

May 22, 2023

The Honorable Anne Carney, Senate Chair
The Honorable Matt Moonen, House Chair
Maine State Legislature
Judiciary Committee
230 State Street
Augusta, Maine 04330

Dear Chair Carney, Chair Moonen, and Members of the Committee:

EPIC writes in support of LD 1705 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 Mainers 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 LD 1705 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/about/>.

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>.

LD 1705 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.

LD 1705 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.

The inclusion of a strong private right of action is the most important tool the Legislature can give to Mainers 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.⁷

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 violation or \$1,000, whichever is

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 Hartzog, *supra* note 7 (note: 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, see 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>.)

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 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 LD 1945.

Conclusion

An individual's ability to control access to their 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 vote "ought to pass" on LD 1705.

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

⁸ 47 USC § 551(f).

⁹ 18 USC § 2710(c)(2).

¹⁰ 15 U.S.C. §§ 1681n-1681o.

¹¹ 18 U.S.C. § 2724.

¹² 47 USC § 227(c)(5).