ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

April 10, 2018

BY EMAIL

Sen. Bill Cunningham
Illinois State Senate
bill@billcunningham.com

Re: S.B. 3053 (reduction of biometric privacy) – OPPOSE

Dear Sen. Cunningham:

I write on behalf of the Electronic Frontier Foundation (EFF) and our Illinois members to respectfully oppose S.B. 3053, including Senate Amendments #1 and #2, which were filed on April 6. This bill would create broad new exemptions from the critical protections now provided by the Illinois Biometric Information Privacy Act (BIPA) of 2008. *See* 740 ILCS 14/1.

Big businesses would have new powers to harvest and aggregate Illinoisans' biometric information, without their consent or knowledge. Businesses could monetize this biometric information as they see fit. They might even sell it to law enforcement agencies and federal immigration officials.

Given the growing public outrage over how Facebook and Cambridge Analytica handled sensitive user data, this is the wrong time to reduce privacy protections.[1]

EFF is a non-profit civil liberties organization that has worked for more than 25 years to protect privacy from emerging technologies. EFF has more than 44,000 dues-paying members from across the country.

I. Why Illinois needs BIPA

EFF strongly supports the current Illinois BIPA. This statute's findings explain how biometrics surveillance is a grave menace to privacy:

[1] *See, e.g.*, *Zuckerberg Faces a Skeptical Congress*, N.Y. Times (April 10, 2018).

> The use of biometrics is growing in the business and security screening sectors … Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, [and] is at heightened risk for identity theft … An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information. The full ramifications of biometric technology are not fully known.

See 740 ILCS 14/5.

There are many additional reasons to limit how big businesses harvests and monetizes our biometric information.

First, our biometric identifiers, unlike other unique identifiers, are readily accessible to other people. Wherever we go, for example, we show our faces, shed our DNA, and leave our fingerprints. There is very little that we can do to stop other people from gathering this information from us.

Our faces are especially easy to capture—remotely, secretly, cheaply, and automatically. Rapidly changing technologies aggravate the problem. New cameras can capture our face images at ever greater distances and with ever higher precision. New computer programs can match our face images with ever greater accuracy. New interoperability allows this face matching across ever more databases.[2]

Second, data thieves will try to steal the biometric databases constructed by big businesses. In 2015, data thieves stole biometric information about millions of people from the U.S. Office of Personnel Management.[3] In 2017, data thieves stole sensitive data about 140 million people from Equifax.[4]

[2] https://www.eff.org/document/testimony-jennifer-lynch-senate-committee-judiciary-subcommittee-privacy-technology-and-law.

[3] https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[4] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

India’s national biometric database has suffered multiple breaches, most recently in January, when the entire repository was reportedly available for purchase online for $10.[5]

Third, businesses may monetize their biometric databases by selling them to law enforcement and immigration enforcement officials. The FBI regularly enlarges the massive scope of its fingerprint database.[6] Police across the country purchase myriad kinds of personal information from data aggregators. The U.S. Department of Homeland Security (DHS) gathers biometrics from international travelers.[7] DHS also purchases all manner of personal information from data aggregators, for purposes of locating and deporting undocumented immigrants.[8]

As with many aspects of our nation’s troubled criminal justice and immigration enforcement systems, placing a new set of highly sensitive personal information in the hands of the government may have a disparate impact against racial, ethnic, and religious minorities.

II. How BIPA protects biometric privacy

The Illinois BIPA generally requires private entities to obtain consent from a person before collecting or disclosing their biometric identifiers. 740 ILCS 14/15(b) & (d). It also requires private entities that possess such identifiers to destroy them upon the satisfaction of the purpose for collection, and in no event more than three years after the entity’s last interaction with the subject. *Id.* at /15(a). Further, private entities must securely store such identifiers. *Id.* at /15(e). Parties injured by violation of these rules may bring a private cause of action. *Id.* at /20.

[5] https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system.

[6] https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.

[7] https://www.eff.org/deeplinks/2017/08/end-biometric-border-screening.

[8] https://www.dailydot.com/layer8/ice-outsource-data-collection/; https://www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service.

In other words, BIPA leaves private businesses free to gather, store, use, and share biometric information—so long as they first obtain consent. This places the decision where it should be: with each individual, to decide for themselves whether it is in their interests to share their biometrics with others. Each individual likewise should get to decide how their biometric information is used, how long it is stored, and with whom it can be shared.

III. S.B. 3053, Senate Amendment #2

EFF strongly opposes Senate Amendments #2 to S.B. 3053, which was filed on April 6.[9] It would strip Illinoisans of necessary protection of their biometric privacy.[10]

A. Exempting biometrics not linked to confidential information

S.B. 3053 would amend BIPA's definitions of "biometric identifiers" and "biometric information," so they only apply if a private entity "links" biometrics "to the subject's confidential and sensitive information." *See* 740 ILCS 14/10 (amended).

This would exempt from BIPA any private entity that harvests biometrics, but does not link them to confidential information. This would include for-profit businesses that harvest our biometrics, without our knowledge or consent, and link our biometrics to information about us that is not "confidential," such as our names.

B. Exempting face recognition

The existing BIPA defines "biometric identifier" to include "scan of . . . face geometry," and to not include "photographs." *See* 740 ILCS 14/10. Courts

[9] http://ilga.gov/legislation/fulltext.asp?DocName=10000SB3053sam002&GA=100&SessionId=91&DocTypeId=SB&LegID=110583&DocNum=3053&GAID=14&Session=

[10] EFF also strongly opposes the original version of this bill. On February 28, EFF sent an opposition letter to you and the other members of the Illinois Senate Telecommunications and Information Technology Committee.

have interpreted this language to mean that face recognition technologies are subject to the limits of BIPA.[11]

S.B. 3053 would amend the definition of "biometric identifier" to exclude "physical or digital photographs," and "data generated from" them. *See* 740 ILCS 14/10 (amended). This likely would exclude face recognition technologies from BIPA. Yet as discussed above, face recognition is among the most intrusive forms of biometric surveillance.

C. Exempting biometric harvesting that lasts less than 24 hours

The existing BIPA bars private entities from collecting biometrics absent informed consent. *See* 740 ILCS 14/15(b). It also bars private entities from possessing biometrics absent a retention policy, under which destruction must occur when the purpose of collection has been satisfied, and in no event longer than three years after the possessor's last interaction with the individual. *See* 740 ILCS 14/15(a).

S.B. 3053 would amend these two critical rules to exempt private entities that retain biometrics for less than 24 hours. *See* 740 ILCS 14/15 (amended).

But such businesses should be covered by BIPA. For example, some stores use biometrics for fraud prevention: they photograph their incoming patrons, use face recognition technology to compare them to databases of suspect photos, and target apparent matches for anti-shoplifting precautions.[12] Such use of biometric technology does not require retention of biometric information for more than 24 hours.

BIPA now properly extends to such fraud prevention biometrics, and should not be amended to exempt such practices. First, people should be able go to the market without being subjected to non-consensual biometric surveillance. Second, face recognition yields a significant number of false positives, especially for people of color. Third, given the many continuing

[11] *See, e.g., Rivera v. Google Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846 (N.D. Ill. 2017).

[12] *See, e.g.,* https://www.facefirst.com/industry/retail-face-recognition/.

inequities in our criminal justice system, such programs are likely to lead new unfair racial disparities in our market places.

D. Exempting businesses that comply with three privacy statutes

S.B. 3053 would amend BIPA to exempt private entities that comply with three privacy statutes: the federal HIPAA, the Illinois data breach statute (known as the Personal Information Protection Act), and the X-Ray Retention Act. *See* 740 ILCS 14/25 (amended).

A vast number of corporations comply with these three privacy statutes, and thus, under S.B. 3053, would become exempt from BIPA. Yet nothing in these three privacy statutes requires for-profit corporations to obtain informed consent before harvesting and monetizing the biometrics of customers and even total strangers.

E. Exempting biometrics used by employers about employees

S.B. 3053 would exempt private entities that collect, store, and transmit biometrics exclusively for "employment [and] human resources" purposes. *See* 740 ILCS 14/25(f)(1)(A) (new).

This new exemption is not appropriate. Some employers gather biometric information from their employees. Employers may require this sensitive information, for example, to "punch in" to work on a time clock, to access secure locations, or for employee wellness programs. Employees have a strong interest in deciding whether to consent to such use of their biometrics, to limit any new uses of their previously collected biometrics, and to ensure that their employers securely store this information. Illinois should not diminish the biometric privacy of its workers, and shift control over sensitive employee biometrics to the unilateral power of employers.

The bill places two limits on this employer exemption, but neither makes up for the lost protections. Specifically, employers taking advantage of this exemption must not sell biometrics, and must have a deletion process. *See* 740 ILCS 14/25(f)(2) & (3) (new). But this is no substitute for opt-in consent, control over new uses, and secure storage.

F. Exempting biometrics used for fraud protection

S.B. 3053 would exempt private entities that collect, store, and transmit biometrics exclusively for "fraud prevention purposes." *See* 740 ILCS 14/25(f)(1)(C) (new). But as discussed above, BIPA should apply to businesses that uses fraud prevention biometrics to screen their customers.

IV. S.B. 3053, Senate Amendment #1

EFF also opposes, and urges you to withdraw, Senate Amendment #1 to S.B. 3053.[13] It contains the same improper exemptions, discussed above, for (a) businesses that comply with certain privacy statutes, (b) businesses that use biometrics for employment and human resources purposes, and (c) businesses that use biometrics for fraud prevention purposes.

[13] http://ilga.gov/legislation/fulltext.asp?DocName=10000SB3053sam001&GA=100&SessionId=91&DocTypeId=SB&LegID=110583&DocNum=3053&GAID=14&Session=

* * *

Thank you for considering EFF’s opposition to S.B. 3053, including both Senate Amendments. This bill would undermine the Illinois Biometric Information Privacy Act, and thus greatly diminish the biometric privacy of all Illinoisans. If you have any questions, please do not hesitate to email me at adam@eff.org, or to call me at (415) 436-9333, extension 176.

Sincerely,

Adam Schwartz
Senior Staff Attorney

cc: Senate President John Cullerton (msimmons@senatedem.ilga.gov)
Senate Minority Leader William Brady
(billbrady@senatorbillbrady.com)
Sen. Pamela J. Althoff (pamela@pamelaalthoff.net)
Sen. Omar Aquino (info@senatoraquino.com)
Sen. Cristina Castro (chayes@senatedem.ilga.gov)
Sen. Michael Connelly (senatorconnelly21@gmail.com)
Sen. Thomas Cullerton (nbenner@senatedem.ilga.gov)
Sen. Napoleon Harris, III (harris@senatedem.illinois.gov)
Sen. Linda Holmes (senatorholmes42@gmail.com)
Sen. Emil Jones, III (ejones3@senatedem.ilga.gov)
Sen. John G. Mulroe (senatorjohnmulroe@att.net)
Sen. Antonio Muñoz (senator.amunoz@yahoo.com)
Sen. Tom Rooney (senatortomrooney@gmail.com)
Sen. Paul Schimpf (senschimpf58@gmail.com)
Sen. Elgie R. Sims, Jr. (esims@senatorelgiesims.com)
Sen. Steve Stadelman (rfair@senatedem.ilga.gov)
Sen. Dave Syverson (info@senatordavesyverson.com)
Sen. Jil Tracy (senatortracy@adams.net)
Sen. Chuck Weaver (chuck@senweaver.com)