



101ST GENERAL ASSEMBLY

State of Illinois

2019 and 2020

HB5374

by Rep. Jim Durkin

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 of "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.

LRB101 18682 LNS 68137 b

A BILL FOR

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 amended
5 by changing Sections 5, 10, 15, 20, and 25 as follows:

6 (740 ILCS 14/5)

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

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

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

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

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

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

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

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

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

15 (740 ILCS 14/10)

16 Sec. 10. Definitions. In this Act:

17 "Biometric identifier" means a retina or iris scan,
18 fingerprint, voiceprint, or scan of hand or face geometry.
19 Biometric identifiers do not include writing samples, written
20 signatures, photographs, human biological samples used for
21 valid scientific testing or screening, demographic data,
22 tattoo descriptions, or physical descriptions such as height,
23 weight, hair color, or eye color. Biometric identifiers do not
24 include donated organs, tissues, or parts as defined in the
25 Illinois Anatomical Gift Act or blood or serum stored on behalf

1 of recipients or potential recipients of living or cadaveric
2 transplants and obtained or stored by a federally designated
3 organ procurement agency. Biometric identifiers do not include
4 biological materials regulated under the Genetic Information
5 Privacy Act. Biometric identifiers do not include information
6 captured from a patient in a health care setting or information
7 collected, used, or stored for health care treatment, payment,
8 or operations under the federal Health Insurance Portability
9 and Accountability Act of 1996. Biometric identifiers do not
10 include an X-ray, roentgen process, computed tomography, MRI,
11 PET scan, mammography, or other image or film of the human
12 anatomy used to diagnose, prognose, or treat an illness or
13 other medical condition or to further validate scientific
14 testing or screening.

15 "Biometric information" means any information, regardless
16 of how it is captured, converted, stored, or shared, based on
17 an individual's biometric identifier used to identify an
18 individual. Biometric information does not include information
19 derived from items or procedures excluded under the definition
20 of biometric identifiers, including information derived from
21 biometric information that cannot be used to recreate the
22 original biometric identifier.

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

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

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

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

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

15 (740 ILCS 14/15)

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

17 (a) A private entity in possession of biometric identifiers
18 or biometric information must develop a written policy, made
19 available to the person from whom biometric information is to
20 be collected or was collected ~~public~~, establishing a retention
21 schedule and guidelines for permanently destroying biometric
22 identifiers and biometric information when the initial purpose
23 for collecting or obtaining such identifiers or information has
24 been satisfied or within 3 years of the individual's last
25 interaction with the private entity, whichever occurs first.

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

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

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

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

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

23 Written consent may be obtained by electronic means.

24 (c) No private entity in possession of a biometric
25 identifier or biometric information may sell, lease, trade, or
26 otherwise profit from a person's or a customer's biometric

1 identifier or biometric information.

2 (d) No private entity in possession of a biometric
3 identifier or biometric information may disclose, redisclose,
4 or otherwise disseminate a person's or a customer's biometric
5 identifier or biometric information unless:

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

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

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

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

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

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

26 (2) store, transmit, and protect from disclosure all

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

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

6 (740 ILCS 14/20)

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

1 statutory damages for each breach of the express written
2 statement and any other violation that postdates the written
3 statement. A prevailing party in any such action may recover
4 ~~for each violation:~~

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

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

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

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

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

18 (740 ILCS 14/25)

19 Sec. 25. Construction.

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

24 (b) Nothing in this Act shall be construed to conflict with
25 the X-Ray Retention Act, the federal Health Insurance

1 Portability and Accountability Act of 1996 and the rules
2 promulgated under either Act.

3 (c) Nothing in this Act shall be deemed to apply in any
4 manner to a financial institution or an affiliate of a
5 financial institution that is subject to Title V of the federal
6 Gramm-Leach-Bliley Act of 1999 and the rules promulgated
7 thereunder.

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

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

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

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