STATE OF NEW YORK

1362--A

2023-2024 Regular Sessions

IN ASSEMBLY

January 17, 2023

Introduced by M. of A. GUNTHER, VANEL, EPSTEIN, REYES, SAYEGH, COOK, ZEBROWSKI, CRUZ, HYNDMAN, GLICK, DICKENS, SMULLEN, J. M. GIGLIO, McDONOUGH, BLANKENBUSH, LUPARDO, EACHUS, KELLES, BENDETT, GALLAHAN, SIMON, GANDOLFO, BRABENEC -- Multi-Sponsored by -- M. of A. ANGELINO -- read once and referred to the Committee on Consumer Affairs and Protection -- recommitted to the Committee on Consumer Affairs and Protection in accordance with Assembly Rule 3, sec. 2 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to biometric privacy

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

Section 1. The general business law is amended by adding a new article 32-A to read as follows:

ARTICLE 32-A

BIOMETRIC PRIVACY ACT

Section 676. Short title.
676-a. Definitions.
676-b. Retention; collection; disclosure; destruction.
676-c. Regulatory authority and enforcement.
676-d. Construction with other laws.
676-e. Severability.

§ 676. Short title. This article shall be known and may be cited as the "biometric privacy act".

§ 676-a. Definitions. As used in this article: 1. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers shall not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair

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

LBD01142-03-4

color, or eye color. Biometric identifiers shall not include donated body parts as defined in section forty-three hundred of the public health law or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, magnetic resonance imaging, positron-emission tomography 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.

2. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information shall not include information derived from items or procedures excluded under the definition of biometric identifiers.

3. "Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property which shall include, but shall not be limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a personal identification number, a pass code, a driver's license number, or a social security number.

4. "Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity shall not include a state or local government agency or any court in the state, a clerk of the court, or a judge or justice thereof.

5. "Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

§ 676-b. Retention; collection; disclosure; destruction. 1. A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information within a reasonable time, but in no event later than sixty days, after it is no longer necessary to maintain for the permissible purpose or purposes identified in the notice or for which the individual provided valid authorization or within three years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

2. No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(a) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or 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 a

biometric identifier or biometric information is being collected, stored, and used; and

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

3. No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

4. No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(a) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(b) the disclosure or redisclosure 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 federal, state or local law or municipal ordinance; or

(d) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

5. A private entity in possession of a biometric identifier or biometric information shall:

(a) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(b) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

§ 676-c. Regulatory authority and enforcement. 1.(a) The attorney general is authorized and empowered to adopt, promulgate, amend and rescind suitable rules and regulations to carry out the provisions of this article, including rules governing the form and content of any disclosures or communications required by this article.

(b) Whenever it appears to the attorney general, either upon complaint or otherwise, that any person or persons has engaged in or is about to engage in any of the acts or practices stated to be unlawful under this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits obtained directly or indirectly by any such violation, to obtain civil penalties of not more than twenty thousand dollars per violation, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

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

(d) In assessing the amount of penalties, the court must consider anyone or more of the relevant circumstances presented by any of

the parties, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the violator's misconduct, and the violator's financial condition.

2. Any action or special proceeding brought by the attorney general pursuant to this section must be commenced within six years of the date on which the attorney general became aware of the violation.

3. In connection with any proposed action or special proceeding under this section, the attorney general is authorized to take proof and make a determination of the relevant facts, and to issue subpoenas in accordance with the civil practice law and rules. The attorney general may also require such other data and information as the attorney general may deem relevant and may require written responses to questions under oath. Such power of subpoena and examination shall not abate or terminate by reason of any action or special proceeding brought by the attorney general under this article.

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

5.(a) Failure to comply with a subpoena issued pursuant to this section without reasonable cause tolls the applicable statutes of limitations in any action or special proceeding brought by the attorney general against the noncompliant person that arises out of the attorney general's investigation.

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

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

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

§ 676-d. Construction with other laws. 1. Nothing in this article shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

2. Nothing in this article shall be construed to conflict with the federal Health Insurance Portability and Accountability Act of 1996.

3. Nothing in the article shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999.

4. Nothing in this article shall be construed to apply to a contractor, subcontractor, or agent of a state agency of local government when working for that state agency of local government.

§ 676-e. Severability. If any provision of this article, or any application of any provision of this article, is held to be invalid, that shall not affect the validity or effectiveness of any other provision of

this article, or of any other application of any provision of this article, which can be given effect without that provision or application; and to that end, the provisions and applications of this article are severable.

§ 2. This act shall take effect on the ninetieth day after it shall have become a law.