SECURE JUSTICE

July 26, 2020

VIA E-MAIL ONLY
Hector Dominguez
Open Data Coordinator – Smart City PDX
Bureau of Planning & Sustainability
E-Mail: smartcitypdx@portlandoregon.gov

Re: **Prohibition on Facial Recognition Technology**

Dear Mr. Dominguez:

On behalf of Secure Justice, thank you for allowing us to provide commentary on the proposed ordinances pertaining to surveillance, public privacy, and facial recognition technology.

Secure Justice is a non-profit organization located in Oakland, California, that advocates against state abuse of power, and for reduction in government and corporate over-reach. We target change in government contracting, and corporate complicity with government policies and practices that are inconsistent with democratic values and principles of human rights. We were part of the team that successfully advocated for prohibitions on city use of facial recognition technology in San Francisco, Oakland, Berkeley and Alameda.

Prohibition on City Use of Facial Recognition Technology[1]

We applaud the intent to prohibit the city's use of dangerous facial recognition technology, and strongly encourage Portland to implement the technology vetting framework described in the ordinance. As Chair of the City of Oakland's Privacy Advisory Commission, I have seen firsthand the importance of a standing body and procurement process that allows for meaningful discussions to occur in public regarding the use of privacy invading and potentially harmful technologies.

Across the country, municipalities like Portland are quickly discovering that facial recognition technology is inappropriate in their respective cites, and several states like California have imposed moratoriums on its use. Beginning with San Francisco and most recently with Boston, large and small governing bodies are listening to their communities as they strongly reject this creepy technology.

We do suggest two amendments to the ordinance. While we understand the intent of the right-to-cure provision and have supported such provisions in our various Bay Area reform efforts, ninety days is far too lengthy when technologies like facial recognition are available. In ninety days, a

[1] The draft we were provided and reviewed is dated July 1, 2020.

bad actor could easily collect and/or identify Portland's entire population. We recommend a shorter period of 30 days.

In addition, the current enforcement mechanism will likely not provide much protection because A) we typically only learn of harm from surveillance long after the fact, and B) this technology works at a distance, in secret, and thus an injured party will almost never discover that they were subject to its use.

We suggest using the private right of action from Oakland's surveillance equipment ordinance (slightly modified for our purposes here):

"Violations of this ordinance are subject to the following remedies:

A. Any violation of this ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in a court of competent jurisdiction to enforce this ordinance. An action instituted under this paragraph shall be brought against the respective city department, and the City of Portland, and, if necessary to effectuate compliance with this ordinance (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this ordinance, to the extent permitted by law.
B. Any person who has been subjected to facial recognition technology in violation of this ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this ordinance, may institute proceedings in a court of competent jurisdiction against the City of Portland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).
C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A or B.
D. Violations of this ordinance by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units." Oakland Municipal Code Chapter 9.64.

On June 25, 2019, the United Nations Special Rapporteur David Kaye released a report on surveillance technology, calling for a worldwide moratorium on invasive technology like facial recognition software. "Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation," the Special Rapporteur said in statement. "And yet they are not subject to any effective global or national control."[2]

[2] https://news.un.org/en/story/2019/06/1041231

We believe the Portland City Council should prohibit the city's acquisition or use of facial recognition technology for the following reasons:

1. **The error rate will create a substantial financial liability for the City of Portland, and waste resources instead of conserving them.**

According to the groundbreaking MIT study conducted by Joy Buolamwini, facial recognition technology has an error rate of up to 34.7% for black women, with a greater propensity to misidentify darker skin tones[3]. It would be irresponsible to allow the Portland Police Department, in a diverse city like yours, to use a technology with such a high error rate especially against the darker skins of certain communities that have historically been over-policed and profiled.

Although proponents of this technology put forth a credible argument about new technology's ability to make us faster and more efficient, they are ignoring the high error rate which will necessarily make us less efficient, as we must discard false positives and/or rely on other sources of information to confirm what the computers are telling us, because the results aren't trustworthy. As our coalition learned recently in Oakland from the Police Chief's own report, "most of the time the search does not yield a match." *See* Chief Kirkpatrick June 17, 2019 Report, Pg. 4 ¶2.

Earlier this year, Robert Julian-Borchak Williams, a black man in Detroit, was arrested by the Detroit Police Department in front of his wife and young children. Mr. Williams had his mug shot taken, and his fingerprint and DNA data taken and entered into law enforcement databases. During his interview, Detroit PD showed a photo to Mr. Williams that they had run through a facial recognition program. Mr. Williams immediately stated that it obviously was not him. "Do you think all black men look alike?" When the investigating officers realized they clearly had the wrong person, the officers casually replied: "I guess the computer got it wrong."[4] This underscores the danger in relying on surveillance technology in the context of policing. In the follow up discussions at Detroit's City Hall, Detroit Police Chief James Craig admitted that the technology they were using had a 96% error rate.[5] There is a clear liability risk from using this technology, as demonstrated by another recently published story from Detroit, again resulting in the wrongful arrest of a black man.[6] As stewards of Portland's tax dollars, the City council should prohibit use of this dangerous technology.

When the technology does yield a supposed match, the results can be terrifying for an individual mistaken for another. In April, Brown University student Amara Majeed was misidentified as one of the Sri Lankan bombers from the Easter terrorist attack.[7] Teenager Ousmane Bah was

[3] http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[4] https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[5] https://arstechnica.com/tech-policy/2020/06/detroit-police-chief-admits-facial-recognition-is-wrong-96-of-the-time/

[6] https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/

[7] https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html

misidentified by facial recognition technology and accused of robbing an Apple Store in Boston, a city he has never been to.[8]

2. Mission creep is historical reality.

No tool with more than one use ever remains confined to a single use for very long. Just ten years ago, license plate readers were introduced to recover stolen vehicles more effectively, to overcome the “hiding in plain sight” phenomenon. Today, they are used for all criminal investigations, at-risk and witness locates, civil investigations such as insurance and worker’s comp fraud, and administrative purposes like neighborhood parking passes and payment of parking fees. We believe that facial recognition is even more versatile than a license plate reader because we cannot separate ourselves from our faces, and thus the impact and mission creep will be larger if you crack open the door for limited uses now. In addition, the expensive part of a citywide mass surveillance system is already in place – cameras are everywhere, typically linked together and remotely viewable. All that remains is the flip of a switch to enable facial recognition.

3. Facial Recognition Technology is anti-democracy and anti-privacy.

We have a human right to privacy. The United States Supreme Court has consistently ruled for decades that we have the right to be anonymous in public. As a people, we have never consented to law enforcement tracking and tagging us like cattle, without at least a reasonable suspicion of wrongdoing. We have never been forced to, nor agreed to, carry a visible ID around with us as we move about our lives. We have consistently said we do not need to identify ourselves walking around, yet with this technology, it is the equivalent of forcing us to identify ourselves to others simply by participating in modern day life and walking outside our front door. We do not need to speculate about this threat – China is presently using facial recognition against its minority Muslim Uighur population by tracking certain ethnic facial features, today’s equivalent of the yellow star for Jews during Hitler’s reign.

If Portland allows for the use of facial recognition technology, the inevitable mission creep will cause it to become ubiquitous, and this is our primary concern: this technology is the most radical, and the most intrusive, that we have ever seen in our lifetimes. If used widely, and certainly by those with police power, it will destroy our first amendment protections due to its chilling effect.

No young person exploring their sexuality will be comfortable exploring a gay bar for the first time. Muslims will be nervous attending their mosques. Inter-racial and same sex relationships, cannabis use, aiding run-away slaves (today, refugees), all these actions occurred in the “underground”, requiring privacy, before they became accepted as the new normal and decriminalized. In a world of perfect surveillance, these types of social changes will no longer be possible, because the status quo will become cemented.

[8] https://slate.com/technology/2019/04/a-teenager-is-accusing-apple-of-misidentifying-him-with-a-facial-id-system.html

A March 2019 David Binder Research poll conducted for the ACLU revealed that over 82% of likely California statewide voters, and 79% of likely Bay Area voters, **oppose** the government using biometric information to monitor and track who we are, and where we go[9]. It is likely that our neighbors to the north in Portland share similar views.

On June 27, 2019, Axon publicly issued a statement affirming that they will not use facial recognition technology in conjunction with their body cameras, following the advice of its independent ethics board.[10] Axon now joins Google and Microsoft as major players that are saying no to the use of their technology in harmful, biased ways. The California legislature has prohibited the use of this technology in body cameras statewide.

The health of our democracy depends on our ability to occasionally say no – that this technology, more so than others, is too radical for use in our community. We are already losing our ability to move about and associate freely, without this intrusive, error-prone technology. Our locational history is tracked by license plate readers, Stingrays, and cellphone tower dumps. There are already thousands of cameras in place, just waiting for facial recognition to be coupled with them. We do not have to accept as inevitable that technology will creep further into our lives

Prohibiting the Use of Face Recognition Technology in Public Spaces[11]

We applaud Portland's groundbreaking effort to prohibit the use of this technology in places of public accommodation, and to protect our public privacy interests.

We do suggest that the exceptions in this ordinance match the language used in the ordinance above, as to user verification. Although the intent here is likely to allow an individual to unlock their own personal device using facial recognition technology such as Apple's FaceID, the language could be interpreted to allow private entities to force an individual to unlock their phone using this technology.

We suggest the following amendment: "An individual may use face recognition technology to access their own personal or employer issued or assigned personal communication devices or computers for the sole purpose of user verification."

In addition, we suggest that the private right of action discussed above also be included in this ordinance.

[9] https://www.aclunc.org/docs/DBR_Polling_Data_On_Surveillance.pdf

[10] https://www.engadget.com/2019/06/27/axon-facial-recognition-ai-police-body-cameras/

[11] The draft we were provided and reviewed is dated July 1, 2020.

Portland's leadership and acknowledgment of the concerns regarding these complicated matters is appreciated. We trust that you will recognize the moment that we are in and prohibit the use of such dangerous technology.

Sincerely,

Brian Hofer
Executive Director
(510) 303-2871
brian@secure-justice.org
https://secure-justice.org/