29 July 2021

Commission on Facial Recognition

Senator Jamie Eldridge and Representative Michael S. Day, Co-Chairs

**Public Comment**

**Government Use of Facial Recognition Technology**

Dear Senator Eldridge, Representative Day, and members of the Commission,

Good morning. My name is Amy van der Hiel. I am writing to provide some comments about the use of facial recognition technology in Massachusetts. I respectfully ask that the Commission recommend the legislature strengthen existing facial recognition law to ensure Massachusetts residents and visitors are shielded from discriminatory, dragnet surveillance and other harms.

I work at the World Wide Web Consortium at the Massachusetts Institute of Technology - however, I am not speaking on behalf of my employer but as a private individual.

In the tech world it is well understood that there is significant potential for error in facial recognition technology. A 2019 study by the National Institute of Standards and Technology found that algorithms falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces. The study found both "false positives," in which an individual is mistakenly identified, and "false negatives" where the algorithm fails to accurately match a face to a specific person in a database [1]. Such mistakes in identification could result in the arrest or jailing of innocent people and there is evidence of potential racial errors in the results.

As well as concerns about the accuracy of the technology, there are also great concerns about whether such technologies might be inappropriately used. In May 2021 the press reported that the Post Office Internet Covert Operations Program (iCOP) not only tracked the social media posts of Americans but also employed facial recognition software like Clearview AI, a facial recognition software which scrapes images off public websites. They also ran keyword searches on social media event pages to identify potential threats from scheduled protests and shared the information gathered with other agencies [2]. That the Post Office had been covertly monitoring Americans shocked many of us and raises huge concerns about oversite, accountability and the ability of public agencies to track, surveil and invade the privacy of the very people they are meant to serve. We have a right to free expression and the right to assemble. We must maintain our freedom to move about in public streets, go to work, attend school and be in our neighborhoods without our privacy and civil liberties being eroded or threatened.

In December 2020, Governor Baker signed into law “An Act Relative To Justice, Equity And Accountability In Law Enforcement In The Commonwealth,” an omnibus police reform legislation. The law, codified in Chapter 253 of the Acts of 2020, contains several provisions pertaining to government agencies’ use of facial recognition technology.

While I support some of those provisions, namely the creation of this Commission, the regulations governing police use of facial recognition fall far short of what is needed.

One important concern is that this law does not prohibit or regulate the use of facial recognition technologies for purposes of surveillance of public spaces like streets and parks; it also does not regulate facial recognition technology as used by law enforcement agencies and does not restrict which public agencies can or cannot acquire and possess a facial recognition system.

Thankfully, lawmakers have addressed these concerns in legislation filed this session. H.135, An Act To Regulate Face Surveillance, sponsored by Representatives Rogers and Ramos, and S.47, An Act To Regulate Face Surveillance, sponsored by Senator Creem, provide for some useful policy solutions to the concerns I mentioned above.

This legislation will prohibit the use of facial recognition for surveillance of public spaces. It will stipulate that the only agencies allowed to use and possess this technology are the Registrar of Motor Vehicles and the State Police, subject to strict limitations and civil rights protections. And it will make a special caveat for the M.S.P. so that its officers can only access the R.M.V. system in three limited cases: to execute a warrant issued under probable cause; in case of an emergency involving immediate danger of death or serious physical injury; and to identify a deceased person.

I encourage you to consider bills H.135 and S.47 when you decide on further regulations of the use of biometric surveillance technology by government entities. We need strong regulations to ensure it doesn’t infringe on our civil rights and civil liberties and this legislation provides an excellent model.

Thank you for your attention and consideration.

Amy van der Hiel

137 Brown Ave, Roslindale, MA

(This testimony expresses my personal view only)

1. “NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software”, National Institute of Standards and Technology, December 19, 2019

https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

2. “Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program”, Yahoo News, Jana Winter, May 18, 2021
https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html?soc\_src=community&soc\_trk=tw