September 29, 2020

Port of Seattle Commission
2711 Alaskan Way
Seattle, WA 98121

We, as members of the Biometrics External Advisory Group and organizations dedicated to protecting people's rights and civil liberties, urge the Port of Seattle Commission to reject the use of invasive face surveillance technology at Seattle-Tacoma International Airport.

On December 10, 2019, the Commission adopted seven principles to guide its decision-making on if and how biometrics should be used at the Port. These principles are: justified, voluntary, private, equitable, transparent, legal, and ethical.[1]

We do not believe that either the current or the proposed uses of biometrics to identify travelers on Port property can be implemented in a manner consistent with these principles. Port staff state that its recommendations "are not meant to suggest that the Port should implement public-facing biometrics, but rather how to do so in alignment with our guiding principles."[2] The only action that would be aligned with those principles would be to ban the use of facial recognition technology to identify members of the public by the Port, as well as by the Port's tenants and contractors.

We respectfully but strongly disagree with the Port's interpretation and application of each of these principles. For example, the Port states that using facial recognition is "equitable"[3] if it is "accurate in identifying people of all backgrounds"[4] and is "justified"[5] if doing so fulfills a "specific operational need."[6] The undersigned members of the Biometrics External Advisory Group have repeatedly voiced our concerns with such interpretations, noting that even if facial recognition tools were accurate (which they are not), accuracy does not create equity and that increasing efficiencies at the Port does not mean that the use of invasive surveillance technology is justified.

We urge reevaluation of the principles, which should lead to reconsideration of the recommendations that justify the procurement and implementation of facial recognition technology at Seattle-Tacoma International Airport. We have shared that the Port should *not* collaborate with U.S. Customs and Border Protection (CBP) and other entities to implement invasive face surveillance systems.[7] We reiterate that by working with government and private entities to legitimize facial recognition technology, the Port will be facilitating the infrastructural

[1] *December 10, 2019 – Port of Seattle Commission Regular Meeting,* PORT OF SEATTLE (Dec. 10, 2019),
[2] *Biometrics Policy Recommendations Cover Memo*, PORT OF SEATTLE, at 1 (Sept. 25, 2020).
[3] *Motion 2019-13: A Motion of the Port of Seattle Commission*, PORT OF SEATTLE, at 1 (Dec. 10, 2019), https://www.portseattle.org/sites/default/files/2019-12/Motion%202019-13__Biometrics%20Principles.pdf.
[4] *Id.*
[5] *Id.* at 2.
[6] *Id.*
[7] *Open Letter to Port of Seattle Commission*, ACLU OF WASH. (Apr. 8, 2020), https://www.aclu-wa.org/docs/open-letter-port-seattle-commission.

expansion of powerful and racially biased face surveillance systems that threaten our constitutionally protected rights and civil liberties.[8]

Face surveillance systems should not be used by government agencies such as CBP. In announcing a recent lawsuit against CBP and the Transportation Security Administration (TSA), the ACLU stated, "Unlike other forms of identity verification, facial recognition technology can enable undetectable, persistent, government surveillance on a massive scale. As this technology becomes increasingly widespread, the government can use it to track individuals' movements and associations, posing grave risks to privacy and civil liberties. When such a technology is placed in the hands of agencies like CBP and TSA—which have been caught tracking and spying on journalists, subjecting innocent travelers to excessive and humiliating searches, and targeting and interrogating individuals because of their national origin, religious beliefs, or political views—we should all be concerned."[9]

We emphasize that face surveillance systems power systemic racism and injustice—whether or not these systems operate accurately. There is a long and ugly history of government use of surveillance tools to target specific communities. To highlight just a few examples, our government used IBM's Hollerith punched card machines to illegally surveil and incarcerate Japanese-Americans during WWII.[10] More recently, law enforcement used automated license plate readers (ALPR) to religiously profile the Muslim community in a decade-long surveillance program that was eventually struck down as illegal.[11] Today, U.S. Immigration and Customs Enforcement (ICE) is using ALPR and facial recognition technology to track and deport immigrants.[12] It is clear that facial recognition technology provides government agencies with unprecedented surveillance power.

An increasing number of cities across the U.S. including Portland,[13] Boston,[14] and San Francisco,[15] have banned public and private[16] uses of facial recognition technology,

---

[8] Jennifer Lee, *Tell the Port Commission to Push Back Against Face Surveillance,* ACLU OF WASH. (Mar. 9, 2020), https://www.aclu-wa.org/story/tell-port-commission-push-back-against-face-surveillance.

[9] Ashley Gorski, *The Government Has a Secret Plan to Track Everyone's Faces at Airports. We're Suing.*, ACLU (Mar. 12, 2020), https://www.aclu.org/news/privacy-technology/the-government-has-a-secret-plan-to-track-everyones-faces-at-airports-were-suing/.

[10] Matthew Wills, *WWII and the First Ethical Hacker*, JSTOR DAILY (Feb. 14, 2017), https://daily.jstor.org/wwii-and-the-first-ethical-hacker/.

[11] Dia Kayyali, *Third Circuit to the City of New York: Being Muslim is not Reasonable Suspicion for Surveillance,* ELEC. FRONTIER FOUND. (Oct. 15, 2015), https://www.eff.org/deeplinks/2015/10/third-circuit-city-new-york-being-muslim-not-reasonable-suspicion-surveillance.

[12] Catie Edmonson, *ICE Used Facial Recognition to Mine State Driver's License Databases,* N.Y. TIMES *(July 7, 2019),* https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

[13] Portland, Oregon Municipal Code § 34.10. *Available at* https://cdn.vox-cdn.com/uploads/chorus_asset/file/21868277/704_Sep_9_2TC_TW_Ord_BPS_2__1_.pdf.; Press Release, City of Portland, *City Council approves ordinances banning use of facial recognition technologies by City of Portland bureaus and by private entities in public spaces* (Sept. 9, 2020), https://www.portland.gov/bps/news/2020/9/9/city-council-approves-ordinances-banning-use-facial-recognition-technologies-city.

Note: Setting an example that we believe that the Port of Seattle Commission should follow, the Portland City Council considered and rejected a request from the Port of Portland for an exception to the ban to allow use of facial recognition for passenger processing at the Portland International Airport. *See* The Identity Project., *Portland bans facial recognition by city agencies or in places of public accommodation*, PAPERS PLEASE (Sept. 9, 2020), https://papersplease.org/wp/2020/09/09/portland-bans-facial-recognition-by-city-agencies-or-in-places-of-public-accommodation/.

[14] Boston, Massachusetts Municipal Code § 16-62. *Available at* https://www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html.

[15] San Francisco, California Administrative Code - Acquisition of Surveillance Technology. *Available at* https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019

recognizing that face surveillance tools not only fuel discriminatory surveillance but also threaten everyone's privacy and civil liberties. Recent state[17] and federal proposals[18] to ban facial recognition technology have garnered widespread support as legislators and the public have become increasingly concerned about the harmful impacts of face surveillance.

The Port of Seattle Commission has a choice to:

(1) *Reject* collaboration with CBP, a sister agency of ICE, and *not* fund CBP's surveillance systems.
(2) *Prohibit* use of facial recognition technology and *not* facilitate the infrastructural expansion of powerful and racially biased face surveillance technology.
(3) *Reevaluate* the Port's interpretation of and compliance with its principles so that they align with the concerns of marginalized communities.

1. We urge the Port of Seattle Commission to reject participation in, and funding of, CBP's facial recognition exit and entry programs.

On March 10, 2020, Port Commissioners voted unanimously to collaborate with CBP in procuring and implementing its facial recognition program for biometric air exit, and did not take adequate account of the many privacy, civil liberties, and community organizations that urged the Port to reject participation.[19] Instead of listening to serious constituent concerns about the Port participating in CBP's mass collection of biometric data, Commissioners voted to authorize a $5.7 million Request for Proposal (RFP)[20] to procure and implement a "shared-use" facial recognition system at Seattle-Tacoma International Airport.[21]

Though Port Commissioners stated that they had no choice but to vote yes to collaborate with CBP,[22] the Commission did have a choice to say no. Airports and airlines are not mandated to participate in or contribute financially to either CBP's biometric air exit or biometric air entry programs,[23] and furthermore, Congress has never authorized the biometric collection of U.S. citizen data.[24] Without explicit authorization, CBP should not be scanning the faces of Americans as they depart or arrive on international flights, and the Port should not be facilitating this unauthorized scanning.

---

[16] Portland, Oregon Municipal Code § 34.10, *supra* note 13.
[17] H.B. 2856, 66th Leg., Reg. Sess. (Wash., 2020). *Available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/2856.pdf#page=1
[18] Press Release, Ed Markey, Senators Markey And Merkley, And Reps. Jayapal, Pressley To Introduce Legislation To Ban Government Use Of Facial Recognition, Other Biometric Technology (June 5, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.
[19] *March 10, 2020 – Port of Seattle Commission Regular Meeting,* PORT OF SEATTLE (Mar. 10, 2020), https://meetings.portseattle.org/index.php?option=com_meetings&view=meeting&Itemid=358&id=1894&active=play.
[20] *Solicitation Detail: SEA Airport Biometric Air Exit System*, PORT OF SEATTLE (Mar. 16, 2020), https://hosting.portseattle.org/sops/#/Solicitations/Detail/c1451f2a-7544-ea11-8141-005056bd5ab4.
[21] *March 10, 2020 – Port of Seattle Commission Regular Meeting, supra* note 19, at Item 8a Biometric Air Exit Memo.
[22] *Feb 25, 2020 – Port of Seattle Commission Regular Meeting*, PORT OF SEATTLE (Feb. 25, 2020), https://meetings.portseattle.org/index.php?option=com_meetings&view=meeting&Itemid=358&id=1892&active=play.
[23] Marc Rotenberg et al., *Comments of the Electronic Privacy Information Center to the Department of Homeland Security Data Privacy and Integrity Advisory Committee*, EPIC (Dec. 10, 2018), https://www.epic.org/apa/comments/EPIC-Comments-DHS-DPIAC-Face-Rec-ReportDec-2018.pdf.
[24] *See* Harrison Rudolph et. al, *Not Ready for Takeoff: Face Scans at Airport Departure Gates*, GEO. L. CTR ON PRIV. & TECH. (Dec. 21, 2017), https://www.airportfacescans.com/.

Additionally, we disagree with the Port's conclusion that the Port's participation in CBP's face surveillance program will give the Port greater control over the program's implementation. Commissioners state that by owning and operating the facial recognition systems in use, the Port will be able to provide the public with clear signage, increasing the opportunity for informed consent and mitigating harm from CBP's activities.[25] Unfortunately, the Port's decision to work with CBP will have exactly the opposite effect. By voting to authorize the RFP on March 10, 2020, Commissioners agreed to comply with CBP's "Biometric Air Exit Business Requirements," which require the Port to install only CBP-approved signage, even if the signage is misleading or incorrect.[26] The Port would have more power to mitigate harm and provide the public with clear signage by rejecting participation in CBP's facial recognition program.

Our state has sent a clear message against Washington's collaboration with CBP. Over the past two years, Washington's state legislature has passed the Keep Washington Working Act and the Courts Open to All Act, which together prohibit state agencies, local law enforcement, and court stakeholders from collaborating with CBP.[27] The Port of Seattle Commission would be better aligned with statewide work in Washington by rejecting collaboration with CBP in its procurement and implementation of face surveillance systems.

We urge the Port of Seattle Commission to reverse its decision to participate in CBP's biometric air exit program. Additionally, we urge the Commission to vote no and reject participation in CBP's biometric air and cruise entry program.

2. We urge the Port of Seattle Commission to prohibit use of facial recognition technology by private entities.

The Port of Seattle should prohibit business tenants such as airlines from integrating with CBP's Traveler Verification Service (TVS)—the agency's "Identity as a Service" biometrics system.[28] The Port should not enable private industry to aid the Department of Homeland Security (DHS) and CBP (DHS's largest law enforcement agency) by allowing it to implement biometrics using CBP's TVS. When Port tenants integrate with CBP's TVS architecture, it is impossible to separate "private" or non-federal surveillance from federal government surveillance of travelers. Travelers may think that they are having their photo taken at a self-service kiosk solely for use by the airport or airline. But in reality, that photo will also be shared with DHS and CBP.

The Port, airlines, and contractors should not obscure the role of DHS and CBP by collecting facial images on their behalf. The Privacy Act,[29] as discussed further below, *requires* that if an individual's personal information is to be used by a federal agency, it must be collected by that

---

[25] *March 10, 2020 – Port of Seattle Commission Regular Meeting, supra* note 19.
[26] *Biometric Air Exit Business Requirements Version 2.0*, U.S. CUSTOMS AND BORDER PROTECTION, at 9, Item 8 (Jan. 2020), https://www.cbp.gov/sites/default/files/assets/documents/2020-Jul/Exit%20BRD2__Redacted_0.pdf.
[27] *See* Keep Washington Working, E.2.S.S.B 5497, 66th Leg., Reg. Sess. (Wash., 2019). *Available at* http://lawfilesext.leg.wa.gov/biennium/2019- 20/Pdf/Bills/Session%20Laws/Senate/5497-S2.SL.pdf?q=20200401125832.; *See* Courts Open to All, S.H.B. 2567, 66th Leg., Reg. Sess. (Wash., 2020). *Available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/House/2567-S.SL.pdf?q=20200401094053.
[28] *Biometric Air Exit Business Requirements Version 2.0*, *supra* note 26.
[29] 5 U.S.C. § 552a (2010). *Available at* https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf.

agency directly from that individual. The best way to provide travelers with clear notice that facial images are being passed on to DHS is to require that any such images be collected by identifiable, uniformed DHS staff, using DHS equipment, at DHS's expense.

The Port has significant control over whether and how private companies can implement biometrics at Port facilities, and it should exercise this control to prohibit private entity collaboration with DHS and CBP.

Additionally, the Port should prohibit private entities from using private-sector proprietary facial recognition systems at Port facilities. We are alarmed that the recommendations from Port staff highlight potential use of facial recognition for purposes including, but not limited to, targeted advertising using dynamic signage, payment at retail stores or restaurants, access to rental cars or airline passenger lounges, ticketing and bag check, and boarding of departing flights and cruise ships.[30] The Port should reject the infrastructural expansion of face surveillance—not invite it in.

We emphasize that use of face surveillance systems will inevitably have disparate impacts on marginalized groups, whether or not the technology operates accurately. However, it is important to recognize that inaccurate and biased facial recognition systems have in many cases, life-or-death consequences. Use of face surveillance has implicated people in crimes they have not committed, as in the case of Robert Julian-Borchak Williams, a Black man who was wrongly arrested and jailed due to a false facial recognition match.[31] Indeed, multiple expert studies have found facial recognition technology to be less accurate at identifying women, youth, trans and gender non-conforming people, and people of color, increasing the risk of false matches. A December 2019 study from the National Institute of Standards and Technology on Face Recognition Software found that false positives are up to 100 times more likely for Asian and African faces when compared to white faces.[32] We underscore that facial recognition causes disparate impacts when it is inaccurate, and it will also lead to harm even if perfectly accurate, as the technology will continue to be deployed disproportionately to surveil marginalized communities.

Finally, it is important that the Port prohibit its tenants from using proprietary facial recognition systems because private surveillance often fuels government surveillance. With companies frequently building and equipping government agencies with face surveillance tools, as well as with the information gathered from such tools, it has become increasingly difficult to distinguish between private and government surveillance. For example, companies such as Clearview AI have provided facial recognition services to thousands of companies as well as to government agencies like ICE.[33] Allowing private entities to use proprietary facial recognition systems at Port facilities will bolster both private and government use of invasive face surveillance technology.

---

[30] *Port of Seattle Public-Facing Biometrics Policy: Biometrics For Traveler Functions by Private Sector Entities Using Proprietary Systems Recommendations,* PORT OF SEATTLE, at 6 (July 24, 2020), https://www.portseattle.org/sites/default/files/2020-08/Public_Facing_Biometrics_for_Traveler_Functions_Using_Private_Propietary_Systems_DRAFT_200724.pdf.

[31] Kashmir Hill, *Wrongfully Accused by an Algorithm,* N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[32] Patrick Grother et al., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, U.S. DEP'T. OF COM., NAT'L INST. OF STANDARDS & TECH. (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[33] Kim Lyons, *ICE just signed a contract with facial recognition company Clearview AI*, THE VERGE (Aug. 14, 2020) https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration.

Many people are recognizing that private uses of face surveillance are as concerning as government uses. Recently, Portland became the first jurisdiction to ban private entity use of facial recognition technologies in places of public accommodation—which includes airports.[34] The Port of Seattle should follow suit and ban private entity use of facial recognition technologies at Seattle-Tacoma International Airport.

3. We urge the Port of Seattle to reevaluate its interpretation of and compliance with its principles.

The undersigned members of the Biometrics External Advisory Group have repeatedly raised serious concerns with the Port's interpretation of the seven principles it has adopted to guide its decision-making on biometrics.

I. Justified

The Port states that facial recognition use is "justified" if the technology is used only for a clear intended purpose, it furthers a specific operational need or benefit, and it is not used for "mass surveillance."[35]

First, use of a surveillance tool is not justified just because it is used for a clear and intended purpose. Even if the intended purpose is ostensibly innocuous, use of powerful surveillance technologies can pose risks to people's civil rights and civil liberties. For example, recently in San Diego, police looked for Black Lives Matter protesters by searching records of smart streetlights. These streetlights were originally pitched as a way to gather pedestrian and vehicle data for the purpose of city planning. However, these streetlights have increasingly served the purpose of law enforcement, as evidenced by San Diego Police Department using this footage to surveil and prosecute protesters.[36]

Second, the Port's definition of "justified" conflates operational benefit and operational need. For some use cases, such as biometric air and cruise entry, the recommendations state that "justified" means meeting an operational need,[37] and in other use cases such as for private proprietary systems, the recommendations state that "justified" means creating an operational benefit.[38] However, all use cases, including the use of facial recognition for air exit, air and cruise entry, and targeted advertising are apparently benefit-based rather than operationally necessary. "Operational need" implies that facial recognition is essential to operations. This is not the case for any of the use cases proposed.

Third, the Port states that use of facial recognition is justified if it is not used for "mass surveillance." However, the Port has too narrowly defined "mass surveillance" as "scanning

---

[34] *See* San Francisco, California Administrative Code - Acquisition of Surveillance Technology, *supra* note 15.
[35] *Motion 2019-13: A Motion of the Port of Seattle Commission*, *supra* note 3, at 1-2.
[36] Jesse Marx, *Police Used Smart Streetlight Footage to Investigate Protesters., Voice* of San Diego (June 29, 2020), *https://www.voiceofsandiego.org/topics/government/police-used-smart-streetlight-footage-to-investigate-protesters/*
[37] *Biometrics Policy Recommendations Cover Memo*, *supra* note 2, at 57.
[38] *Id.* at 15.

large groups of people without lawful purpose, rather than use on one person at a time with their active participation."[39] Logging of individuals' movements and when, where, how and with whom they travel, whether by air or sea or otherwise, is *per se* surveillance. "Surveillance," or "the act of observing persons or groups,"[40] does not depend on whether or not it is done overtly or covertly—both can constitute an invasion of privacy. The Port's proposed use of facial recognition for biometric entry/exit and its proposal to allow private entities to use both government and proprietary facial recognition systems would be considered "mass" or "bulk" surveillance as defined by academics,[41] technical experts,[42] and governmental entities.[43] Mass surveillance can in some cases be lawful and overt, but still pose threats to people's privacy and civil liberties.

II. Voluntary

The Port states that facial recognition use is "voluntary" if an "opt-in or "opt-out" procedure is provided and unintended image capture is prevented.[44]

However, as previously noted, the Port's participation in CBP's biometric air exit program expressly prohibits the Port from having control over signage to notify people of their right to not have their face surveilled. Even though U.S. citizens technically have the right to opt out of CBP's face surveillance programs, CBP has frequently failed to provide accurate information to travelers regarding their opt-out rights.

A recent report by the Government Accountability Office (GAO) found that CBP's privacy notices—which are intended to provide travelers with information on procedures to opt out—"were not always current or complete, provided limited information on how to request to opt

---

[39] *Id.* at 31.

[40] *Surveillance: Definition from Nolo's Plain-English Law Dictionary,* LEGAL INFO. INST., https://www.law.cornell.edu/wex/surveillance (last visited Sept. 24, 2020).

[41] Seda Gürses, Arun Kundnani, and Joris Van Hoboken, *Crypto and Empire: The Contradictions of Counter-surveillance Advocacy*, 38 MEDIA, CULTURE & SOC'Y 576 (2016). *Available at* https://journals.sagepub.com/doi/abs/10.1177/0163443716643006.

[42] "Based in part on briefings from the IC [Intelligence Community], the committee adopted a definition better suited to understanding the trade-off between civil liberties and effective intelligence: If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted." From National Research Council, *Bulk Collection of Signals Intelligence: Technical Options* 2 (2015). *Available at* https://www.microsoft.com/en-us/research/uploads/prod/2019/09/Bulk-Collection-of-Signals-Intelligence.pdf.

[43] "On 9 March 2004, the European Parliament (2004) declared that any form of mass surveillance was unjustified and that only targeted measures were justifiable. Targeted surveillance refers to the surveillance of a specific individual (or individuals) on a case-by-case basis, based on reasonable suspicion (or probable cause). This type of surveillance was only authorized if it included appropriate safeguards such as the requirement of search warrants or court orders. Any measure that did not meet these requirements of surveillance is - and in the case of the European Parliament was - considered unjustified." ... "Shortly after the Madrid bombings (which occurred on 11 March 2004), however, this view changed. The European Council (2004)'s statement, in the Declaration on Combating Terrorism (adopted on the 25th of March 2004), on the urgency and necessity to adopt measures of mass surveillance clearly attests to this. In particular, the Declaration on Combating Terrorism called for the creation of "passenger name record" (PNR) checks on all flights in and out of the European Union (whereby the personal information of passengers is recorded, stored and transferred to authorities in the United States upon request), IDs, visas, and passports with biometric identifiers (e.g. digital fingerprints and retinal scans), and the wide retention of communications data. The mass surveillance of movement (PNR and biometric IDs) and of communications (data retention) were now all said to be justified." From Marie Helen Maras, *The social consequences of a mass surveillance measure: What happens when we become the 'others'?,* 40 INT'L JOURNAL OF LAW, CRIME, AND JUSTICE 65 (2012) *Available at* https://www.sciencedirect.com/science/article/abs/pii/S175606161100070X.

[44] *Motion 2019-13: A Motion of the Port of Seattle Commission*, *supra* note 3, at 2.

out of facial recognition, and were not always available."[45] The GAO also found that some of CBP's privacy notices were outdated and contained wrong or inconsistent information.[46] Moreover, there have been documented cases where individuals have been denied their right to opt-out. For example, in December 2019, a CBP officer incorrectly told an ACLU attorney crossing from Mexico into the U.S. that he did not have the right to opt out of biometric air entry.[47]

Furthermore, some academics argue that valid consent is not even possible in the context of face surveillance. Researchers Selinger and Hartzog have stated that "[o]ne reason consent to facial recognition is highly suspect is that people do not and largely cannot possess an appropriate level of knowledge about the substantial threats that facial recognition technology poses to their own autonomy… Even if some people withhold consent for face surveillance, others will inevitably give it. Rules that facilitate this kind of permission will normalize behavior, entrench organizational practices, and fuel investment in technologies that will result in a net increase of surveillance. Expanding a surveillance infrastructure will increase the number of searches that occur which in itself, will have a chilling effect over time as law enforcement and industry slowly but surely erode our collective and individual obscurity."[48]

III. Private

The Port states that facial recognition is "private" if data collected by facial recognition technology are stored only if needed, for no longer than required by law, and protected from unauthorized access.[49]

However, abiding by minimum data protection standards does not mean that the Port's use of facial recognition technology provides people with adequate privacy. In Biometrics External Advisory Group meetings, the Port has admitted that it has no control over what CBP does with the data it collects and with whom it shares the data.

CBP claims that airlines will be restricted in their retention and use of facial images by contracts with CBP. But none of those contracts have been disclosed, even when requested pursuant to the Freedom Of Information Act.[50] According to the aforementioned GOA report, "as of May 2020, CBP had audited only one of its more than 20 commercial airline partners and did not have a plan to ensure that all partners are audited for compliance with the program's privacy requirements."[51] It does not appear that the Port has audited, or would have any way to audit, compliance with contracts between airlines and CBP. Additionally, such contracts would be enforceable only by CBP itself, not by the Port or third parties.

---

[45] *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, U.S. GOV'T ACCOUNTABILITY OFFICE, at 39 (Sept. 2020), https://www.gao.gov/assets/710/709107.pdf.
[46] *Id.* at 39- 40
[47] Shaw Drake, *A Border Officer Told Me I Couldn't Opt Out of the Face Recognition Scan. They Were Wrong.*, ACLU (Dec. 5, 2019), https://www.aclu.org/news/immigrants-rights/a-border-officer-told-me-i-couldnt-opt-out-of-the-face-recognition-scan-they-were-wrong/
[48] Evan Selinger and Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOYOLA LAW REVIEW 101 (2020), Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557508.
[49] *Motion 2019-13: A Motion of the Port of Seattle Commission*, *supra* note 3, at 2.
[50] *See* Edward Hasbrouck, Unanswered FOIA request to CBP, PAPERS PLEASE (July 16, 2018), https://papersplease.org/wp/wp-content/uploads/2018/07/biometric-partnership-FOIA.pdf.
[51] *Facial recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, *supra* note 46.

Given all of the above, it cannot be said that the recommendations for the proposed uses of facial recognition will protect people's privacy.

IV. Equitable

The Port states that facial recognition use is "equitable" if it is "reasonably accurate at identifying people of all backgrounds," and if systems are in place to treat mismatching issues.[52]

First, we reiterate that equity cannot be simplified as accuracy. Face surveillance systems fuel systemic racism and discriminatory policing, whether or not these systems operate accurately.

Second, under the Port's definition of "equitable," it is unclear at what level of accuracy it will be acceptable to use facial recognition. Relative differences in accuracy rates between different groups may lead to discrimination, even if the system is "highly accurate," on average.

V. Transparent

The Port states that facial recognition use is "transparent" if use of biometric technology for passenger processing at Port facilities is communicated to visitors and travelers and if individuals are notified about any collection of their biometric data and how that data may be used. The Port also states that reports on the performance and effectiveness of the technology should be made public.[53]

However, facial recognition use cannot be truly transparent unless the Port knows and can share with the public with which entities people's data are being shared and for what purposes people's data are being used. Unfortunately, because the Port cannot know what CBP does with people's data and with which third parties the data are shared, the Port cannot guarantee transparency.

VI. Lawful

The Port states that facial recognition is lawful if use complies with all laws including privacy laws and laws prohibiting discrimination or illegal search against individuals or groups.[54]

The Port or the Port's airline tenants collaborating with CBP would likely violate the Privacy Act, a federal law mandating that data be collected directly from individuals by a federal agency if the data are used as part of the basis of making decisions about access to federal rights and privileges (such as federally-licensed air travel).[55]

The Privacy Act also prohibits collection of information concerning the exercise of rights protected by the First Amendment without *explicit* statutory authorization. The First Amendment protects "the right of the people peaceably to assemble"[56] and records of when,

---

[52] *Motion 2019-13: A Motion of the Port of Seattle Commission*, *supra* note 3, at 2.
[53] *Id.*
[54] *Id.*
[55] 5 U.S.C. § 552a (2010), *supra* note 29.
[56] U.S. Const. amend. I. *Available at* https://constitution.congress.gov/constitution/amendment-1/.

where, and with whom we travel are records of how we exercise rights protected by the First Amendment. Neither CBP nor TSA has explicit statutory authority to collect facial images of U.S. citizens or domestic travelers, and thus, collection of this information is prohibited by the Privacy Act.

By collecting facial images and sending them to CBP, the Port or airlines operating at the Port would potentially be complicit in CBP's violation of federal law. The Port should not facilitate CBP's unlawful outsourcing of personal data collection.

VII. Ethical

The Port states that facial recognition use is "ethical" if actions respect key moral principles that include honesty, fairness, equality, dignity, diversity, and individual rights.

Respectfully, there are serious ethical questions regarding collaboration with CBP, an agency with a long history of abuse,[57] to build a powerful surveillance system. Face surveillance systems violate everyone's privacy, and especially violate the dignity and rights of communities that continue to be targeted by law enforcement. Expanding face surveillance systems will exacerbate systemic racism. In order to abide by this principle, the Port should refuse to collaborate with CBP and reject facilitating the growth of both private and government face surveillance infrastructure.

We urge the Port of Seattle Commission to reject collaboration with CBP, prohibit all use of facial recognition technology at Seattle-Tacoma International Airport, and reevaluate its interpretation of and compliance with the aforementioned principles guiding decision-making on if and how biometrics should be used at the Port.

Signed,

ACLU of Washington
Advocacy for Principled Action in Government
Asia Pacific Cultural Center
Asian Counseling and Referral Service (ACRS)
Casa Latina
Church Council of Greater Seattle
Coalition of Seattle Indian-Americans
Council on American Islamic Relations Washington (CAIR-WA)
Densho
Eastside for All
El Centro de la Raza
Electronic Privacy Information Center (EPIC)
Entre Hermanos
Faith Action Network (FAN)
Fight for the Future

[57] *US: Stop Using Untrained, Abusive Agencies at Protests,* HUMAN RIGHTS WATCH (June 5, 2020), https://www.hrw.org/news/2020/06/05/us-stop-using-untrained-abusive-agencies-protests.

Freedom to Read Foundation
Indivisible Eastside
Indivisible Plus Washington
Indivisible Whidbey
InterIm Community Development Association (InterIm CDA)
Japanese American Citizens League (JACL) – Seattle Chapter
John T. Williams Organizing Committee
La Resistencia
Latino Community Fund of Washington
Legacy of Equality Leadership & Organizing (LELO)
MAPS-AMEN (American Muslim Empowerment Network)
MediaJustice
Mijente
Northwest Immigrant Rights Project
OneAmerica
Planned Parenthood Votes Northwest and Hawai'i
Puget Sound Sage
Real Change
The Identity Project
Transit Riders Union
Urban League of Metropolitan Seattle
Washington Association of Criminal Defense Lawyers (WACDL)
Washington Defender Association (WDA)