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

January 31, 2022

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

Dear Chair Wilson and Members of the Committees:

EPIC writes in support of House Bill 259 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, and identity.[1] Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. HB 259 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]

HB259 is modeled after the Illinois Biometric Information Privacy Act (BIPA).[4] Passed in 2008, BIPA has been referred to as one of the most effective and important privacy laws in America.[5] BIPA and HB259 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.

---

[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] 740 Ill. Comp. State. Ann. 14/15.
[5] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI NOW INSTITUTE (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf;

BIPA and HB259 also include a requirement that a business obtains informed, written consent before collecting or otherwise obtaining a person's biometric information.[6] 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.

The inclusion of a private right of action in HB259 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:

> 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.[7]

We encourage the Committee to read Professor Hartzog's case study in its entirety and have attached it to our testimony.

Many privacy laws include a private right of action to empower individuals and have made it possible to hold accountable those who fail to protect or respect personal data. In crafting liability provisions in privacy statutes, legislatures have frequently included a liquidated damages provision to avoid protracted disputes over quantifying privacy damages. This is necessary because it is often difficult to assign a specific economic value to the harm caused by a privacy violation.

For example, when federal legislators passed the Cable Communications Policy Act in 1984, they established privacy rights for cable subscribers and created a private right of action for recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher.[8] The Video Privacy Protection Act specifies liquidated damages of $2,500.[9] The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state court against credit reporting agencies, users of credit reports, and furnishers.[10] In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The

[6] 740 Ill. Comp. Stat. Ann. 14/15.
[7] Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, *supra* note 5.
[8] 47 USC § 551(f).
[9] 18 USC § 2710(c)(2).
[10] 15 U.S.C. §§ 1681n-1681o.

Drivers Privacy Protection Act similarly includes a private right of action.[11] The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss or up to $500 in damages per violation.[12]

The statutory damages set in privacy laws are not exorbitant; they are necessary to ensure that privacy rights will be taken seriously and violations not ignored. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations. EPIC strongly supports the private right of action provisions in HB259.

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 HB259 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

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel and Director,
EPIC Surveillance Oversight Project

Attachment: Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020).

[11] 18 U.S.C. § 2724.
[12] 47 USC § 227(c)(5).