Boston City Councilor Lydia Edwards
Chair, City Council Committee on Government Operations
Docket #0683. City Council
City Hall. 5th Floor
Boston MA 02201

June 5, 2020

Re: Docket #0683, Ordinance Banning Facial Recognition Technology in Boston

Dear Chair Edwards:

The Electronic Frontier Foundation (EFF) strongly supports legislation that bans government agencies and employees from using face surveillance technology or information derived from such technology. This technology is a menace to privacy, free speech, and racial justice. We thank the sponsors of the Boston ordinance on face recognition for their attention to this critical issue. EFF will support this bill if three changes are made: to close a police loophole; to ensure enforcement; and to avoid undue application to private groups.

EFF works to ensure that technology supports freedom, justice, and innovation for all the people of the world. We are a non-profit advocacy group with more than 30,000 members that advances the interests of tech users in legislative bodies throughout the country.

1. Why Boston should ban government use of face surveillance

Face surveillance is profoundly dangerous for many reasons.[1] First, it invades our privacy, by tracking a unique marker we show everywhere we go and cannot change: our own faces. Surveillance cameras in public spaces are proliferating, operated by myriad government and private entities. These cameras are increasingly networked into unified systems. Face surveillance technologies are growing increasingly powerful. In combination, these technologies can track everyone who lives and works in public. We must not build an infrastructure that empowers government to easily track where everyone is going, what they are doing, and who they are with.

Second, government use of face surveillance technology in public places will chill people from engaging in protests. Courts have long recognized that government surveillance of First Amendment activity has a "deterrent effect." *See, e.g., Lamont v. Postmaster*, 381 U.S. 301 (1965). Empirical research confirms this problem. *See, e.g.,* Stoycheff, "Facebook's spiral of silence effects in the wake of NSA Internet monitoring" (2016); Penney, "Online surveillance and Wikipedia use" (2016).[2]

[1] https://www.eff.org/pages/face-recognition.

[2] https://journals.sagepub.com/doi/pdf/10.1177/1077699016630255; https://scholarship.law.berkeley.edu/btlj/vol31/iss1/5/.

Third, surveillance technologies have an unfair disparate impact against people of color, immigrants, and other vulnerable populations. Governments have, for example, used them to spy on advocates for racial justice.[3] Surveillance technologies often criminalize entire neighborhoods.[4] For example, watch lists are often over-inclusive and error-riddled, and cameras often are over-deployed in minority areas.[5] And these spying tools increasingly are being used in conjunction with powerful mathematical algorithms, which often amplify bias.[6]

Fourth, once government builds a face surveillance infrastructure, there is the inherent risk that thieves will steal its sensitive data, employees will misuse it, and policy makers will redeploy it in new unforeseen manners.[7]

Thus, face surveillance is so dangerous that governments must not use it at all. At least four cities in Massachusetts have already banned government use of this technology.[8] So have at least three cities in California.[9] EFF is working with advocacy groups across the country to enact similar bans, through a campaign we call "About Face."[10] Now it is Boston's turn to help lead this nationwide movement.

When a private entity acts on behalf of government, it should also be subject to the ban on government use of face surveillance. But when a private entity acts for itself, a different rule should apply: a business cannot apply face surveillance to a person unless the person first gives their informed, voluntary, opt-in consent. That's the rule under the Illinois Biometric Information Privacy Act (BIPA),[11] which is now being used to

---

[3] https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter; https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/?utm_term=.13db56fe4bb8.

[4] https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf

[5] https://www.eff.org/deeplinks/2017/04/next-steps-toward-reforming-californias-unfair-gang-databases; https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

[6] https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/.

[7] https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/.

[8] https://www.eff.org/document/somerville-face-surveillance-ban; https://www.eff.org/document/article-839-ban-town-use-face-surveillance; https://www.eff.org/document/19176-ordinance-prohibiting-use-face-surveillance-systems; https://www.eff.org/document/amend-chapter-2128-surveillance-technology-ordinance-adding-2128020-definitions-new.

[9] https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019; https://www.eff.org/document/oakland-face-surveillance-ban; https://www.eff.org/document/berkeley-face-surveillance-ban.

[10] https://www.eff.org/aboutface.

[11] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

challenge Clearview AI's infamous collection of three billion faceprints from internet users.[12] Some consumers might determine that it is in their interests to allow a business to collect their faceprint to, for example, unlock their phone or enter a building. But this must be the consumer's own autonomous choice, freely and knowingly given.

3. What the Boston ordinance would do

There are many provisions of the Boston ordinance that EFF likes a great deal. Three deserve emphasis. First, the Boston ordinance would ban any Boston agency or official from obtaining or using any face surveillance system or any information derived from such a system. *See* Sec. (b)(1)(a). Second, it would suppress evidence collected in violation of this rule. *See* Sec. (c)(2). Third, it would allow any person to bring a private right of action to enforce this rule. *See* Sec. (c)(3).

3. How the Boston ordinance should be strengthened

EFF respectfully seeks three amendments to the Boston ordinance on government use of face recognition technology. First, the bill has an exemption for evidence generated by face surveillance that relates to investigation of crime. *See* Sec. (b)(2)(a). As written, this exemption might extend to occasions when Boston police generate such evidence or ask another entity to do so. Of all the city agencies that might use face surveillance, police use raises the most concerns. Thus, EFF respectfully requests the following ***additional language***:

> Nothing … shall prohibit Boston or any Boston official from … using evidence relating to the investigation of a specific crime that may have been generated from a face surveillance system***, so long as such evidence was not generated by or at the request of Boston or any Boston official***.

Second, the private right of action does not provide fee shifting for a prevailing plaintiff. But without such fee shifting, the only private enforcers will be advocacy organizations and wealthy individuals. Fee shifting is a commonplace remedy to ensure effective enforcement of all manner of statutes that protect the public. Thus, EFF respectfully requests the following additional language:

> Any violation of this ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this ordinance. ***A court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in such proceedings.***

[12] https://www.aclu.org/press-releases/aclu-sues-clearview-ai.

Third, the ban extends not just to government use of face surveillance, but also to private sector use of face surveillance conducted with a government permit. *See* Sec. (b)(1)(c). As noted above, while EFF supports a ban on government use of face surveillance, the better approach to private sector use of face surveillance is to require opt-in consent. Here, a private entity should be allowed to get a city permit, for example, to use a city public forum to conduct an educational event about the privacy hazards of face surveillance, including an opportunity for members of the public to give their consent to participate in a one-off use of face recognition technology. Thus, EFF respectfully requests the following additional language:

> It shall be unlawful for Boston or any Boston official to issue any permit or enter into any other agreement that authorizes any third party***, on behalf of Boston or any Boston official,*** to obtain, retain, possess, access, or use (i) any face surveillance system, or (ii) information derived from a face surveillance system.

* * *

Thank you for your work to ban face surveillance in Boston. EFF will support the Ordinance Banning Facial Recognition Technology in Boston, if it is amended as set forth above.

Sincerely,

Adam Schwartz
Senior Staff Attorney
adam@eff.org