favor-
49 ably than another, in whole or in part, on the basis of one or more
50 factors enumerated in section two hundred ninety-six of the executive
51 law.

52 25. Notwithstanding any inconsistent provision of law, no payment
53 shall be made for an automated decision system that makes final deci-
54 sions, judgments, or conclusions without human intervention that impact
55 the constitutional or legal rights, duties, or privileges of any indi-

vidual in New York state or for any automated decision system that deploys or triggers any weapon.

§ 10. Section 814 of the education law, as added by chapter 526 of the laws of 2006 and subdivision 3 as added by chapter 545 of the laws of 2008, is amended to read as follows:

§ 814. Courses of study in internet safety. 1. ~~[Any school district in the state may provide, to pupils]~~ The regents shall ensure that the course of instruction in grades kindergarten through twelve~~[, instruction designed to promote the]~~ includes a component on digital literacy, digital privacy, and the proper and safe use of the internet.

2. The boards of education and trustees of the cities and school districts of the state shall require instruction to be given in such topics, by the teachers employed in the schools therein, commencing with the two thousand twenty-five--two thousand twenty-six school year. All pupils who attend public or charter schools shall receive such instruction.

3. The commissioner, in consultation with the chief privacy officer and the office of information technology services, shall ~~[provide technical assistance to assist in the development of curricula]~~ develop and establish a program for such courses of study which shall be age appropriate and developed according to the needs and abilities of pupils at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the internet. Such program shall include:

(a) Learning standards for digital literacy, digital privacy, and the proper and safe use of the internet in grades kindergarten through twelve that, at a minimum, instruct students on how to identify online fraud, as well as reliable sources and information, help students to understand how online activities are tracked and recorded, where personal information posted online may go, with whom it may be shared, and how it may be used, and offer best practices for protecting digital security and digital privacy;

(b) Model curricula for digital literacy, digital privacy, and the proper and safe use of the internet in grades kindergarten through twelve that are suitable to student age, based on cognitive, emotional, and behavioral capacity;

(c) Guidelines and professional training and development resources to support implementation of such instruction in schools;

(d) Public availability of all program materials related to digital literacy, digital privacy, and the proper and safe use of the internet on the department's website; and

(e) A system to track and evaluate such digital literacy, digital privacy, and the proper and safe use of the internet education, including, but not limited to, a reporting requirement that tracks and makes district compliance publicly available.

4. Such program shall be reviewed periodically by the commissioner, in consultation with the chief privacy officer and the office of information technology, at intervals specified by the commissioner, and updated as necessary.

5. The commissioner shall prescribe rules and regulations relating to such contents, topics, and courses to be included in a digital literacy, digital privacy, and the proper and safe use of the internet curriculum; provided, however, that the curricula need not be uniform throughout the state; and provided further, however, that school districts shall utilize either a curriculum for digital literacy, digital privacy, and the proper and safe use of the internet prescribed by the commissioner

1 or a curriculum in accordance with the standards and criteria estab-
2 lished by the commissioner.

3 6. The commissioner shall make recommendations to the board of regents
4 about a program on digital literacy, digital privacy, and the proper and
5 safe use of the internet, relevant learning standards, model curricula,
6 and curriculum resources, guidelines, and professional development
7 resources within one year of the effective date of this section. Upon
8 approval and adoption by the board of regents, the department shall
9 issue guidance to school districts and publish on its website model
10 curricula and instructional resources required by this section.

11 7. Prior to making such recommendations to the regents, the commis-
12 sioner shall seek the recommendations of teachers, school administra-
13 tors, teacher educators, digital privacy and security experts, journal-
14 ism experts, the chief information security office, and others with
15 educational expertise in the proposed curriculum.

16 ~~[3-]~~ 8. The commissioner shall develop age-appropriate resources and
17 technical assistance for schools to provide to students in grades three
18 through twelve and their parents or legal guardians concerning the safe
19 and responsible use of the internet. The resources shall include, but
20 not be limited to, information regarding how child predators may use the
21 internet to lure and exploit children, protecting personal information,
22 internet scams and cyber-bullying.

23 § 11. Severability. If any provision of this act, or any application
24 of any provision of this act, is held to be invalid, that shall not
25 affect the validity or effectiveness of any other provision of this act,
26 or of any other application of any provision of this act, which can be
27 given effect without that provision or application; and to that end, the
28 provisions and applications of this act are severable.

29 § 12. This act shall take effect immediately; provided, however, that
30 sections one, two, three, four, five and six of this act shall take
31 effect one year after it shall have become a law and section eight of
32 this act shall take effect two years after it shall have become a law.
33 Effective immediately, the addition, amendment and/or repeal of any rule
34 or regulation necessary for the implementation of this act on its effec-
35 tive date are authorized to be made and completed on or before such
36 effective date.