PRAMILA JAYAPAL
7TH DISTRICT, WASHINGTON

HOUSE COMMITTEE ON THE JUDICIARY

VICE CHAIR, SUBCOMMITTEE ON
IMMIGRATION AND CITIZENSHIP

MEMBER, SUBCOMMITTEE ON ANTITRUST,
COMMERCIAL, AND ADMINISTRATIVE LAW

HOUSE COMMITTEE ON THE BUDGET

HOUSE COMMITTEE ON
EDUCATION AND LABOR

MEMBER, SUBCOMMITTEE ON
HIGHER EDUCATION AND WORKFORCE INVESTMENT

MEMBER, SUBCOMMITTEE ON
WORKFORCE PROTECTIONS

Congress of the United States
House of Representatives
Washington, DC 20515-4707

1510 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3106

1904 3RD AVENUE
SUITE 510
SEATTLE, WA 98101
(206) 674-0040

September 29, 2020

To the Port of Seattle Commission:

Thank you for inviting my office to serve on the Port's Biometrics External Advisory Group. As the Congresswoman representing Washington's 7th district—home to several Port facilities, and countless employees and customers—I too am committed to ensuring our constituents' interests are heard and represented. For that reason, I am writing to express deep concern for the Port's use of facial recognition technology for any discretionary purpose. Algorithmic bias against people of color, women, children, and seniors presents significant and consequential justice and equity problems for anyone who uses or works at a Port of Seattle facility. Further, there are broad civil liberties concerns as Federal law currently provides no privacy safeguards or standards for the use of facial recognition, or other biometric surveillance technology. What my staff has learned while serving on the Advisory Group coupled with the evolution of my own thinking prompt me to suggest that the Port Commission consider a moratorium on the use of biometrics technology in all Port activities under its purview except for voluntary programs like CLEAR.

Facial recognition technology is plagued with significant bias, as numerous reports have found that this technology has difficulty recognizing people of color, transgender individuals, and people wearing masks.[1] Specifically, a December 2019 National Institute of Standards and Technology report found that false positives are up to 100 times more likely for Asian and Black faces, with American Indians having the highest rates of being falsely identified.[2] This bias has, at times, grave implications. Earlier this year Robert Julian-Borchak Williams, a Black man in Detroit, Michigan was wrongfully arrested and imprisoned due to a flawed match from a facial recognition algorithm.[3] This is the first *known* case of wrongful arrest due to false match, and exemplifies the danger of law enforcement reliance on a technology that is rife with bias.

[1] Rebecca Heilweil, *Masks Can Fool Facial Recognition Systems, But the Algorithms Are Learning Fast*, Vox (Jul. 28, 2020) https://www.vox.com/recode/2020/7/28/21340674/face-masks-facial-recognition-surveillance-nist

[2] NIST, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019) https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[3] Kashmir Hill, *Wrongfully Accused by an Algorithm*, New York Times (June 24, 2020) https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html?auth=login-email&login=email

The lack of federal regulation on the use of facial recognition technology also presents civil liberties concerns about the widespread implications of its use and the associated data that is collected. Private companies have begun to respond to the lack of regulation on government use of FRT. In 2019, Axon, the country's largest supplier of police body cameras banned face recognition systems on its technology.[4] Recently, Microsoft, IBM and Amazon banned police use of their facial recognition technology, citing lack of federal law on the matter to ensure ethical use.[5] These concerns about ethical use are compounded when taken in conjunction with the longstanding concerns regarding a lack of accountability and ineffective planning and management within Customs and Border Protection.[6] Just this month, the Department of Homeland Security Office of Inspector General found that CBP did not adequately safeguard sensitive data on an unencrypted device used during its facial recognition technology pilot, resulting in a massive data breach that allowed hackers to steal approximately 184,000 facial recognition images and post some on the dark web.[7]

I recognize that the reason the Port Commission is where it is today, deliberating the use of this fraught technology, is because of Customs and Border Protection's (CBP) federal mandate to expedite biometric entry-exit in the wake of 9/11. I further recognize that the Commission is having to do this despite its visible and concerted efforts to make Port facilities welcoming and open to people of all colors and ethnicities and statuses. However, under this administration particularly, CBP has less interest in these same considerations. In fact, under current law, CBP could use an opt-in framework for the technology, but it has instead chosen to make it opt-out.

Because of these concerns, I introduced the Facial Recognition and Biometric Technology Moratorium Act in the House. This bill would:

- Place a prohibition on the domestic use of facial recognition technology by federal entities, which can only be lifted with an act of Congress;
- Place a prohibition on the use of other biometric technologies, including voice recognition, gait recognition, and recognition of other immutable physical characteristics, by federal entities, which can only be lifted with an act of Congress;

[4] Charlie Warzel, *A Major Police Body Cam Company Just Banned Facial Recognition*, New York Times (June 27, 2019) https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html

[5] Jay Greene, *Microsoft Won't Sell Police It's Facial Recognition Technology, Following Similar Moves by Amazon and IBM*, The Washington Post (June 11, 2020) https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/

[6] Department of Homeland Security Office of Inspector General, *CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities* (July 28, 2020) https://www.oig.dhs.gov/sites/default/files/assets/2020-07/OIG-20-55-Jul20.pdf

Daniel E. Martínez, Ph.D., Guillermo Cantor, Ph.D. and Walter Ewing, Ph.D., *No Action Taken: Lack of CBP Accountability in Responding to Complaints of Abuse*, American Immigration Council (May 4, 2014) https://www.americanimmigrationcouncil.org/research/no-action-taken-lack-cbp-accountability-responding-complaints-abuse

[7] Department of Homeland Security Office of Inspector General, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot* (Sept. 21, 2020) https://subscriber.politicopro.com/f/?id=00000174-bc62-dc18-a57d-be63f54f0000&source=email

- Condition federal grant funding to state and local entities, including law enforcement, on those entities enacting their own moratoria on the use of facial recognition and biometric technology;
- Prohibit the use of federal dollars for biometric surveillance systems;
- Prohibit the use of information collected via biometric technology in violation of the Act in any judicial proceedings;
- Includes a private right of action for individuals whose biometric data is used in violation of the Act and allows for enforcement by state Attorneys General; and
- Allow states and localities to enact their own laws regarding the use of facial recognition and biometric technologies.

Given the current landscape, without the guidance of a federal moratoria or even regulations on basic civil liberties protections, I understand that the Port must move forward with setting its own guidance. I commend your efforts to focus on civil liberties concerns, and I applaud your own moratorium on the use of biometrics by Port of Seattle Police. I also support the intention to retain some level of control over CBP's actions by managing use of facial recognition technology for air exit.

With respect to all non-mandated, discretionary uses, I have concerns about any government or private entity use. For that reason, while I agree the Port's guiding principles provide strong guidance for evaluating the use of the technology, I believe we must more seriously consider the fundamental question of *if* the technology should be used at this time. Considering the impacts of facial recognition technology on vulnerable communities and the preserving civil rights and liberties should be the main drivers in the decision-making process regarding this technology. When we act in the best interest of the most vulnerable, with an eye to upholding the rights of all, we are acting in the best interest of everyone.

I understand that in those cases where the Port decides to allow facial recognition technology, the guiding principles are intended to act as safeguards for community members, travelers, and customers. Protections should stay focused on these populations, rather than providing pathways to justify business use. The "justified" principle, for instance, should more critically ask what promise facial recognition technology has in moving us toward a more just society. Currently, facial recognition technology and its uses do not advance justice for people of color, women, children, and seniors and I strongly oppose the use of any tool that further marginalizes vulnerable communities. Each guiding principle should center these communities in use case consideration. Efficiency or cost to businesses cannot be equal to or more important than civil liberties.

As a member of the Port's Biometrics External Advisory Group, I urge you to center the concerns of civil liberties advocates and communities of color in your decisions on the use of facial recognition at the Port of Seattle. I am hopeful that community input will continue to be prioritized to ensure the voices of customers, immigrants, and travelers are heard.

Once again, I commend you on doing all that you can to elevate civil liberties concerns through this process.

Sincerely,

Pramila Jayapal

PRAMILA JAYAPAL
Member of Congress