HB4686

LRB10338147JRC68280b

103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

HB4686

Introduced 2/6/2024, by Rep. Tim Ozinga

SYNOPSIS AS INTRODUCED:

740 ILCS 14/5
740 ILCS 14/10
740 ILCS 14/15
740 ILCS 14/20
740 ILCS 14/25

Amends the Biometric Information Privacy Act. Changes the term "written release" to "written consent". Provides that the written policy that is developed by a private entity in possession of biometric identifiers shall be made available to the person from whom biometric information is to be collected or was collected (rather than to the public). Provides that an action brought under the Act shall be commenced within one year after the cause of action accrued if, prior to initiating any action against a private entity, the aggrieved person provides a private entity 30 days' written notice identifying the specific provisions the aggrieved person alleges have been or are being violated. Provides that if within the 30 days the private entity actually cures the noticed violation and provides the aggrieved person an express written statement that the violation has been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the private entity. Provides that if a private entity continues to violate the Act in breach of the express written statement, the aggrieved person may initiate an action against the private entity to enforce the written statement and may pursue statutory damages for each breach of the express written statement and any other violation that postdates the written statement. Provides that a prevailing party may recover: against a private entity that negligently violates the Act, actual damages (rather than liquidated damages of $1,000 or actual damages, whichever is greater); or against a private entity that willfully (rather than intentionally or recklessly) violates the Act, actual damages plus liquidated damages up to the amount of actual damages (rather than liquidated damages of $5,000 or actual damages, whichever is greater). Provides that the Act does not apply to a private entity if the private entity's employees are covered by a collective bargaining agreement that provides for different policies regarding the retention, collection, disclosure, and destruction of biometric information. Makes other changes.

LRB103 38147 JRC 68280 b

A BILL FOR

AN ACT concerning civil law.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 5. The Biometric Information Privacy Act is amended by changing Sections 5, 10, 15, 20, and 25 as follows:

(740 ILCS 14/5)

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are wary ~~weary~~ of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do 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 do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act 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 biological materials regulated under the Genetic Information Privacy Act. 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, 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.

"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 does not include information derived from items or procedures excluded under the definition of biometric identifiers<u>, including information derived from biometric information that cannot be used to recreate the original biometric identifier</u>.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not

limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

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

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

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the person from whom biometric information is to be collected or was collected ~~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 3 years of the individual's last interaction with

the private entity, whichever occurs first. Absent a valid order, warrant, or subpoena issued by a court of competent jurisdiction or a local or federal governmental agency, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) 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:

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

(2) 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

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

Written consent may be obtained by electronic means.

(c) 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.

(d) 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:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative provides written consent ~~consents~~ to the disclosure or redisclosure;

(2) 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;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

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

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) 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

(2) 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.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/20)

Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party<u>, which shall be commenced within one year after the cause of action accrued if, prior to initiating any action against a private entity, the aggrieved person provides a private entity 30 days' written notice identifying the specific provisions of this Act the aggrieved person alleges have been or are being violated. If, within the 30 days, the private entity actually cures the noticed violation and provides the aggrieved person an express written statement that the violation has been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the private entity. If a private entity continues to violate this Act in breach of the express written statement provided to the aggrieved person under this Section, the aggrieved person may initiate an action against the</u>

private entity to enforce the written statement and may pursue statutory damages for each breach of the express written statement and any other violation that postdates the written statement. A prevailing party in any such action may recover ~~for each violation~~:

(1) against a private entity that negligently violates a provision of this Act, ~~liquidated damages of $1,000 or~~ actual damages~~, whichever is greater~~;

(2) against a private entity that willfully ~~intentionally or recklessly~~ violates a provision of this Act, actual damages plus liquidated damages up to the amount of actual damages ~~of $5,000 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 State or federal court may deem appropriate.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/25)

Sec. 25. Construction.

(a) Nothing in this Act 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.

(b) Nothing in this Act shall be construed to conflict

with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

(c) Nothing in this Act 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 and the rules promulgated thereunder.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State or federal agency or local unit of government when working for that State or federal agency or local unit of government.

(f) Nothing in this Act shall be construed to apply to a private entity if the private entity's employees are covered by a collective bargaining agreement that provides for different policies regarding the retention, collection, disclosure, and destruction of biometric information.

(Source: P.A. 95-994, eff. 10-3-08.)