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

October 22, 2019

The Honorable James B. Eldridge, Chair
The Honorable Claire D. Cronin, Chair
General Court of the Commonwealth of Massachusetts
Joint Committee on the Judiciary
24 Beacon St. Room 136
Boston, MA 02133

Dear Chairs Eldridge and Cronin:

EPIC writes in support of Senate Bill 1385 and House Bill 1538, *An Act establishing a moratorium on face recognition and other remote biometric surveillance systems.* 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.[4] ***An individual's ability to***

[1] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[2] EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/; *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Comm. on the Judiciary* (2013) (statement of Amie Stepanovich, Director of the EPIC Domestic Surveillance Project), https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf; Comments *of EPIC to DHS*, Docket No. DHS-2007-0076 CCTV: Developing Privacy Best Practices (2008), *available at* https://epic.org/privacy/surveillance/epic_cctv_011508.pdf.
[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 Federal Bureau of Investigation, *Privacy Act of 1974; Systems of Record Notice of a Modified System of Records Notice* (July 6, 2016), https://epic.org/apa/comments/EPIC-CPCLO-FBI-NGI-Comments.pdf.
[4] *See* Ian Kerr & Jennifer Barrigar, *Privacy, Identity and Anonymity* (Apr. 1, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3396076.

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.

Facial recognition's surveillance capabilities have been on full display in China. China is not only a leading user of mass surveillance technology, particularly facial recognition, they also lead in exporting the technology.[5] The Chinese government has implemented a massive facial recognition surveillance system.[6] China has leveraged their surveillance network to implement an "advanced facial recognition technology to track and control the Uighurs, a largely Muslim minority."[7] And China continues to expand the use of facial recognition technology. A university in China is testing the use of facial recognition to monitor whether students attend classes and track their attention during lectures.[8] Soon, to buy a smartphone in China will require a facial scan.[9]

In Hong Kong, where protests have been ongoing since March, face scans have become a weapon. Protesters fear that facial recognition technology is being used to identify and track them.[10] In response to this fear, protesters have resorted to covering their faces and have taken down facial recognition cameras. Hong Kong reacted by banning masks and face paint.[11] Many demonstrators worry that the mass surveillance implemented on the mainland of China will be implemented in Hong Kong.

Not all uses of facial recognition are equally problematic. For instance, where the user has control and there is no government mandate, such as using Face ID for iPhone authentication, the same privacy issues do not arise. Facial recognition can also be used for verification or

---

[5] Steven Feldstein, *The Global Expansion of AI Surveillance* 13-15 (Sept. 2019), https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.
[6] Simon Denyer, *China's Watchful Eye*, Wash. Post (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.
[7] Paul Mozur, *One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[8] Brendan Cole, *Chinese University Tests Facial Recognition System to Monitor Attendance and Students' Attention to Lectures*, Newsweek (Sept. 2, 2019), https://www.newsweek.com/nanjing-china-facial-recognition-1457193.
[9] Kyle Wiggers, *AI Weekly: In China, You Can No Longer Buy a Smartphone without a Face Scan*, VentureBeat (Oct. 11, 2019), https://venturebeat.com/2019/10/11/ai-weekly-in-china-you-can-no-longer-buy-a-smartphone-without-a-face-scan/.
[10] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N.Y. Times (July 26, 2019), https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.
[11] Matt Novak, *Hong Kong Announces Ban on Masks and Face Paint That Helps Protesters Evade Facial Recognition*, Gizmodo (Oct. 4, 2019), https://gizmodo.com/hong-kong-announces-ban-on-masks-and-face-paint-that-he-1838765030.

authentication using 1:1 matching – where the system does not check every record in a database for a match, but matches the individual's face to their claimed identity.[12] This 1:1 matching is a much more privacy protective implementation of facial recognition. 1:1 matching does not require a massive biometric database, there is no need to retain the image, and the machines conducting the 1:1 match need not be connected to the cloud. Such an implementation virtually eliminates data breach risks and the chance of mission creep.

EPIC has pursued the privacy and security risks raised by facial recognition in many forums, including letters to federal agencies, congressional testimony, and complaints before federal agencies. In 2002, EPIC Executive Director Marc Rotenberg testified about facial recognition before Congress.[13] He explained there are several ways to compromise the effectiveness of a biometric system: by false identification at enrollment, physical alteration of a personal biometric, skewing the sample collection by not cooperating, and hacking into or falsifying data.[14] Facial recognition system errors would lead to innocent people being falsely matched to watchlists or databases, while suspects would pass through the system unrecognized.

Ten years ago over 100 hundred privacy organizations and privacy experts in the Madrid Declaration[15] called for a moratorium on facial recognition as a system of mass surveillance, saying:

> A moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate.

There is growing support in the states and in Congress for a moratorium on facial recognition technology. Earlier this month, California enacted a law banning the use of facial recognition technology in law enforcement body cameras.[16] San Francisco, Berkley, and Oakland, California, and Somerville, Mass. have all passed local bans on the use of facial recognition by city agencies.[17]

In Congress, there is bipartisan support for halting the use of facial recognition technology by the government. Senator Edward Markey [D-MA] and Senator Mike Lee [R-UT] have been calling for the Department of Homeland Security to pause its use of facial recognition technology for almost two years.[18] In their most recent statement, the Senators said "DHS should pause their efforts until

---

[12] Lucas D. Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Ctr. for Catastrophe Preparedness & Response, N.Y. Univ., 11 (2009), *available at* https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf.

13 *Identity Theft Involving Elderly Victims: Joint Hearing Before the Special Comm. on Aging*, 107th Cong. (2002) (statement of Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr.), *available at* http://www.epic.org/privacy/biometrics/testimony_071802.html.

14 *Id.*

[15] The Madrid Privacy Declaration, *available at* http://thepublicvoice.org/madrid-declaration/.

[16] 2019 Cal. Legis. Serv. Ch. 579 (A.B. 1215).

[17] *See* EPIC, State Facial Recognition Policy, https://epic.org/state-policy/facialrecognition/.

[18] Davey Alba, *These Senators Want Homeland Security To "Pause" Its Airport Facial Recognition Program* (Mar. 12, 2019), https://www.buzzfeednews.com/article/daveyalba/these-senators-want-homeland-security-to-pause-its-facial; Letter from Sens. Edward Markey and Mike Lee to Kirstjen Nielson, Secretary, Dept. of Homeland Security (Dec. 21, 2017), https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20letter1.pdf;

American travelers fully understand exactly who has access to their facial recognition data, how long their data will be held, how their information will be safeguarded, and how they can opt out of the program altogether."[19] Prior to his passing, Rep. Elijah Cummings [D-MD] and Rep. Jim Jordan [R-OH] – the Chair and Ranking Member of the House Oversight Committee – were reportedly working on legislation that would place a moratorium on funding facial recognition technology use by the federal government.[20] "It seems to me, it's time for a time out," said Ranking Member Jim Jordan at a recent hearing on facial recognition technology.[21]

Society is simply not in a place right now where we are in place to deploy facial recognition technology. It would be a mistake to deploy facial recognition at this time.

Recommendations

Because of the special risks involved with biometric data, including facial recognition data and faceprints, the Commonwealth 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.

2. ***Provably non-discriminatory.*** May not be deployed unless non-discrimination is certified.

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

---

Letter from Sens. Edward Markey and Mike Lee to Kirstjen Nielson, Secretary, Dept. of Homeland Security (May 11, 2018), https://www.markey.senate.gov/imo/media/doc/Biometric%20Exit%20Program%20Letter.pdf; Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.

[19] Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.

[20] POLITICO Morning Tech, *Lawmakers want limits on facial recognition funds* (Aug. 22, 2019), https://www.politico.com/newsletters/morning-tech/2019/08/22/lawmakers-want-limits-on-facial-recognition-funds-472395.

[21] *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*, House Comm. on Oversight and Gov't Reform, 116th Cong. (May 22, 2019) (Sen. Jim Jordan at 1:26:08), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and

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.[22]

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 can work to ensure the security and privacy of Massachusetts residents. The Commonwealth should not deploy facial recognition techniques until the above principles are established. As such safeguards have not yet been established, EPIC recommends a moratorium on the deployment of facial recognition technologies.

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

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

[22] *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.