STATE OF NEW YORK

9793

IN ASSEMBLY

February 9, 2018

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

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. Right of action.
676-d. Construction with other laws.

§ 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 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

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

LBD14465-02-8

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 when the initial purpose for collecting or obtaining such identifiers or information has been satisfied 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 redisclsoure 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. Right of action. Any person aggrieved by a violation of this article shall have a right of action in supreme court against an offending party. A prevailing party may recover for each violation:

1. against a private entity that negligently violates a provision of this article, liquidated damages of one thousand dollars or actual damages, whichever is greater;

2. against a private entity that intentionally or recklessly violates a provision of this article, liquidated damages of five thousand dollars or actual damages, whichever is greater;

3. reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

4. other relief, including an injunction, as the court may deem appropriate.

§ 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.

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