

February 7, 2023

The Honorable Melony Griffith, Chair  
Senate Finance Committee  
Maryland General Assembly  
3 East  
Miller Senate Office Building  
Annapolis, MD 21401

Dear Chair Griffith and Members of the Committee:

EPIC writes in support of SB169/ HB33 regarding biometric identifiers and biometric information privacy. Biometric data is highly sensitive. A person's biometric data is linked to that person's dignity, autonomy, safety, and identity.<sup>1</sup> Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. SB169 would protect Marylanders by requiring that the use and retention of biometric data is minimized and that data is kept secure.

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.<sup>2</sup> EPIC has long advocated for strict limits on the collection and use of biometric data.<sup>3</sup>

Late last year, the owner of Madison Square Garden and Radio City Music Hall began using facial recognition to deny all lawyers working for law firms engaged in litigation against MSG access to concerts and sporting events.<sup>4</sup> Radio City Music Hall refused entry to the chaperone of a Girl Scout troop going to see the annual "Christmas Spectacular" show because of who she works for. Facial recognition makes it possible to gate entry to otherwise public spaces. Despite public outcry, MSG owner James Dolan recently "doubled down" on using facial recognition to exclude his personal enemies.<sup>5</sup> A business owner could just as easily use facial recognition deny services to

---

<sup>1</sup> Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

<sup>2</sup> EPIC, *About EPIC*, <https://epic.org/epic/about.html>.

<sup>3</sup> See e.g. Brief for EPIC as Amici Curiae, *Patel v. Facebook.*, 932 F.3d 1264 (9th Cir. 2019), <https://epic.org/amicus/bipa/patel-v-facebook/>;

Brief for EPIC as Amici Curiae, *Rosenbach v. Six Flags Entm't Corp.*, 2017 Ill. App. 2d 170317 (Ill. 2019), <https://epic.org/amicus/bipa/rosenbach/>; Comments of EPIC to the Dept. of Homeland Security, *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 F.R. 56338, 4 (Oct. 13, 2020), <https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf>.

<sup>4</sup> Kashmir Hill and Cory Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. Times (Jan. 3, 2023), <https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html>.

<sup>5</sup> Aaron McDade, *James Dolan defends use of facial-recognition technology to ban entry into Madison Square Garden and Radio City Music Hall*, Insider (Jan. 28, 2023), <https://www.businessinsider.com/james-dolan-stands-behind-msg-facial-recognition-ban-entry-2023-1?op=1>.

members of this Committee who voted against the owner's interests. A biometric privacy bill like SB169 would prevent this and many other harms.

SB169 is modeled after the Illinois Biometric Information Privacy Act (BIPA).<sup>6</sup> Passed in 2008, BIPA has been referred to as one of the most effective and important privacy laws in America.<sup>7</sup> BIPA and SB169 set out a simple privacy framework: businesses may not sell, lease, trade, or otherwise profit from a person's biometric information; businesses must comply with specific retention and deletion guidelines; and companies must use a reasonable standard of care in transmitting, storing, and protecting biometric information that is as protective or more protective than the company uses for other confidential and sensitive information.

BIPA and SB169 also include a requirement that a business obtains informed, written consent before collecting or otherwise obtaining a person's biometric information. Though "notice-and-choice" regimes are not sufficient to protect privacy, the consent provision has proven to be effective in Illinois because it is easy to enforce. It is much easier for an individual to discover and prove that a company collected their biometric data without the requisite consent than it is to prove a violation of the retention and deletion rules that are implemented by businesses after the data is collected. We encourage the Committee to retain this provision.

As this bill moved through the House last year, the private right of action was weakened to require individuals to prove injury or loss sustained as a result of a violation of the law, rather than simply a violation of the law qualifying as an injury-in-fact, as it does in Illinois. Unfortunately, SB169 mirrors this change, which renders the private right of action almost meaningless. Although the impact of improper collection and use of an individual's biometric data is very serious, the ability for an individual to prove harm is particularly difficult.<sup>8</sup> Unlike physical crimes, harms arising from improper data collection or inadequate data protection are often concealed. In addition, the harms caused by such privacy violations are not easily quantified, though the consequences of a lost job, denial of entry to public spaces, or breach of one's biometric information are very real.

If Maryland passes this law to enshrine a right for Marylanders to avoid the improper collection of their biometric data, that right should be enforceable. EPIC recommends reverting to the private right of action provisions from the bill as introduced last session.

The inclusion of a private right of action in SB169 is the most important tool the Legislature can give to Marylanders to protect their privacy. Modeled after BIPA's private right of action, the bills would impose enforceable legal obligations on companies that choose to collect and store individuals' biometric data. As EPIC Advisory Board member Professor Woody Hartzog has written:

---

<sup>6</sup> 740 Ill. Comp. State. Ann. 14/15.

<sup>7</sup> Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>.

<sup>8</sup> See e.g. Brief for EPIC as Amici Curiae, *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), <https://epic.org/wp-content/uploads/amicus/spokeo/EPIC-Amicus-Brief.pdf>.

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook’s share price actually rose 2 percent after the FTC announced its historic \$5 billion fine for the social media company’s privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. [...] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.<sup>9</sup>

The ACLU’s suit against facial recognition company Clearview AI recently settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.<sup>10</sup> BIPA does not just provide Illinoisans with more privacy than most other states, it has nationwide consumer protection effects that similar laws like SB169 will bolster.

EPIC also recommends that any exceptions to the written consent requirement be narrowly defined to avoid abuse. Under SB169 §14-4505 (b)(1)(I), private entities may “collect, use, disclose, redisclose, or otherwise disseminate” biometric information without an individuals’ consent for “fraud prevention or security purposes”. Although such purposes may be legitimate, overly broad definitions of security purposes invite abuse. EPIC suggests the following language to narrow the definition of security purposes under which the use of biometrics should be allowed:

1. To respond to a security incident. For purposes of this paragraph, security is defined as network security and physical security and life safety.
2. To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services. For purposes of this paragraph, the term “illegal activity” means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm.

These narrower definitions would prevent pretextual uses like the deployment of facial recognition at Madison Square Garden and prevent generalized security concerns from validating broad surveillance practices like Clearview AI.

## **Conclusion**

An individual’s ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security and privacy. The unregulated collection and use of biometrics threatens that right to privacy and puts individuals’ identities at risk. We urge the Committee to give SB169 a favorable report with amendment.

---

<sup>9</sup> Hartzog, *supra* note 7.

<sup>10</sup> Ryan Mac and Kashmir Hill, *Clearview AI settles suit and agrees to limit sales of facial recognition database*, N.Y. Times (May 9, 2022), <https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html>.

If EPIC can be of any assistance to the Committee, please contact EPIC Deputy Director Caitriona Fitzgerald at fitzgerald@epic.org.

Sincerely,

/s/ Caitriona Fitzgerald  
Caitriona Fitzgerald  
EPIC Deputy Director

/s/ Jake Wiener  
Jake Wiener  
EPIC Counsel