



Sen. Terry Link

**Filed: 4/11/2008**

09500SB2400sam004

LRB095 19768 RPM 49426 a

1 AMENDMENT TO SENATE BILL 2400

2 AMENDMENT NO. \_\_\_\_\_. Amend Senate Bill 2400, AS AMENDED,  
3 by replacing everything after the enacting clause with the  
4 following:

5 "Section 1. Short title. This Act may be cited as the  
6 Biometric Information Privacy Act.

7 Section 5. Legislative findings; intent. The General  
8 Assembly 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 "Pay By Touch" at banks, grocery  
16 stores, gas stations, and school cafeterias.

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

8 (d) An overwhelming majority of members of the public are  
9 opposed to the use of biometrics when such information is tied  
10 to personal finances and other personal information.

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

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

19 Section 10. Definitions. In this Act:

20 "Biometric identifier" means any indelible personal  
21 physical characteristic which can be used to uniquely identify  
22 an individual or pinpoint an individual at a particular place  
23 at a particular time. Examples of biometric identifiers  
24 include, but are not limited to iris or retinal scans,  
25 fingerprints, voiceprints, and records or scans of hand

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

22 "Biometric information" means any information, regardless  
23 of how it is captured, converted, stored, or shared, based on  
24 an individual's biometric identifier used to identify an  
25 individual. Biometric information does not include information  
26 derived from items or procedures excluded under the definition

1 of biometric identifiers. Biometric information does not  
2 include information captured from a patient in a health care  
3 setting or information collected, used, or stored for health  
4 care treatment, payment, or operations under the federal Health  
5 Insurance Portability and Accountability Act of 1996.

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

14 "Legally effective written release" means informed written  
15 consent or a release executed by an employee as a condition of  
16 employment.

17 "Private entity" means any individual, partnership,  
18 corporation, limited liability company, association, or other  
19 group, however organized. A private entity does not include a  
20 public agency. A private entity does not include any court of  
21 Illinois, a clerk of the court, or a judge or justice thereof.

22 "Public agency" means the State of Illinois and its various  
23 subdivisions and agencies, and all units of local government,  
24 school districts, and other governmental entities. A public  
25 agency does not include any court of Illinois, a clerk of the  
26 court, or a judge or justice thereof.

1           Section 15. Retention; collection; disclosure;  
2           destruction.

3           (a) A public agency or private entity in possession of  
4           biometric identifiers or biometric information must develop a  
5           written policy, made available to the public, establishing a  
6           retention schedule and guidelines for permanently destroying  
7           biometric identifiers and biometric information when the  
8           initial purpose for collecting or obtaining such identifiers or  
9           information has been satisfied or within 3 years of the  
10          individual's last interaction with the public agency or private  
11          entity, whichever occurs first. Absent a valid warrant or  
12          subpoena issued by a court of competent jurisdiction, a public  
13          agency or private entity in possession of biometric identifiers  
14          or biometric information must comply with its established  
15          retention schedule and destruction guidelines.

16          (b) No public agency or private entity may collect,  
17          capture, purchase, receive through trade, or otherwise obtain a  
18          person's or a customer's biometric identifier or biometric  
19          information, unless it first:

20                 (1) informs the subject in writing that a biometric  
21                 identifier or biometric information is being collected or  
22                 stored;

23                 (2) informs the subject in writing of the specific  
24                 purpose and length of term for which a biometric identifier  
25                 or biometric information is being collected, stored, and

1 used; and

2 (3) receives a legally effective written release  
3 executed by the subject of the biometric identifier or  
4 biometric information or the subject's legally authorized  
5 representative.

6 (c) Subsections (a) and (b) of this Section do not apply to  
7 a public agency:

8 (1) engaged in criminal investigations, arrests,  
9 prosecutions, or law enforcement;

10 (2) overseeing pretrial detention, post-trial  
11 commitment, corrections or incarceration, civil  
12 commitment, probation services, or parole services;

13 (3) serving as the State central repository of  
14 biometrics for criminal identification and investigation  
15 purposes;

16 (4) furnishing biometric identifiers or biometric  
17 information to a State or federal repository of biometrics  
18 pursuant to State or federal law or municipal ordinance;

19 (5) receiving biometric identifiers or biometric  
20 information pursuant to State or federal law or municipal  
21 ordinance;

22 (6) acting pursuant to a valid warrant or subpoena  
23 issued by a court of competent jurisdiction;

24 (7) issuing driver's licenses, driver's permits,  
25 identification cards issued pursuant to the Illinois  
26 Identification Card Act, or occupational licenses; or

1           (8) performing employee background checks in  
2           accordance with the public agency's hiring policies or  
3           statutory obligations.

4           Nothing in subsections (a) and (b) of this Section shall be  
5           construed to conflict with the retention and collection  
6           practices for fingerprints, other biometric identifiers, or  
7           biometric information under the Criminal Identification Act,  
8           the Illinois Uniform Conviction Information Act, or the federal  
9           National Crime Prevention and Privacy Compact. Subsection (a)  
10          of this Section does not apply to school districts; however, a  
11          school district that collects biometric identifiers or  
12          biometric information must adopt retention schedules and  
13          destruction policies in accordance with the School Code.  
14          Subsection (a) of this Section does not apply to a fingerprint  
15          vendor or fingerprint vendor agency; however, a fingerprint  
16          vendor or fingerprint vendor agency must adopt retention  
17          schedules and destruction polices in accordance with the  
18          Private Detective, Private Alarm, Private Security,  
19          Fingerprint Vendor, and Locksmith Act of 2004.

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

24          (e) No public agency or private entity in possession of a  
25          biometric identifier or biometric information may disclose,  
26          redisclose, or otherwise disseminate a person's or a customer's

1 biometric identifier or biometric information unless:

2 (1) the subject of the biometric identifier or  
3 biometric information or the subject's legally-authorized  
4 representative consents to the disclosure or redisclosure;

5 (2) the disclosure or redisclosure completes a  
6 financial transaction requested or authorized by the  
7 subject of the biometric identifier or the biometric  
8 information;

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

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

14 (f) Nothing in subsections (d) or (e) of this Section shall  
15 be construed to prohibit or inhibit a public agency (i) engaged  
16 in criminal investigations, arrests, prosecutions, or law  
17 enforcement, (ii) overseeing pretrial detention, post-trial  
18 commitment, corrections or incarceration, civil commitment,  
19 probation services, or parole services, (iii) serving as the  
20 State central repository of biometrics for criminal  
21 identification and investigation purposes, (iv) furnishing  
22 biometric identifiers or biometric information to a State or  
23 federal repository of biometrics pursuant to State or federal  
24 law, or (v) issuing driver's licenses, driver's permits, or  
25 identification cards pursuant to the Illinois Identification  
26 Card Act from:



1           (1) sharing biometric identifiers or biometric  
2 information with another public agency engaged in criminal  
3 investigations, arrests, prosecutions, or law enforcement  
4 to further such criminal investigations, arrests,  
5 prosecutions, or law enforcement;

6           (2) sharing biometric identifiers or biometric or  
7 biometric information with another public agency  
8 overseeing pretrial detention, post-trial commitment,  
9 corrections or incarceration, civil commitment, probation  
10 services, or parole services;

11           (3) sharing biometric identifiers or biometric  
12 information pursuant to, or required by, State or federal  
13 law; or

14           (4) sharing biometric identifiers or biometric  
15 information pursuant to a valid warrant or subpoena issued  
16 by a court of competent jurisdiction.

17           (g) Nothing in subsections (d) or (e) of this Section shall  
18 be construed to conflict with the reporting and sharing  
19 practices for fingerprints, other biometric identifiers, or  
20 biometric information under the Criminal Identification Act,  
21 the Illinois Uniform Conviction Information Act, and the  
22 federal National Crime Prevention and Privacy Compact. Nothing  
23 in subsection (d) of this Section shall be construed to  
24 conflict with the reporting and sharing practices of a  
25 fingerprint vendor or fingerprint vendor agency under the  
26 Private Detective, Private Alarm, Private Security,

1 Fingerprint Vendor, and Locksmith Act of 2004.

2 (h) Nothing in subsections (d) or (e) of this Section shall  
3 be construed to prohibit or inhibit a public agency that issues  
4 occupational licenses from:

5 (1) sharing biometric identifiers or biometric  
6 information pursuant to or when required by State or  
7 federal law; or

8 (2) sharing biometric identifiers or biometric  
9 information pursuant to a valid warrant or subpoena issued  
10 by a court of competent jurisdiction.

11 (i) Nothing in subsections (d) or (e) of this Section shall  
12 be construed to prohibit a public agency from performing  
13 employee background checks in accordance with the public  
14 agency's hiring policies or statutory obligations.

15 (j) A public agency in possession of biometric identifiers  
16 or biometric information shall store, transmit, and protect  
17 from disclosure all biometric identifiers and biometric  
18 information in a reasonable manner that is the same as or more  
19 protective than the manner in which the public agency stores,  
20 transmits, and protects other similar confidential and  
21 sensitive information specific to that public agency. The  
22 storage, transmittal, and protection from disclosure standards  
23 under this subsection (j) are solely the choice of the public  
24 agency to adopt in accordance with this Act, other applicable  
25 State or federal law, evolving advances in technology, budget  
26 constraints, and comparable practices specific to that public

1 agency.

2 (k) A private entity in possession of a biometric  
3 identifier or biometric information shall:

4 (1) store, transmit, and protect from disclosure all  
5 biometric identifiers and biometric information using the  
6 reasonable standard of care within the private entity's  
7 industry; and

8 (2) store, transmit, and protect from disclosure all  
9 biometric identifiers and biometric information in a  
10 manner that is the same as or more protective than the  
11 manner in which the private entity stores, transmits, and  
12 protects other confidential and sensitive information.

13 (l) All information and records held by a public agency  
14 pertaining to biometric identifiers and biometric information  
15 shall be confidential and exempt from copying and inspection  
16 under the Freedom of Information Act to all except to the  
17 subject of the biometric identifier or biometric information.  
18 The subject of the biometric identifier or biometric  
19 information held by a public agency shall be permitted to copy  
20 and inspect only their own biometric identifiers and biometric  
21 information.

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

1 recover for each violation:

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

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

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

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

13 Section 25. Construction. Nothing in this Act shall be  
14 construed to impact the admission or discovery of biometric  
15 identifiers and biometric information in any action of any kind  
16 in any court, or before any tribunal, board, agency, or person.  
17 Nothing in this Act shall be construed to conflict with the  
18 X-Ray Retention Act or the federal Health Insurance Portability  
19 and Accountability Act of 1996. Subcontractors or agents of a  
20 public agency must comply with this Act to the extent and  
21 manner this Act applies to that public agency.

22 Section 30. Home rule. Any home rule unit of local  
23 government, any non home rule municipality, or any non home  
24 rule county within the unincorporated territory of the county

1 may enact ordinances, standards, rules, or regulations that  
2 protect biometric identifiers and biometric information in a  
3 manner or to an extent equal to or greater than the protection  
4 provided in this Act. This Section is a limitation on the  
5 concurrent exercise of home rule power under subsection (i) of  
6 Section 6 of Article VII of the Illinois Constitution.

7 Section 95. Applicability. This Act applies to private  
8 entities beginning on the effective date of this Act. This Act  
9 applies to public agencies beginning on January 1, 2011.

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