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

February 28, 2018

BY EMAIL

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

Rep. André Thapedi
Illinois State House
illinois32district@gmail.com

Re: SB 3053 and HB 5103 (reduction of biometric privacy) – OPPOSE

Dear Sen. Cunningham and Rep. Thapedi:

I write on behalf of the Electronic Frontier Foundation (EFF) and our Illinois members to respectfully oppose SB 3053 and HB 5103. These two bills 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. These exceptions would greatly diminish BIPA, and strip Illinoisans of necessary protection of their biometric privacy.

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

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:

> 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 business 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 facial images at ever greater distances and with ever higher precision. New computer programs can match our facial images with ever greater accuracy. New interoperability allows this facial matching across ever more databases.[1]

Second, data thieves will try to steal the biometric databases constructed by big business. In 2015, data thieves stole biometric information about millions of people from the U.S. Office of Personnel Management.[2] In 2017, data thieves stole sensitive information about 140 million people from Equifax.[3]

---

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

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

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

Third, companies 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.[4] 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.[5] DHS also purchases all manner of personal information from data aggregators, for purposes of locating and deporting undocumented immigrants.[6]

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 of the identifiers. *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.

In other words, BIPA leaves private companies 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 biometric information 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.

---

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

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

[6] 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.

III. SB 3053 and HB 5103 would undermine BIPA.

SB 3053 and HB 5103 would add the following broad new exceptions to BIPA:

> Nothing in this Act shall be deemed to apply to a private entity collecting, storing, or transmitting biometric information if: (i) the biometric information is used exclusively for employment, human resources, fraud prevention, or security purposes; (ii) the private entity does not sell, lease, trade, or similarly profit from the biometric identifier or biometric information collected; or (iii) the private entity stores, transmits, and protects the biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

Each of these proposed new exceptions is unwarranted. Together, they would greatly undermine BIPA.

Employment, human resources, and security

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.

Fraud prevention

Some stores use biometrics for fraud prevention. For example, they photograph their incoming patrons, use facial recognition technology to compare them to photos in mugshot databases, and target apparent matches for anti-shoplifting precautions.

BIPA properly prohibits this practice, and should not be amended to allow this practice. First, people should be able go to the market to buy necessaries without being subjected to biometric surveillance. Second, facial recognition yields a significant number of false positives, especially for people of color. Third, past arrest is a poor indicator of present criminal intent. Fourth, given the many continuing inequities in our criminal justice system, such programs are likely to lead new unfair racial disparities in our market places.

Biometric surveillance without sale, lease, trade, or "similar profit"

There are many ways that big business might make money on biometrics without selling, leasing, trading, or "similarly profiting" from it. For example, a company might gather biometric information from people they have no previous business connection to, publish that biometric information for free on their website, thereby attract visitors to their website, and then monetize those visits through paid advertising. People should enjoy their current rights under BIPA to avoid such unconsented biometric harvesting and disclosure.

Biometric surveillance by entities with any amount of data security

The bills would exempt every private entity that "protects" the biometric information it harvests, aggregates, and monetizes in "the same" manner that it protects "other confidential and sensitive information." This is the broadest of the proposed new exceptions. Arguably, this exception would be so easy to satisfy that it would effectively repeal BIPA.

Biometric harvesters would not need to meet any objective standard of data protection. Rather, they would only need to protect biometric information as well as they protect other sensitive information. This might be a dangerously low level of protection. For example, the bills would exempt a business from BIPA if it used the password "1234," and no other data security protocol, to protect both its legal department email and its biometric database. After crossing this minimal threshold, the business would be free to capture biometric information from massive numbers of people, insecurely store it, sell it at a profit, and never get anyone's consent, or even notify them.

Notably, compared to these bills, BIPA already imposes a higher secure storage duty on the businesses that amass biometrics: "the reasonable standard of care within the private entity's industry." 740 ILCS 14/15(e)

* * *

Thank you for considering EFF's opposition to SB 3053 and HB 5103. These bills 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)
Speaker Michael Madigan (info@madiganforus.com)
House Minority Leader Jim Durkin (repdurkin@hotmail.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)