STATE OF NEW YORK

6042

2021-2022 Regular Sessions

IN ASSEMBLY

March 5, 2021

Introduced by M. of A. CRUZ -- read once and referred to the Committee on Consumer Affairs and Protection

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:

Section 1. Short title. This act shall be known and may be cited as the "digital fairness act".

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

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

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

LBD09748-03-1

The legislature further finds that entities that collect, use, retain, share, and monetize personal information have specialized knowledge about the algorithms and data security measures they use, as well as about how they collect, use, retain, share, and monetize personal information, that the average individual is unlikely to understand. Just as banks, lawyers, and medical providers, given their specialized knowledge, have special obligations to individuals, entities collecting intimate personal information in the digital age and benefiting from similarly specialized knowledge should have similar obligations.

The legislature also finds that individuals in New York state, like individuals across the country, value privacy and wish to control who has access to their personal information. Ninety-two percent of Facebook users alter the social network's default privacy settings, demonstrating that they wish to choose with whom they share personal information. Similarly, ninety-two percent of Americans believe companies should obtain individuals' permission before sharing or selling their personal information.

The legislature additionally finds that biometric information is unlike other unique identifiers, because biometric information is biologically unique to an individual and cannot be changed if compromised. As a result, biometric information merits special protections.

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

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

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

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

ARTICLE 39-FF

DIGITAL FAIRNESS ACT

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

1. "Biometric information" shall mean a record of one or more measurable biological or behavioral characteristics that can be used singularly or in combination with other characteristics, or with other information, for automated recognition of a known or unknown individual. Examples of such term shall include, but not be limited to: fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, gait, handwriting, key stroke dynamics, and mouse movements.

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

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

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

5. "Data processor" shall mean a person that processes personal information on behalf of a covered entity.

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

(a) Has implemented technical safeguards that prohibit reidentification of the individual to whom such information may pertain;

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

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

(d) Makes no attempt to reidentify such information.

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

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

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

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

information available to another person, intentionally or unintentionally, including but not limited to, sharing, publishing, releasing, transferring, disseminating, making available, selling, leasing, providing access to, failing to restrict access to, or otherwise communicating orally, in writing, electronically, or by any other means.

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

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

13. "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.

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

15. "Personal information" shall mean information that is captured in exchange for any kind of value provided to the individual to whom the information pertains, including but not limited to a good or service, the placement of targeted advertisements, or a membership; as a result of an individual, household, or device's establishment or maintenance of an account with a covered entity; or as a result of an individual, household, or device's interaction with a covered entity. Such term shall also include 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 that provides or provided information to a covered entity in exchange for any kind of value provided to the individual to whom such information pertains or that established, maintained, establishes or maintains an account with a covered entity. 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 covered entity, to identify an individual, household, or device.

16. "Monetize" shall mean to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, an individual's personal information by a covered entity, a third party, or a data processor in exchange for monetary or other consideration, as well as to leverage or use an individual's personal information to place a targeted advertisement or to otherwise profit, regardless of whether such individual's personal information changes hands.

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

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

19. "Targeted advertisement" shall mean an advertisement directed to an individual where the advertisement is selected based on personal information obtained or inferred over time from such individual's or the 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.

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

21. "Use model" shall mean a discrete purpose for which collected personal information is to be processed, including but not limited to, first party marketing, third party marketing, first party research and development, third party research and development, and product improvement.

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

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

(b) Persistently available and readily accessible on a covered entity's website or mobile application;

(c) At the physical place of business or any offline equivalent maintained by the covered entity; and

(d) At or prior to the point of sale of a product or service, subscription to a service, or establishment of an account with, the covered entity or if there is no such sale, subscription, or establishment, before the individual uses such product or service of the covered entity.

2. The short-form privacy notice required by subdivision one of this 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.

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

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

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

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

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

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

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

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

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

(g) If required by state or federal law.

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

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

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

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

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

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

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

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

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

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

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

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

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

the security standards developed are more protective of personal information than the industry standard of care.

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

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

(c) A covered entity that maintains an individual's personal information shall provide the access to such personal information under paragraph (b) of this subdivision, in a usable and searchable format that allows the individual to transfer the personal information from one entity to another entity without hindrance.

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

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

(i) Clear and conspicuous;

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

(iii) In a language other than English if the covered entity communicates with the individual to whom the information pertains in such other language.

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

(i) Where the covered entity has reasonable doubts or cannot verify the identity of the individual making a request under paragraphs (b), (c) or (d) of this subdivision, the covered entity may request additional personal information necessary for the specific purpose of confirming the identity of such individual. In such cases, the additional personal information shall not be processed for any purpose other than verifying the identity of the individual and shall be deleted immediately upon verification or failure to verify the individual.

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

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

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

(h) A covered entity shall not share an individual's device identifiers with any third party without the individual's freely given, specific, informed, and unambiguous opt-in written consent.

3. Confidentiality. (a) A covered entity shall not disclose personal information to a third party unless that third party is contractually bound to the covered entity to meet the same privacy and security obligations as the covered entity. A covered entity shall exercise reasonable oversight and take reasonable actions, including by auditing the data security and processing practices of the third party no less than once annually, to ensure the third party's compliance. The covered entity shall publish the results of such audit publicly on its website.

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

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

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

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

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

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

(a) Informs the subject or the subject's legally authorized representative in writing that biometric information is being collected or stored;

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

(c) Receives a written release executed by the subject of the biometric information or the subject's legally authorized representative.

3. Absent a law enforcement investigation pursuant to a criminal incident, no governmental entity shall collect, capture, purchase, receive through trade, or otherwise obtain an individual's biometric information, unless:

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

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

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

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

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

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

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

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

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

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

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

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

7. (a) Subdivisions one through six of this section shall not apply to biometric information captured from a patient by a health care provider or health care facility, as defined in section eighteen of the public health law, or biometric information collected, used, or stored for medical education or research, public health or epidemiological purposes, health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996, or to X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

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

(i) Clinical, treatment, scientific, public health, medical educational, medical training, research, or insurance purposes;

(ii) If required by state or federal law;

(iii) To respond to a warrant issued by a court of competent jurisdiction under the procedures described in the federal rules of criminal procedure or article six hundred ninety of the criminal procedure law; or

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

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

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

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

(a) A violation of this article, or a violation of a rule or regulation promulgated to effectuate the provisions of this article, with respect to the personal information of an individual constitutes a rebuttable presumption of harm to such individual.

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

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

(ii) Punitive damages; and

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

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

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

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

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

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

(d) Any other relief the court deems appropriate.

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

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

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

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

(d) Any other relief the court deems appropriate.

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

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

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

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

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

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

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

§ 4. Section 292 of the executive law is amended by adding nine new subdivisions 39, 40, 41, 42, 43, 44, 45, 46 and 47 to read as follows:

39. The term "advertiser" shall mean a person who proposes a commercial transaction or disseminates a public or private communication of which the primary purpose is to solicit for an opportunity.

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

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

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

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

44. The term "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 covered entity, to identify an individual, household, or device.

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

46. The term "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 this article.

47. The term "targeted advertisement" shall mean an advertisement directed to an individual where the advertisement is selected based on personal information obtained or inferred over time from such individual's or the 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.

§ 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, disabil-

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

2. A covered entity or governmental 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 this subdivision, shall require advertisers to certify that they are in compliance with section two hundred ninety-six of this article.

3. 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 or governmental entity's compliance with this section.

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

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

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

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

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

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

(e) "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 covered entity, to identify an individual, household, or device.

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

(g) "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.

(h) "Targeted advertisement" shall mean an advertisement directed to an individual where the advertisement is selected based on personal information obtained or inferred over time from such individual's or the 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;

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

(F) Whether any training is required by the state agency for an individual to use such automated decision system or access information collected by or inputted into such automated decision system or the decisions rendered by the automated decision system;

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

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

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

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

(K) A description of any public or community engagement held and any future public or community engagement plans in connection with the automated decision system; and

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

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

(A) Has implemented technical safeguards that prohibit reidentification of the individual to whom such information may pertain;

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

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

(D) Makes no attempt to reidentify such information.

(iv) "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.

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

(vi) "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.

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

b. The state and any governmental agency, political subdivision or public benefit corporation of the state that purchases, obtains, procures, acquires, employs, uses, deploys, or accesses information from an automated decision system shall publish on its website at least ninety days prior to the purchase, obtaining, use, acquisition, or deployment of new automated decision systems and, for existing automated decision systems, within one hundred eighty days of the effective date of this subdivision, an automated decision system use policy.

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

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

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

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

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

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

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

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

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

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

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

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

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

e. 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 that assigns or contributes to the determination of rights, benefits, opportunities, or services for an individual unless it first implements a process to provide a plain-language notification to any individual whose personal information is processed by the automated decision system and whom the automated decision system's decision affects of the fact that such system is in use, the system's name, vendor, and version, what decision or decisions will be used to make or support; and what policies and guidelines apply to its deployment.

f. 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 that assigns or contributes to the determination of rights, benefits, opportunities, or services for an individual unless it first implements a process to provide a plain-language notification to any individual whose personal information is processed by such automated decision system and whom such automated decision system's decision affects, of the involvement of an automated decision system in making the decision, the degree of human intervention in the system, how the automated decision system made the decision, the justification for the decision, the variables considered in rendering the decision, whether and how the decision deviated from the automated decision's system's recommendation, how the individual may contest the decision pursuant to paragraph g of this subdivision, and the process for requesting human review of the decision pursuant to paragraph g of this subdivision.

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

(ii) The committee on open government, in consultation with the division of human rights, the office of information technology services, and experts and representatives from the communities that will be directly affected by automated decision systems, may promulgate rules and regulations specifying the requirements for such notice.

g. 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 that assigns or contributes to the determination of rights, benefits, opportunities, or services for an individual unless it first develops a process for human review.

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

(ii) An individual who was denied or assigned a right, benefit, opportunity or service, may request human review of the decision rendered by the automated decision system.

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

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

(A) Any injunctive or other equitable relief the court deems appropriate;

(B) Any actual damages resulting from any violation of this subdivision, or ten thousand dollars in damages for each such violation, whichever is greater;

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

(D) Any other relief the court deems appropriate.

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

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

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

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

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

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

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

25. Notwithstanding any inconsistent provision of law, no payment shall be made for an automated decision system that makes final decisions, judgments, or conclusions without human intervention that impact 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-three--two thousand twenty-four 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

or a curriculum in accordance with the standards and criteria established by the commissioner.

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

7. Prior to making such recommendations to the regents, the commissioner shall seek the recommendations of teachers, school administrators, teacher educators, digital privacy and security experts, journalism experts, the chief information security office, and others with educational expertise in the proposed curriculum.

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

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

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