epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

February 20, 2023

The Honorable C.T. Wilson
House Economic Matters Committee
Room 231
House Office Building
Annapolis, MD 21401

Dear Chair Wilson and Members of the Committee:

EPIC writes in support of 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.[1] Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. HB33 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.[2] EPIC has long advocated for strict limits on the collection and use of biometric data.[3]

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.[4] A Girl Scout leader chaperoning her troop to the annual Christmas Spectacular at Radio City Music Hall was refused entry because she worked at a law firm that was involved in litigation against MSG – even though she wasn't involved in the case. Facial recognition makes it possible to gate entry to otherwise public spaces. A business owner could just as easily use facial recognition deny services to members of this Committee who voted against the owner's interests. A biometric privacy bill like HB33 would prevent this and many other harms.

---

[1] 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.
[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] 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.
[4] 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.

HB33 is modeled after the Illinois Biometric Information Privacy Act (BIPA).[5] Passed in 2008, BIPA has been referred to as one of the most effective and important privacy laws in America.[6] BIPA and HB33 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.

HB33 also includes a requirement that a business obtains informed, written consent before collecting a person's biometric information. Though "notice- and-choice" regimes are not sufficient to protect privacy, the consent provision in BIPA has been effective because it is easy to enforce. It is easier for an individual to prove that a company collected their biometric data without 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.

Unfortunately, the private right of action in this bill was weakened last session 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. This makes it difficult for individuals to bring a case because although the impact of improper collection and use of an individual's biometric data is serious, the ability for an individual to prove harm is very difficult.[7] Unlike physical crimes, harms arising from improper data collection or inadequate security 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 the General Assembly enshrines a right for Marylanders to protect 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 strong private right of action 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 individuals' biometric data. As EPIC Advisory Board member Professor Woody Hartzog has written:

> 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.[8]

[5] 740 Ill. Comp. State. Ann. 14/15.
[6] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf.
[7] 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.
[8] Hartzog, *supra* note 7.

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.[9] BIPA does not just provide Illinoisans with more privacy than most other states, it has nationwide consumer protection effects that similar laws like HB33 will bolster.

EPIC also recommends that any exceptions to the written consent requirement be narrowly defined to avoid abuse. Under HB33 §14-4504 (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 strengthen the private right of action and give HB33 a favorable report.

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

[9] 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.