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

November 23, 2021

The Honorable James Eldridge, Chair
The Honorable Michael Day, Chair
Joint Committee on the Judiciary
24 Beacon St. Room 136
Boston, MA 02133

Dear Chairs Eldridge and Day:

EPIC writes in support of Senate Bill 47 and House Bill 135, *An Act to regulate face surveillance.* We appreciate your interest in facial recognition technology.

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.[1] EPIC is focused on protecting individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[2] EPIC has litigated the government's use of facial recognition technology and made specific recommendations regarding the protection of privacy.[3]

Facial recognition poses threats to privacy and civil liberties. Facial recognition techniques can be deployed covertly, remotely, and on a mass scale. There is a lack of well-defined regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous identification by government agencies eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, and poses a specific risk to the First Amendment rights of free association and free expression. ***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 use of facial recognition technology erodes that ability.***

There is little a person in the United States could to do to prevent the capture of their image by the government or a private company. Participation in society necessarily exposes one's images in public spaces. But ubiquitous and near effortless identification eliminates the individual's ability to control the disclosure of their identities to others and poses a special risk to the First Amendment rights of free association and free expression, particularly to those who engage in lawful protests.

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

[2] EPIC, *EPIC Surveillance Oversight,* https://epic.org/issues/surveillance-oversight/.

[3] *See EPIC v. FBI*, 72 F.Supp.3d 338 (D.D.C. 2014), http://epic.org/foia/fbi/ngi/; *See also EPIC v. U.S. Customs and Border Protection*, No. 19-cv-689 (D.D.C. filed Mar. 12, 2019), https://epic.org/foia/dhs/cbp/alt-screening-procedures/; Comments of EPIC to Dept. of Homeland Security, *Agency Information Collection Activities: Public Perceptions of Emerging Technologies* (July 12, 2021), https://epic.org/wp-content/uploads/2021/10/EPIC-Comment-DHS-Emerging-Technologies-July2021.pdf.

Growing Support Nationwide for Regulating Face Surveillance

There is growing support in state legislatures and local governments nationwide for a ban on face surveillance. Since last year's State House debate on a facial recognition moratorium, Virginia and Maine have enacted laws very similar to the bills pending before you.

Virginia's law went into effect on July 1, and bans local law enforcement agencies from using facial recognition technology without legislative approval.[4] It also bans the use of tools like Clearview AI by requiring that, if approval is given, the local police must have "exclusive control" over the facial recognition system they use.

In June 2021, Maine enacted an even stronger law – prohibiting government use of facial recognition except in very limited circumstances, including by the RMV and State Police in serious criminal investigations.[5] The Maine law includes a private right of action, meaning that individuals may bring a lawsuit if they believe a government agency or official has violated the law.

So Massachusetts would not be an outlier here – there is growing recognition that facial recognition technology simply is not ready for prime time and law enforcement should not be using it.

The approach in Senate Bill 47 and House Bill 135 is good – it's important to impose a general prohibition on government use and possession of remote biometrics, and then carve out specific exceptions to that general prohibition if needed. Too often, surveillance policy is made via the procurement process at the executive level—not by legislators informed by public opinion and debate. If a state agencies want to use facial recognition technology, the agency request authorization for that use from the Legislatures – that process ensures that civil rights protections will be considered and enshrined into that statute.

This technology is too dangerous to let deployments come before specific statutory authorization – the safeguards need to be in place first.

Safeguards Needed Prior to Deployment

Because of the special risks involved with biometric data, were this bill to pass, the Legislature must require agencies collecting, handling, storing, and transmitting this kind of data to adhere to these principles prior to deployment:

1. ***Prohibition on mass surveillance.*** Use must be context dependent. Biometric data should be processed fairly and lawfully, collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with these specified purposes.

[4] Va. Code. Ann. § 15.2-1723.2, § 23.1-815.1; *see also* Denise Lavoie, *Virginia lawmakers ban police use of facial recognition*, Associated Press (Mar. 29, 2021), https://apnews.com/article/technology-legislature-police-law-enforcement-agencies-legislation-033d77787d4e28559f08e5e31a5cb8f7.

[5] Me. Rev. Stat. Ann. tit. 25, §6001 (2021); *see also* Dave Gershgorn, *Maine passes the strongest state facial recognition ban yet*, The Verge (June 30, 2021), https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law.

2. ***Provably non-discriminatory.*** May not be deployed unless non-discrimination is certified. Both the technology used (e.g. the facial recognition system) and the database searched against should be demonstrably unbiased.

3. ***Minimal Retention.*** No retention after identity confirmed.

4. ***Transparency***. The data subject has the right to access the data undergoing processing and, where appropriate, to rectify, erase, or block its processing

5. ***Security.*** Biometric data should be encrypted and stored separately from other data. Access to this data should be limited to those who need it. Data-handlers should assure the security of this data during transmission to third-parties.[6]

6. ***Monitoring for inappropriate uses***

7. ***Accountability***. Facial recognition technology should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, and its risks. Institutions must be responsible for outcomes from the use of facial recognition technology and there must be some consequence for agencies that fail to abide by these principles. This could include a private right of action.

8. ***Independent auditing***

Conclusion

Because of the risks inherent in facial recognition technology, it is vital for the Commonwealth to create a framework within which state agencies and the Legislature can work to ensure the security and privacy of Massachusetts residents. There must be a process in place to ensure the above safeguards are established before any state agency obtains or uses a facial recognition system.

EPIC urges you to give a favorable report to Senate Bill 47 and House Bill 135.

Sincerely,

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Deputy Director

[6] *See, e.g.*, 740 Ill. Comp. Stat. 14/15(e); Tex. Bus. & Com. Code Ann. § 503.001(c) (West 2011); *Privacy Code*, *supra* note 113, at Principle 12.