Written testimony for the 7/30 public comment meeting of the Legislature's Special Commission on Facial Recognition

C Lobdell <clobdell@gmail.com>
Thu 7/29/2021 11:28 PM

To: Manning, Jacqueline O. (HOU) <Jacqueline.O.Manning@mahouse.gov>

Dear Co-chairs Day and Edridge and committee members,

My name is Claire Lobdell. I'm a resident of Northampton, MA which in 2019 banned the municipal use of face surveillance technology (a.k.a. facial recognition software). I'm also a librarian and a member of the Library Freedom Project, a digital privacy and anti-surveillance education and advocacy organization.

I urge you to draft legislation that would ban the use of facial surveillance technology by government entities in Massachusetts. Facial surveillance technologies have been shown to misidentify black and brown people and gender non-conforming people more often than white, gender-conforming folks (1, 2), which has led police to mistakenly arrest and imprison innocent black men (3). Ruha Benjamin explains in her book Race After Technology that the algorithms that power artificial intelligence systems like face surveillance software encode the biases of their creators—the same biases as society at large. She calls face surveillance and related technologies "the new Jim Code" because they perpetuate the systems of surveillance and control that whites in this country have exerted over black and brown people through slavery, the Jim Crow era, the War on Drugs, and into the present (4).

Face surveillance companies including Clearview AI (5)—which has been used extensively by law enforcement agencies—and Ever AI (6) among others, have used extremely devious, unethical, and sometimes illegal methods to compile their databases. The Commonwealth of Massachusetts should not endorse these practices by contracting with such companies.

Finally, I ask you to consider that surveillance technologies and the vast databases they create can and are used in ways that outstrip the imaginations and intentions of their creators. The same database of images that is used to locate a criminal can be used by a police officer to stalk an intimate partner. When that database is hacked by an outside entity, it can do untold damage to peoples' lives. We are safer if these technologies are not deployed in the first place.

Thank you for your time and work on this issue.

Claire Lobdell

References

1. Najibi, Alex. "Racial Discrimination in Face Recognition Technology." Science in the News, 24 Oct. 2020, sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

2. Snow, Jacob. "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots." American Civil Liberties Union, 26 July 2018, www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

3. Hill, Kashmir. "Another Arrest, and Jail Time, due to a Bad Facial Recognition Match." The New York Times, 29 Dec. 2020, www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html?searchResultPosition=10. Accessed 29 July 2021.

4. Benjamin, Ruha. Race after Technology : Abolitionist Tools for the New Jim Code. Medford, Ma,

Polity, 2019.

5. Statt, Nick. "ACLU Sues Facial Recognition Firm Clearview AI, Calling It a 'Nightmare Scenario' for Privacy." The Verge, 28 May 2020, www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws.

6. Solon, Olivia, and Cyrus Farivar. "Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools." NBC News, 9 May 2019, www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371. Accessed 30 July 2021.