



Sen. Bill Cunningham

Filed: 4/6/2018

10000SB3053sam002

LRB100 19520 HEP 38183 a

1 AMENDMENT TO SENATE BILL 3053

2 AMENDMENT NO. \_\_\_\_\_. Amend Senate Bill 3053 by replacing  
3 everything after the enacting clause with the following:

4 "Section 5. The Biometric Information Privacy Act is  
5 amended by changing Sections 10, 15, 20, and 25 and by adding  
6 Section 35 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 that  
11 is linked by a private entity to the subject's confidential and  
12 sensitive information. Biometric identifiers do not include  
13 physical or digital photographs; video recordings; audio  
14 recordings; data generated from physical or digital  
15 photographs, video recordings, or audio recordings; writing  
16 samples; ~~7~~ written signatures; ~~7~~ photographs; human biological

1 samples used for valid scientific testing or screening;IT  
2 demographic data;IT tattoo descriptions;IT or physical  
3 descriptions such as height, weight, hair color, or eye color.  
4 Biometric identifiers do not include donated organs, tissues,  
5 or parts as defined in the Illinois Anatomical Gift Act or  
6 blood or serum stored on behalf of recipients or potential  
7 recipients of living or cadaveric transplants and obtained or  
8 stored by a federally designated organ procurement agency.  
9 Biometric identifiers do not include biological materials  
10 regulated under the Genetic Information Privacy Act. Biometric  
11 identifiers do not include information captured from a patient  
12 in a health care setting or information collected, used, or  
13 stored for health care treatment, payment, or operations under  
14 the federal Health Insurance Portability and Accountability  
15 Act of 1996. Biometric identifiers do not include an X-ray,  
16 roentgen process, computed tomography, MRI, PET scan,  
17 mammography, or other image or film of the human anatomy used  
18 to diagnose, prognose, or treat an illness or other medical  
19 condition or to further validate scientific testing or  
20 screening.

21 "Biometric information" means any information, regardless  
22 of how it is captured, converted, stored, or shared, based on  
23 an individual's biometric identifier that is linked by a  
24 private entity to the subject's confidential and sensitive  
25 information ~~used to identify an individual~~. Biometric  
26 information does not include information derived from items or

1 procedures excluded under the definition of biometric  
2 identifiers.

3 "Confidential and sensitive information" means personal  
4 information that can be used to uniquely identify an individual  
5 or an individual's account or property. Examples of  
6 confidential and sensitive information include, but are not  
7 limited to, a genetic marker, genetic testing information, a  
8 unique identifier number to locate an account or property, an  
9 account number, a PIN number, a pass code, a driver's license  
10 number, or a social security number.

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

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

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

21 (740 ILCS 14/15)

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

23 (a) A private entity in possession of biometric identifiers  
24 or biometric information for more than 24 hours must develop a  
25 written policy, made available to the public, establishing a

1 retention schedule and guidelines for permanently destroying  
2 biometric identifiers and biometric information when the  
3 initial purpose for collecting or obtaining such identifiers or  
4 information has been satisfied or within 3 years of the  
5 individual's last interaction with the private entity,  
6 whichever occurs first. Absent a valid warrant or subpoena  
7 issued by a court of competent jurisdiction, a private entity  
8 in possession of biometric identifiers or biometric  
9 information must comply with its established retention  
10 schedule and destruction guidelines.

11 (b) No private entity may collect, capture, purchase,  
12 receive through trade, or otherwise obtain a person's or a  
13 customer's biometric identifier or biometric information and  
14 retain it for more than 24 hours, unless it first:

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

19 (2) informs the subject or the subject's legally  
20 authorized representative in writing of the specific  
21 purpose and length of term for which a biometric identifier  
22 or biometric information is being collected, stored, and  
23 used; and

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

1 (c) No private entity in possession of a biometric  
2 identifier or biometric information may sell, lease, trade, or  
3 otherwise exchange for financial consideration ~~profit from~~ a  
4 person's or a customer's biometric identifier or biometric  
5 information.

6 (d) No private entity in possession of a biometric  
7 identifier or biometric information may disclose, redisclose,  
8 or otherwise disseminate a person's or a customer's biometric  
9 identifier or biometric information unless:

10 (1) the subject of the biometric identifier or  
11 biometric information or the subject's legally authorized  
12 representative consents to the disclosure or redisclosure;

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

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

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

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

25 (1) store, transmit, and protect from disclosure all  
26 biometric identifiers and biometric information using the

1 reasonable standard of care within the private entity's  
2 industry; and

3 (2) store, transmit, and protect from disclosure all  
4 biometric identifiers and biometric information in a  
5 manner that is the same as or more protective than the  
6 manner in which the private entity stores, transmits, and  
7 protects other confidential and sensitive information.

8 (f) It is not unlawful under this Act for any user to  
9 collect, capture, otherwise obtain, or possess a biometric  
10 identifier or biometric information on a personal device,  
11 unless the biometric identifier or biometric information is  
12 used for the purpose of committing a criminal or tortious act.  
13 It is not unlawful under this Act for a private entity to  
14 create or make available a device, software, or other  
15 functionality that collects, captures, otherwise obtains, or  
16 possesses biometric identifiers or biometric information on a  
17 personal device. It is not unlawful under this Act for a cloud  
18 service provider to take any action at the direction of or on  
19 behalf of a user of the cloud service.

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

21 (740 ILCS 14/20)

22 Sec. 20. Right of action. Any person aggrieved by a  
23 violation of this Act that occurs in this State shall have a  
24 right of action in a State circuit court or as a supplemental  
25 claim in federal district court against an offending party. A

1 prevailing party may recover for each violation:

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

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

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

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

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

13 (740 ILCS 14/25)

14 Sec. 25. Construction.

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

19 (b) Nothing in this Act shall be deemed to apply in any  
20 manner to a private entity that complies ~~construed to conflict~~  
21 with the X-Ray Retention Act, the federal Health Insurance  
22 Portability and Accountability Act of 1996 as amended by the  
23 Health Information Technology for Economic and Clinical Health  
24 Act of 2009, the Personal Information Protection Act, and the  
25 rules promulgated under those Acts ~~either Act.~~

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

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

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

14 (f) Nothing in this Act shall be deemed to apply to a  
15 private entity collecting, storing, or transmitting biometric  
16 information if:

17 (1) the biometric information is used exclusively for:

18 (A) employment, human resources, compliance,  
19 identification, or authentication purposes;

20 (B) preventing or investigating acts of terrorism,  
21 human trafficking, kidnapping, or violence; or

22 (C) safety, security, or fraud prevention  
23 purposes;

24 (2) the private entity does not sell, lease, or trade  
25 the biometric identifier or biometric information  
26 collected; and



1           (3) the private entity documents a process and time  
2           frame to delete any biometric information used for the  
3           purposes identified in paragraph (1).

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

5           (740 ILCS 14/35 new)

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