



102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

SB0300

Introduced 2/19/2021, by Sen. Jason A. Barickman

SYNOPSIS AS INTRODUCED:

740 ILCS 14/10
740 ILCS 14/15
740 ILCS 14/20
740 ILCS 14/21 new
740 ILCS 14/22 new
740 ILCS 14/25

Amends the Biometric Information Privacy Act. Changes the definitions of "biometric information" and "written consent". Provides that a right of action 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 the Act the aggrieved person alleges have been or are being violated. Provides that if within the 30 days the private entity cures the noticed violation as to the person providing notice and provides the person providing notice an express written statement that the violations have been cured and that no further violations shall occur, no action for damages of any kind may be initiated by the person providing notice 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, as well as any other violation of the Act 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); 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). Add language governing: when certain claims accrue; limitations regarding the collection and use of biometric information to detect or contain the spread of COVID-19; and construction of the Act. Makes other changes.

LRB102 13254 LNS 18598 b

1 AN ACT concerning civil law.

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

4 Section 5. The Biometric Information Privacy Act is
5 amended by changing Sections 10, 15, 20, and 25 and by adding
6 Sections 21 and 22 as follows:

7 (740 ILCS 14/10)

8 Sec. 10. Definitions. In this Act:

9 "Biometric identifier" means a retina or iris scan,
10 fingerprint, voiceprint, or scan of hand or face geometry.
11 Biometric identifiers do not include writing samples, written
12 signatures, photographs, human biological samples used for
13 valid scientific testing or screening, demographic data,
14 tattoo descriptions, or physical descriptions such as height,
15 weight, hair color, or eye color. Biometric identifiers do not
16 include donated organs, tissues, or parts as defined in the
17 Illinois Anatomical Gift Act or blood or serum stored on
18 behalf of recipients or potential recipients of living or
19 cadaveric transplants and obtained or stored by a federally
20 designated organ procurement agency. Biometric identifiers do
21 not include biological materials regulated under the Genetic
22 Information Privacy Act. Biometric identifiers do not include
23 information captured from a patient in a health care setting

1 or information collected, used, or stored for health care
2 treatment, payment, or operations under the federal Health
3 Insurance Portability and Accountability Act of 1996.
4 Biometric identifiers do not include an X-ray, roentgen
5 process, computed tomography, MRI, PET scan, mammography, or
6 other image or film of the human anatomy used to diagnose,
7 prognose, or treat an illness or other medical condition or to
8 further validate scientific testing or screening.

9 "Biometric information" means any information, regardless
10 of how it is captured, converted, stored, or shared, based on
11 an individual's biometric identifier used to identify an
12 individual. Biometric information does not include information
13 derived from items or procedures excluded under the definition
14 of biometric identifiers. Biometric information does not
15 include information that cannot be used to recreate the
16 original biometric identifier.

17 "Confidential and sensitive information" means personal
18 information that can be used to uniquely identify an
19 individual or an individual's account or property. Examples of
20 confidential and sensitive information include, but are not
21 limited to, a genetic marker, genetic testing information, a
22 unique identifier number to locate an account or property, an
23 account number, a PIN number, a pass code, a driver's license
24 number, or a social security number.

25 "Private entity" means any individual, partnership,
26 corporation, limited liability company, association, or other

1 group, however organized. A private entity does not include a
2 State or local governmental ~~government~~ agency. A private
3 entity does not include any court of Illinois, a clerk of the
4 court, or a judge or justice thereof.

5 "Written release" means informed written consent or, in
6 the context of employment, a release executed by an employee
7 as a condition of employment. Written consent includes consent
8 obtained by electronic means.

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

10 (740 ILCS 14/15)

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

12 (a) A private entity in possession of biometric
13 identifiers or biometric information must develop a written
14 policy, made available to the person from whom biometric
15 identifiers or biometric information is to be or was collected
16 ~~public~~, establishing a retention schedule and guidelines for
17 permanently destroying biometric identifiers and biometric
18 information when the initial purpose for collecting or
19 obtaining such identifiers or information has been satisfied
20 or within 3 years of the individual's last interaction with
21 the private entity, whichever occurs first. Absent a valid
22 order, warrant, or subpoena issued by a court of competent
23 jurisdiction or a local, State, or federal governmental
24 agency, or as otherwise required by law, a private entity in
25 possession of biometric identifiers or biometric information

1 must comply with its established retention schedule and
2 destruction guidelines.

3 (b) No private entity may collect, capture, purchase, or
4 receive through trade, ~~or otherwise obtain~~ a person's or a
5 customer's biometric identifier or biometric information,
6 unless it first:

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

11 (2) informs the subject or the subject's legally
12 authorized representative in writing of the specific
13 purpose and length of term for which a biometric
14 identifier or biometric information is being collected,
15 stored, and used; and

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

20 (c) No private entity in possession of a biometric
21 identifier or biometric information may sell, lease, trade, or
22 otherwise profit from a person's or a customer's biometric
23 identifier or biometric information.

24 (d) No private entity in possession of a biometric
25 identifier or biometric information may disclose or ~~r~~
26 redisclose, ~~or otherwise disseminate~~ a person's or a

1 customer's biometric identifier or biometric information
2 unless:

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

7 (2) the disclosure or redisclosure completes a
8 financial transaction requested or authorized by the
9 subject of the biometric identifier or the biometric
10 information or the subject's legally authorized
11 representative;

12 (3) the disclosure or redisclosure is required by
13 local, State, or federal governmental agency, or as
14 otherwise required by law ~~or municipal ordinance~~; or

15 (4) the disclosure is required pursuant to a valid
16 order, warrant, or subpoena issued by a court of competent
17 jurisdiction or a local, State, or federal governmental
18 agency, or as otherwise required by law.

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

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

25 (2) store, transmit, and protect from disclosure all
26 biometric identifiers and biometric information in a

1 manner that is the same as or more protective than the
2 manner in which the private entity stores, transmits, and
3 protects other confidential and sensitive information.

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

5 (740 ILCS 14/20)

6 Sec. 20. Right of action. Any person aggrieved by a
7 violation of this Act shall have a right of action in a State
8 circuit court or as a supplemental claim in federal district
9 court against an offending party that shall be commenced
10 within one year next after the cause of action accrued, if,
11 prior to initiating any action against a private entity, the
12 aggrieved person provides a private entity 30 days' written
13 notice identifying the specific provisions of this Act the
14 aggrieved person alleges have been or are being violated. If
15 within the 30 days the private entity cures the noticed
16 violation as to the person providing notice and provides the
17 person providing notice an express written statement that the
18 violations have been cured and that no further violations
19 shall occur, no action for damages of any kind may be initiated
20 by the person providing notice against the private entity. If
21 a private entity continues to violate this Act in breach of the
22 express written statement provided under this Section, the
23 aggrieved person may initiate an action against the private
24 entity to enforce the written statement and may pursue
25 statutory damages for each breach of the express written

1 statement, as well as any other violation of the Act that
2 postdates the written statement. A prevailing party in any
3 such action may recover ~~for each violation:~~

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

7 (2) against a private entity that willfully
8 ~~intentionally or recklessly~~ violates a provision of this
9 Act, actual damages plus liquidated damages up to the
10 amount of actual damages ~~of \$5,000 or actual damages,~~
11 ~~whichever is greater;~~

12 (3) reasonable attorneys' fees and costs, including
13 expert witness fees and other litigation expenses; and

14 (4) other relief, including an injunction, as the
15 State or federal court may deem appropriate.

16 As used in this Section, "cure" means to provide the
17 disclosures or obtain the consent required by this Act within
18 30 days of the receipt of the written notice described in this
19 Section or to, within that same period, otherwise demonstrate
20 compliance with this Act.

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

22 (740 ILCS 14/21 new)

23 Sec. 21. Accrual. A claim accrues under subsection (b) of
24 Section 15 upon a person's first use of the technology that the
25 person claims collected the person's biometric identifier or

1 biometric information. A claim accrues under subsection (d) of
2 Section 15 upon the first disclosure or redisclosure of the
3 person's biometric identifier or biometric information.

4 (740 ILCS 14/22 new)

5 Sec. 22. COVID-19 limitation. Notwithstanding any
6 provision of this Act, a private entity shall not be subject to
7 any enforcement proceeding or liability under any provision of
8 this Act if the private entity collected, obtained, or
9 retained the biometric identifier or biometric information as
10 part of its efforts to detect or contain the spread of
11 COVID-19.

12 (740 ILCS 14/25)

13 Sec. 25. Construction.

14 (a) Nothing in this Act shall be construed to impact the
15 admission or discovery of biometric identifiers and biometric
16 information in any action of any kind in any court, or before
17 any tribunal, board, agency, or person.

18 (b) Nothing in this Act shall be construed to conflict
19 with the X-Ray Retention Act, the federal Health Insurance
20 Portability and Accountability Act of 1996 and the rules
21 promulgated under either Act.

22 (c) Nothing in this Act shall be deemed to apply in any
23 manner to a financial institution or an affiliate of a
24 financial institution that is subject to Title V of the

1 federal Gramm-Leach-Bliley Act of 1999 and the rules
2 promulgated thereunder.

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

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

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