# SB0602

LRB10211317LNS16650b

## 102ND GENERAL ASSEMBLY

## State of Illinois

## 2021 and 2022

### SB0602

Introduced 2/24/2021, by Sen. Bill Cunningham

## SYNOPSIS AS INTRODUCED:

740 ILCS 14/10
740 ILCS 14/15
740 ILCS 14/25
740 ILCS 14/35 new

Amends the Biometric Information Privacy Act. Changes the definitions of "biometric identifier" and "written release". Defines "biometric lock", "biometric time clock", "electronic signature", "in writing", and "security purpose". Provides that if the biometric identifier or biometric information is collected or captured for the same repeated process, the private entity is only required to inform the subject or receive consent during the initial collection. Waives certain requirements for collecting, capturing, or otherwise obtaining a person's or a customer's biometric identifier or biometric information under certain circumstances relating to security purposes. Provides that nothing in the Act shall be construed to: conflict with information captured by an alarm system installed by a licensed person; and apply to information captured by a biometric time clock or biometric lock that converts a person's biometric identifier to a mathematical representation. Provides that the Department of Labor shall provide on its website information for employers regarding the requirements of the Act. Effective immediately.

LRB102 11317 LNS 16650 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 10, 15, and 25 and by adding Section 35 as follows:

(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 identifiers do not include information captured and converted to a mathematical representation, including, but not limited to, a numeric string or similar method that cannot be used to recreate the biometric identifier.

"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.

"Biometric lock" means a device that is used to grant access to a person and converts the person's biometric identifier or biometric information to a mathematical representation, including, but not limited to, a numeric string or similar method that cannot be used to recreate the person's biometric identifier.

"Biometric time clock" means a device that is used for time management and converts a person's biometric identifier

or biometric information to a mathematical representation, including, but not limited to, a numeric string or similar method that cannot be used to recreate the person's biometric identifier.

"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.

"Electronic signature" means a signature in electronic form attached to or logically associated with an electronic record.

"In writing" includes, but is not limited to, electronic communications or notices.

"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.

"Security purpose" means for the purpose of preventing retail theft, fraud, or any other misappropriation or theft of a thing of value, including protecting property from trespass,

controlling access to property, or protecting any person from stalking, violence, or harassment, and including assisting a law enforcement investigation.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment. Written release includes electronic communications, and such a release or communication by electronic signature of the employee as provided under Section 5-120 of the Electronic Commerce Security Act.

(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 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 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.

(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 release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(b-5) If the biometric identifier or biometric information is collected or captured for the same repeated process, the private entity is only required to inform the subject or receive consent pursuant paragraphs (1), (2), and (3) of subsection (b) during the initial collection.

(b-10) A private entity may collect, capture, or otherwise obtain a person's or a customer's biometric identifier or biometric information without satisfying the requirements of subsection (b) if:

(1) the private entity collects, captures, or

otherwise obtains a person's or a customer's biometric identifier or biometric information for a security purpose;

(2) the private entity uses the biometric identifier or information only for a security purpose;

(3) the private entity retains the biometric identifier or information no longer than is reasonably necessary to satisfy a security purpose; and

(4) the private entity documents a process and time frame to delete any biometric information used for the purposes identified in this subsection.

(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 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 14/25)

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 or information captured by an alarm system as defined by that Act installed by a person licensed under that Act and the rules adopted thereunder.

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

(f) Nothing in this Act shall be construed to apply to information captured by a biometric time clock or biometric lock that converts a person's biometric identifier to a mathematical representation, including, but not limited to, a numeric string or similar method that cannot be used to recreate the person's biometric identifier.

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

(740 ILCS 14/35 new)

Sec. 35. Department of Labor website. The Department of Labor shall provide on its website information for employers regarding the requirements of this Act.

Section 99. Effective date. This Act takes effect upon becoming law.