Port
of Seattle

PORT OF SEATTLE PUBLIC-FACING BIOMETRICS POLICY

BIOMETRIC AIR EXIT RECOMMENDATIONS

VERSION AS APPROVED BY THE PORT COMMISSION ON MARCH 10, 2020

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Biometrics is the measurement and analysis of physical and behavioral characteristics that are used to identify individuals through technology. Examples of physical characteristics include the unique features of an individual's face or their fingerprint, while examples of behavioral characteristics includes an individual's voice, signature, or how they walk.

Due to technological advances, perceived customer benefits and federal requirements, there is a significant increase in public-facing facial recognition technology deployment by public and private sector users, including in airport and seaport settings. In fact, U.S. Customs and Border Protection (CBP) is Congressionally mandated to implement a biometric exit and entry screening process for all international passengers.

Facial biometrics are already being used at dozens of U.S. airports and cruise terminals by those who see the technology as a major benefit to travelers – both because of a faster and more efficient travel experience, as well as a more accurate security process. However, many members of the public and various advocacy organizations have expressed concerns about the rapidly expanding use of facial recognition. These stakeholders have raised issues around privacy, equity and civil liberties, as well as the potential for unregulated "mass surveillance."

Public-facing biometrics are already used in various forms at the Port of Seattle's aviation and maritime facilities, such as 1) CLEAR, a private company providing an option to those customers who want expedited screening at U.S. Transportation Security Administration (TSA) checkpoints to voluntarily supply their biometric data in order to verify their identities, 2) CBP's use of biometrics at Seattle-Tacoma International Airport (SEA)[1] to validate departing international traveler identities, and 3) Norwegian Cruise Line use of biometrics on ship while docked at Pier 66 to validate the identities of disembarking passengers. CBP will also use facial recognition technology to screen almost all arriving international passengers once SEA's International Arrivals Facility (IAF) opens in the coming year.

In advance of any expansion of biometric uses at Port of Seattle facilities by the Port or its private sector tenants, the Port of Seattle Commission desires to develop proper policy frameworks and clear guidelines to reduce potential misuse and abuse of biometrics, while improving public understanding of the benefits and risks of this technology in various applications. On December 10, 2019, after holding two Study Sessions, conducting stakeholder outreach and doing multiple site visits, the Port Commission adopted seven "biometrics guiding principles," and directed staff to translate those principles into tangible, enforceable policies. Specifically, the Port strives to balance operational needs, business priorities and regulatory mandates with protections for the interests and rights of passengers, employees and other visitors to our facilities.

Over the last three months, a working group of Port staff has collaborated with an external advisory group of key stakeholders to accomplish that task. **One of the key findings from this process is that the various use cases of biometrics require separate analysis as to how the Port should (consistent with local, state and federal requirements) apply the biometrics guiding principles to develop policy.** One unified set of policies is not practical because of key differences from one use case to another, such as who manages the data, requirements imposed by state or federal law, and the benefits and risks associated with each use.

---

[1] On certain departing Lufthansa, Hainan, Emirates and Virgin Atlantic flights

This set of recommendations is specific to "biometric air exit," which is the use of facial recognition by CBP, the Port and/or airlines as part of CBP's Traveler Verification Service (TVS) to validate the identities of departing international airline passengers as they board the aircraft. *Throughout this document, "biometrics" and "facial recognition" will be used interchangeably because CBP's biometric exit and entry uses facial recognition technology.*

The recommendations that have resulted from the working group and external advisory group process are listed below, along with concerns from some external advisors who do not support some of these recommendations. All sides of the discussion are represented here to provide Port Commissioners full information prior to adoption of any policies. Additional recommendations for other use cases will be similarly provided.

2. INTRODUCTION

The goal of the Port's Biometric Working Group is to translate the seven biometrics principles adopted by the Port Commission into tangible, enforceable policies that ensure, to the greatest extent possible, that the use of public-facing biometrics at Port facilities conform to these principles.

It is important to note that the Port has broad authority to establish policies that govern the activities of Port staff and the use of Port resources, to the extent such policies are consistent with federal law. Private sector stakeholders operating at Port facilities (such as airlines) are also subject to the Port's policies, to the extent that the Port's policies do not conflict with private stakeholders' own federal obligations and/or the terms of their agreements with the Port – such as lease agreements or operating agreements with the Port, which may vary on a case-by-case basis. *The Port has very limited authority to influence, much less direct, the activities of federal agencies operating at Port facilities.*

The recommendations below are specific to biometric air exit, which is the use of facial recognition by the Port, airline tenants, and/or by CBP itself as part of CBP's Traveler Verification Service to confirm the identities of departing international airline passengers as they board their aircraft. It is important to note that CBP not only has the authority to implement biometric air exit at SEA without Port agreement, but that this is already taking place and continuing to expand. *CBP is using facial recognition for departing international passenger at SEA on departing Lufthansa, Hainan, Emirates and Virgin Atlantic flights; therefore, the ultimate decision for the Port Commission is whether the Port wants CBP to continue to conduct this activity at our airport, or whether they would prefer Port and/or airline staff conduct these screenings (using Port-dictated policy guidelines).*

In this document, Port staff has endeavored to recommend policies of general applicability wherever possible; however, some recommendations are divided into 1) recommendations that apply to the Port, 2) recommendations that apply to airlines, and 3) recommendations related to CBP. Where the Port lacks authority to mandate compliance with particular policies, the recommendation is to work collaboratively with these stakeholders to achieve voluntary compliance where appropriate, and/or highlight how these stakeholders' own policies match Port principles. The Port should also advocate for the adoption of new laws and regulations that align with the Port's biometric principles.

Finally, while the recommendations below represent the thinking of Port staff, there is not consensus among all members of the Port's External Advisory Group on these recommendations. Therefore, stakeholder concerns about each recommendation are also included below so that the Port Commission can consider all perspectives before they adopt any final policies. Ultimately, the Port Commission is the governing body that can approve any recommendations.
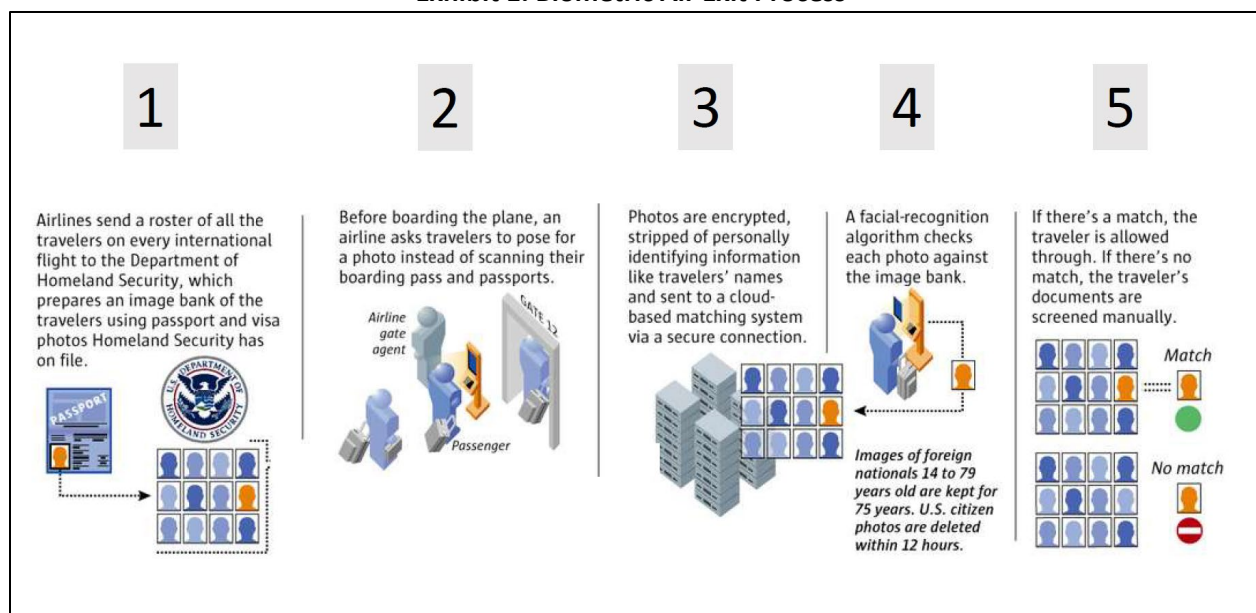
3. BASICS OF BIOMETRIC AIR EXIT

Biometric air exit is primarily intended to realize CBP's goal of determining whether foreign nationals have overstayed their authorized periods of admission, as well as to confirm whether the departing individual is truly the same person who entered the United States. Currently, this process relies upon passenger information provided by airline carriers through CBP's Advance Passenger Information System (APIS), which is then matched to the entry data collected by CBP officers at the time that a foreign national was admitted to the United States.

Direction for CBP to move to biometric data collection originated as a recommendation of the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission. In its final report, the 9/11 Commission concluded that "funding and completing a biometric entry-exit screening system for travelers to and from the United States is essential to our national security." Based on the 9/11 Commission's recommendations, Congress included biometric entry/exit provisions in the Intelligence Reform and Terrorism Prevention Act of 2004. The FY 2013 Consolidated and Further Continuing Appropriations Act transferred entry/exit policy and operations to CBP. In addition, the FY 2016 Consolidated Appropriations Act authorized funding for a biometric exit program costing up to $1 billion to be collected through fee surcharges over a period of 10 years. More recently, President Trump included direction to expedite completion of this transition to biometric identification in section 7 of Executive Order 13769, which is known as the Muslim ban or travel ban: "The Secretary of Homeland Security shall expedite the completion and implementation of a biometric entry-exit tracking system for all travelers to the United States, as recommended by the National Commission on Terrorist Attacks Upon the United States."

CBP has begun implementing its biometric exit program through its development of the Traveler Verification Service (TVS) and associated pilot programs. TVS is essentially a system of related databases hosted by CBP, containing the biometric facial recognition "template" of individuals that are ticketed on international flights. These templates are based on images previously collected by CBP or other federal agencies, such as from passport or visa application photos. TVS allows CBP and/or one of its authorized partners (i.e. – airports or airlines) to deploy camera systems that capture an image of an individual and send the image to CBP, along with the person's flight information, for processing. CBP attempts to match the image to its "gallery" of biometric templates for that particular flight and, if it confirms a match, transmits a "match/no match" confirmation back to the partner.

Exhibit 1. Biometric Air Exit Process

1 Airlines send a roster of all the travelers on every international flight to the Department of Homeland Security, which prepares an image bank of the travelers using passport and visa photos Homeland Security has on file.

2 Before boarding the plane, an airline asks travelers to pose for a photo instead of scanning their boarding pass and passports.

Airline gate agent

Passenger

3 Photos are encrypted, stripped of personally identifying information like travelers' names and sent to a cloud-based matching system via a secure connection.

4 A facial-recognition algorithm checks each photo against the image bank.

Images of foreign nationals 14 to 79 years old are kept for 75 years. U.S. citizen photos are deleted within 12 hours.

5 If there's a match, the traveler is allowed through. If there's no match, the traveler's documents are screened manually.

Match

No match

Reprinted from The Seattle Times

It is important to note that airports and airlines are not currently mandated to participate in CBP's biometric air exit program. Of the two dozen airports and airlines that have partnered with CBP to

implement biometric air exit, all of them have joined the program voluntarily because they believe it improves customer facilitation and homeland security.

Authorized users of TVS are required by CBP to comply with a set of business requirements. For example, each camera must be connected to the TVS via a secure, encrypted connection, and each CBP's partner's IT system must allow CBP to audit compliance with these requirements.

The biometric air exit program is only used at departure gates and only when international departing flights are boarding. It is worth noting that, if an airport or airline does not choose to partner with CBP to implement biometric air exit, CBP has authority to implement the program using its own staff and equipment at any international air departure gate. This is already occurring at SEA on certain departing Lufthansa, Hainan, Emirates and Virgin Atlantic flights.

It is also worth noting that TVS is not limited to the biometric air exist use case; for example, TVS can also be used for other traveler identity verification functions, such as curb-to-gate implementations (where international departing passengers' identity can be used to facilitate ticketing, bag check and TSA screening as well). This set of recommendations considers only the use of TVS in support of biometric air exit. With respect to the biometric air exit use case, as with any other use case utilizing TVS, the Port will have limited visibility into (and no authority over) the design of the CBP-provided TVS system.

CBP has stated that its biometric air exit program fully aligns with the Port's Biometrics Principles. The agency details its thoughts on this topic in the letter agency officials sent the Port Commission in December 2019, attached as Appendix D.

4. APPLYING THE PORT'S PUBLIC-FACING BIOMETRICS GUIDING PRINCIPLES TO BIOMETRIC AIR EXIT

a. Justified

The Port Commission's Biometrics Motion states that:

> *Biometric technology at port facilities should be used only for a clear intended purpose that furthers a specific operational need. The port does not condone biometrics for "mass surveillance" – for example, use of facial recognition on large groups of people without a lawful purpose, rather than single-use for travelers.*

1. Key Issues to address

The Justified principle essentially speaks to two key issues of concern: 1) requiring an explicitly articulated operational need in order to approve the use of biometrics, and 2) ensuring that biometrics are not used for "mass surveillance" at Port facilities. The Commission motion defines mass surveillance as scanning large groups of people without lawful purpose, rather than use on one person at one time with their active participation.

As it relates to a specific operational need, travel document checks are a well-established activity in connection with the boarding of an aircraft on an international itinerary. That is why CBP refers to biometric air exit as the automation of an existing verification process. CBP is already provided information about every person boarding a departing international aircraft by airlines, and CBP has the

picture of most travelers from U.S. passport or foreign visitor visa application photos. CBP and Congress have determined that biometric air exit is operationally necessary to ensure national security and ensure compliance with immigration laws.

Biometric air exit is not mass surveillance. Biometric air exit captures an image of individuals with their awareness and active participation, which aligns with the Commission's definition. Recommendations for protecting against unintended image capture of other individuals are included under the Voluntary principle.

Finally, the Port should have a process in place for reviewing and approving airport or airline requests to implement biometric air exit systems, as referenced throughout the recommendations in this document, in order to ensure that each implementation complies with the Port's Biometrics Principles to the greatest extent possible.

2. Working Group Recommendations

"Justified" recommendations at a glance		
Port	Airline	Federal
If staff makes request to implement biometric air exit program, approval must come from the Aviation Managing Director (AMD) after the AMD has notified the Port ED and Port Commission. *If request requires Commission authorization*, memo to Commission must explain alignment with Biometric Principles. *If procurement process is required*, request information on alignment with Biometric principles. If the Port implements a "common use" biometric air exit solution, it must be used for all departing international flights at SEA.	*If airline makes request* to implement biometric air exit program, approval must come from the Aviation Managing Director after the AMD has notified the Port ED and Port Commission with an explanation how the proposed implementation aligns with all relevant principles.	The port does not have jurisdiction to approve or reject CBP decisions regarding use case implementation. *If CBP plans to implement or expand biometric exit at SEA,* they should notify the Port in advance.

For Port

Recommendation 1a: Port staff who request implementation of a common use[2] biometric air exit system at SEA gates used for international departing flights must receive approval from the Aviation Managing Director before proceeding with the procurement process, including by providing an explanation as to how it will comply with the Port's Biometric Principles and Biometric Air Exit Policies. Staff must also provide documentation that their proposed process is compliant with CBP's Biometric Air Exit Requirements[3] and TVS application programming interface (API) specifications[4].

Recommendation 2a: If the proposed implementation of biometric air exit by Port staff does not require a Commission authorization[5], then the Aviation Managing Director must notify the Port Executive Director and the Port Commission before approving the request. This notification must be at least three (3) weeks in advance of any staff action. The Aviation Managing Director must consider the following criteria in deciding whether or not to approve the implementation:

- Demonstrated operational benefit, which is defined as an added increased efficiency or effectiveness in passenger processing vs existing manual processes
- Compliance with all Port principles and policies
- Compliance will all CBP requirements
- Net benefit-cost to travelers – both overall and for specific subsets of travelers – of the added customer facilitation vs. potential privacy and other risks

The Managing Director should also seek feedback from the Technology Ethical Advisory Board, once it is established (see recommendation under Ethical).

Recommendation 3: If the requested implementation of biometric air exit by Port staff requires a Commission authorization[6], then the Commission memo must include a justification as to how the proposal complies with the Port's Biometric Principles and Biometric Air Exit Policies, as well as a recommendation from the Aviation Managing Director on how and why this request meets the Justified principle.

Recommendation 4: If the proposed implementation of biometric air exit by Port staff requires a procurement, then the vendor solicitation document must include a request for explanation of how the technology will comply with the Port's Biometric Principles and Biometric Air Exit Policies, as well as CBP's Biometric Air Exit Requirements.

Recommendation 5: If the Port implements a common use biometric air exit solution, it must be used for all departing international flights at SEA; any previously approved biometric air exit solutions implemented by individual airlines will be removed and replaced by the Port's selected technology.

For Airlines
Recommendation 1b: An airline requesting to implement biometric air exit at SEA gates used for international departing flights must receive approval from the Aviation Managing Director and provide an explanation as to how the implementation will comply with the Port's Biometric Principles and

---

[2] Meaning that the airport would provide technology that is then used by whatever airlines is using the departure gate for a departing international flight.
[3] Available upon request via https://portofseattle.nextrequest.com/requests/new
[4] Available upon request via https://portofseattle.nextrequest.com/requests/new
[5] Commission authorization is required for procurements valued at or above $300,000.
[6] Ibid.

Biometric Air Exit Policies. The airline requesting to implement biometric air exit at SEA gates must provide documentation that its proposed process has been approved by CBP, specifically documenting compliance with CBP's Biometric Air Exit Requirements[7] and TVS API specifications[8].

Recommendation 2b: The Aviation Managing Director must notify the Port Executive Director and the Port Commission before approving an airline request for biometric air exit, with an explanation of how the proposal complies with the Port's Biometrics Principles. This notification must be at least three (3) weeks in advance of any staff action. The Aviation Managing Director must consider the following criteria in deciding whether or not to approve the implementation:

- Demonstrated operational benefit, which is defined as increased efficiency or effectiveness in passenger processing vs existing manual processes
- Compliance with all Port principles and policies
- Compliance will all CBP requirements
- Net benefit-cost to travelers – both overall and for specific subsets of travelers – of the added customer facilitation vs. potential privacy and other risks

The Managing Director should also seek feedback from the Technology Ethical Advisory Board, once it is established (see recommendation under Ethical).

For CBP
Due to both practical and legal considerations, the Port may not deny CBP the right to implement biometric air exit at SEA using CBP's own staff and resources. However, because CBP would be making use of Port-controlled facilities to deploy biometric air exit, it is reasonable to ask CBP to notify the Port if and when it intends to conduct biometric air exit, so that the Port can maintain situational awareness.

In general, the Port can enhance CBP's efforts related to publicizing information about the biometric air exit program; recommendations related to this issue are listed under the Transparent principle.

Recommendation B: The Port should request that CBP notify the Port in advance of implementing or expanding biometric air exit.

3. Stakeholder Concerns
External Advisory Group members raised the following concerns:
- There should be greater clarity regarding the criteria with which the Aviation Managing Director (AMD) will decide if a request will be accepted.
    - Port staff response: Added language to Recommendation 2a and 2b to address this.

- Beyond the AMD process, the policy recommendations should specify the situations warranting the use of biometrics. There should be more clarity on what constitutes as an "operational need."
    - Port staff response: Added language to Recommendation 2a and 2b to address this.

- Operational need is better phrased as operational benefit.
    - Port staff response: Changed 2a and 2b

---

[7] Available upon request via https://portofseattle.nextrequest.com/requests/new
[8] Available upon request via https://portofseattle.nextrequest.com/requests/new

- Net benefit-cost is different for different subcategories of individuals.
  - Port staff response: Port staff response: Changed 2a and 2b

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.
  - Port staff response: For this section, added Recommendation B.

b. Voluntary

The Port Commission's Biometrics Motion states that:

> *The use of biometrics to identify and validate travelers through port facilities should be voluntary, and reasonable alternatives should be provided for those who do not wish to participate – through a convenient "opt-in" or "opt-out" process, except in specific situations authorized by the port or required by federal law such as U.S. Customs and Border Protection's (CBP) entry and exit requirements for non-U.S. citizens. Unintended capture of data by biometric technology from those travelers opting out of such biometric data collection, or of any non-travelers or other visitors at the airport, should be prevented; any unintended capture of this data should not be stored.*

1. Key Issues to address

There are two main aspects of the Voluntary principle: 1) providing for an opt-in or opt-out procedure, and 2) preventing unintended image capture.

Current CBP regulations state that opt-out is the method for departing international travelers to choose not to participate in biometric screening.[9] However, the Port should continue to pursue whether opt-in is allowed and logistically feasible. Regardless, it is essential that all travelers fully understand their rights not to participate and the consequences of such a choice; similarly, the Port must ensure that opt-out or opt-in procedures are respectful and appropriate. These issues are covered in other recommendations.

As related to image capture, the Port can specify requirements for the physical configuration of its facilities in an effort to prevent unintended image capture during biometric air exit operations.

2. Working Group Recommendations

"Voluntary" recommendations at a glance		
Port	Airline	Federal
If port approves biometric air exit program implementation, the port should set standards for where and how facial recognition cameras can be used at international departure	*If port approves* biometric air exit program implementation, airline staff should be trained to prevent unintended capture and comply with Port standards	CBP policy states that legal U.S. residents are allowed to opt-out of biometric screening

---

[9] From CBP guidelines: "While U.S. Citizens who are entering or exiting the country are generally required to be in possession of a valid U.S. passport, CBP does not require U.S. Citizens or exempt aliens to have their pictures taken. Travelers who do not wish to participate in this facial comparison process may notify a CBP Officer or an airline, airport or cruise line representative in order to seek an alternative means of verifying their identities and documents."

gates and should train staff to prevent unintended capture *If procurement process is required*, request information on ways the vendor can help avoid unintended image capture *If the Port approves the implementation of biometric air exit for use at SEA by the Port or airlines,* the Port should continue to pursue whether opt-in is allowed and logistically feasible. If it is, opt-in is a preferable way to implement the voluntary nature of the program.	*If the Port finds that opt-in is allowed and logistically feasible,* then airlines implementing biometric air exit should utilize that as the method to implement the voluntary nature of the program.	

For Port

Recommendation 6: If the Port approves the implementation of biometric air exit for use at SEA by Port staff that requires a procurement, then the vendor proposal must include how its technology can help minimize the unintended capture of images of nontravelers or visitors.

Recommendation 7a: The Port should develop standards and guidelines for where and how facial recognition cameras can be used at international departure gates. In particular, these guidelines should include ways to avoid unintended image capture – for example, by positioning the camera in a direction that does not face the main passenger area, use of a screen behind the individual being photographed, or use of a camera with a minimal field view.

Recommendation 8a: If the Port approves any implementation of biometric air exit for use at SEA, the Port should design training standards for all users of biometric exit technology at SEA that includes the abovementioned standards for avoiding unintended capture.

Recommendation Aa: If the Port approves the implementation of biometric air exit for use at SEA by the Port or airlines, the Port should continue to pursue whether opt-in is allowed and logistically feasible. If it is, opt-in is a preferable way to implement the voluntary nature of the program.

For Airlines

Recommendation 7b: If the Port approves the use of biometric air exit by airlines, each airline must submit a plan for minimizing unintended capture of images of nontravelers.

Recommendation 8b: If the Port approves the implementation of biometric air exit for use at SEA, the Port should require all participating airlines to demonstrate that their employees have received training in line with the Port's standards for avoiding unintended capture.

Recommendation Ab: If the Port finds that opt-in is allowed and logistically feasible, then airlines implementing biometric air exit should utilize that as the method to implement the voluntary nature of the program.

For CBP

As stated above, current CBP policy states that travelers are allowed to opt-out of biometric air exit screening. However, the Port should pursue whether opt-out is an option as well. Regardless, enshrining the voluntary nature of this program in legislation is part of the Port's federal advocacy efforts outlined in the Lawful principle.

3. Stakeholder Concerns

External Advisory Group members raised the following concerns:

- The Port should further define and recommend opt-in and opt-out procedures, and explore ways to institute opt-in as a legitimate option. Travelers should be engaged on their preferences in this regard.
  - o Port response: Opt-out is the CBP-required method for biometric air exit. However, we will mandate opt-in for almost all other use cases.

- The Port should continue to research and explore potential legal and logistical requirements of opt-in vs. opt-out.
  - o Port response: Changed text under Key Issues to Address and For CBP. Added recommendations Aa and Ab.

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.
  - o Port staff response: For this section, CBP would not be bound by the Port's unintended capture standards or training rules, so those would not happen.

c. Private

The Port Commission's Biometrics Motion states that:

> *Data collected by biometric technology at port facilities or by port employees from travelers through port facilities should be stored only if needed, for no longer than required by applicable law or regulations, and should be protected against unauthorized access. The port opposes this data being knowingly sold or used for commercial purposes unrelated to processing travelers at port facilities without their clear and informed consent. Individuals should be provided a process to challenge instances where they feel their rights have been violated.*

1. Key Issues to address

The Private principle is an essential aspect of travelers' confidence in their participation in any biometric air exit program. Individuals want to know that their data is secure, not being used for any inappropriate purpose, and protected.

CBP has published a Privacy Impact Assessment report that outlines its efforts to protect data privacy, and any airport or airline implementing biometric air exit must agree to comply with CBP's business requirements. For example, CBP does not permit its private sector partners to retain or share the photos captured at the boarding gate (or at any other location using TVS); however, the enforcement of these

business requirements is currently the sole responsibility of CBP. There is no present mechanism for the Port to enforce these business requirements.

The issue of giving individuals an opportunity to challenge violations of their rights is covered under the Ethical principle.

2. Working Group Recommendations

"Private" recommendations at a glance		
Port	Airline	Federal
If/when data is transmitted between the Port and CBP it must: a) occur over an encrypted connection; b) be exempt from state public disclosure requirements; c) be immediately deleted once complete; and d) not be used for any other purpose *If procurement process is required*, request information on alignment with privacy protections.	*If/when* data is transmitted between the Port and CBP it must: a) occur over an encrypted connection b) be immediately deleted once complete c) not be used for any other purpose	The port does not have jurisdiction over CBP's privacy policies or procedures.

For Port

Recommendation 9: For any Port implementation of biometric air exit that requires a procurement, all vendor proposals must include an explanation of how the technology solution will meet the Port's biometric Privacy principles and CBP's Biometric Air Exit Requirements, including by providing relevant privacy policies, data collection and storage practices, and cybersecurity practices.

Recommendation 10: The Port should endeavor to seek clarification from the State of Washington Attorney General whether transmission of biometric data to CBP is exempt from state public disclosure requirements, so as to protect personally identifying information from release in conformity with the Port's obligations under the Washington Public Records Act and record retention requirements.

Recommendation 11a: For any Port implementation of biometric air exit, all transmission of biometric data to CBP should meet CBP's Biometric Air Exit Requirements regarding encryption and other security standards.

Recommendation 12a: Any data transmitted to CBP by the Port or received by the Port from CBP must be deleted in accordance with CBP's Biometric air exit requirements.

Recommendation 13a: No data transmitted to CBP by the Port or received by the Port from CBP may be used for any other purpose other than for processing departing international passengers at the boarding gate through TVS, in accordance with CBP's Biometric Air Exit Requirements. Unauthorized third-parties may not be provided access to any such data.

For Airlines

Recommendation 11b: For any airline implementation of biometric air exit, any transmission of biometric data to CBP should meet CBP's Biometric Air Exit Requirements regarding encryption and other security standards.

Recommendation 12b: Any data transmitted to CBP by an airline at SEA or received by an airline at SEA from CBP should be deleted in accordance with CBP's Biometric Air Exit Requirements.

Recommendation 13b: Any data transmitted to CBP by an airline at SEA or received by an airline at SEA from CBP should not be used for any other purpose other than for processing departing international passengers at the boarding gate through TVS, in accordance with CBP's Biometric Air Exit Requirements. Unauthorized third-parties should not be provided access to any such data.

For CBP

The Port is not legally authorized to regulate CBP's privacy policies or procedures. CBP is required to comply with federal privacy laws and regulations, and it sets forth its compliance with many such requirements in the Privacy Impact Assessment noted above. However, there is no comprehensive federal framework governing privacy protections for biometric data. The Port can help enhance CBP's efforts related to explaining their data privacy efforts; see recommendations under the Transparent principle.

3. Stakeholder Concerns

External Advisory Group members raised the following concerns:

- These recommendations should better define the duration of image storage.
  - o Port response: Duration of image storage is fully described in the CBP Business Requirements, which all Biometric Air Exit users must follow.

- These recommendations should better explore and describe what CBP audit procedures exist to ensure that policies are being met. It is important for the Port to have insights into those audit results. The Port should also explore how it might conduct its own audits, within the limitations of CBP's federal jurisdiction.
  - o Port response: Added language in Recommendation 19a under the Transparency recommendations to address this concern. Added a new Recommendation 20 to address this concern.

- The Port should clarify the data security measures taken by the airlines and the technology vendor, both generally and specifically with regard to unauthorized access by third parties.
  - o Port response: Restrictions on unauthorized use and access – and associated data security requirements – are fully described in the CBP Business Requirements, which all Biometric Air Exit users must follow.

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.
  - o Port staff response: For this section, CBP comply with the same privacy standards as the Port or airlines would be bound by via the Business Requirements. However, the Port would not have control over vendor selection.

d. Equitable

The Port Commission's Biometrics Motion states that:

> *The port opposes discrimination or systemic bias based on religion, age, gender, race or other demographic identifiers. Biometric technology used at port facilities or by port employees should be reasonably accurate in identifying people of all backgrounds, and systems should be in place to treat mismatching issues with proper cultural sensitivity and discretion.*

1. Key Issues to address

The Equitable principle essentially speaks to two key issues: 1) concern that facial recognition technology does not perform as effectively on individuals who are not male Caucasians, and that 2) regardless of why the CBP algorithm identifies a mismatch, systems should be in place to resolve the issue with minimal impact to the traveler.

A recent study by the National Institute of Standards and Technology (NIST) found that facial recognition technology's ability to identify individuals with diverse characteristics varies significantly based on the algorithm at the heart of the system, the application that uses it, and the data inputs.[10] **However, the NIST report confirmed that the NEC algorithm used by CBP in its Biometric Air Exit program ranked first or second in most categories evaluated, including match performance in galleries that are much bigger than those used by CBP.** CBP attributes these accuracy rates in large part to the fact that individuals are being compared against a database of only several hundred travelers built from the flight manifest. The specific algorithm used is a component of the CBP TVS.

Treating no-matches or mismatches with "cultural sensitivity and discretion" requires that individuals that are not verified through TVS are subject to additional document review in a manner and location that draws the least possible attention to the situation and does not create a feeling of fear or discomfort for the traveler.

2. Working Group Recommendations

"Equitable" recommendations at a glance		
Port	Airline	Federal
Request and compare against updated accuracy rates from CBP before approving Port-requested biometric air exit program Port should develop training standards for handling facial recognition mismatching issues appropriately *If procurement process is required*, request information on alignment with equity protections	Request and compare against updated accuracy rates from CBP before approving airline-requested biometric air exit program All airline employees operating biometric air exit program must be trained on facial recognition limitations, how to deal with inaccuracies, and cultural sensitivity	The port does not have jurisdiction over CBP accuracy algorithm.

---

[10] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

For Port
Recommendation 14: If the desired implementation of biometric air exit by Port staff requires a procurement, then the vendor proposal must include an explanation of how it will meet the Port's Equity principle and CBP's Biometric Air Exit Requirements. Vendors will need to provide, to the extent applicable, information regarding how their equipment and services enhance, to the extent possible, accuracy levels in identifying peoples of all backgrounds, gender, and age.

Recommendation 15a: The Port should request updated accuracy rates from CBP – including a request for any available data segmented by key traveler characteristics – before approving any Port staff-requested biometric air exit implementation.

Recommendation 16a: The Port should develop training standards for collecting and processing biometric data. The training must include, but not be limited to: the capabilities and limitations of facial recognition, and how to deal with mismatching issues with sensitivity and discretion.

For Airlines
Recommendation 15b: The Port should request updated accuracy rates from CBP – including a request for any available data segmented by key traveler characteristics – before approving any airline-requested biometric air exit implementation.

Recommendation 16b: Before approving any airline-requested biometric air exit program, the Port should require airlines to verify that their employee training for operating biometric air exit includes the terms of CBP's Biometric Air Exit Requirements, the capabilities and limitations of facial recognition, and how to deal with mismatching issues with sensitivity and discretion.

For CBP
The Port does not have jurisdiction over – or access to – CBP's algorithm. However, the Port can request CBP's cooperation in sharing accuracy rates and work collaboratively to address any systemic deficiencies in TVS attributable to travelers' backgrounds, gender, or age; see recommendations under the Transparent principle. The Port can also design standards to ensure that travelers who cannot be identified through TVS are subject to secondary screening in a manner and location that draws the least possible attention to the situation and does not create a feeling of fear or discomfort.

3. Stakeholder Concerns
External Advisory Group members raised the following concerns:
- The Port should clarify its authority to review airline training.
  - Port response: Port legal opinion is that we do not have authority to require specific airline employee training. However, by asking for demonstration that airlines are meeting our training standards, we will achieve the goals of this recommendation.

- The Port should seek to more explicitly review and benchmark against the operational results of other airports' biometric air exit systems. This effort is key to the recommendation to "compare and review CBP accuracy rates before approval".
  - Port response: We receive a weekly report from CBP with accuracy rates from all participating airports, and will include this data in our accountability report requirements, listed in Recommendation 19a under Transparency.

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.
  - Port staff response: For this section, CBP would not be bound by the Port's training standards, so those would not happen.

e. Transparent

The Port Commission's Biometrics Motion states that:

> *Use of biometric technology for passenger processing at port facilities should be communicated to visitors and travelers. Individuals should be notified about any collection of their biometric data to facilitate travel at port facilities, and how that data may be used, in easily understood terms. Reports on the performance and effectiveness of the technology should also be made public to ensure accountability.*

1. Key Issues to address

The Transparent principle essentially speaks to three key issues: 1) the need for any use of biometric air exit to be clearly communicated to anyone visiting SEA, 2) the need to ensure that passengers using biometric air exit are informed in a clear, concise manner about biometric air exit, how it is used, and their rights related to the system, and 3) the need for accountability reports to be created and published for the public.

The Transparent principles requires that SEA passengers should be made aware that biometric air exit is going to be used on their departing international flight, understand what it is, and be informed of their rights related to the program (including their ability to opt-out). This requires clear, consistent and standardized communications protocols, in coordination with airlines and CBP.

Similarly, information about the system must be continuously verified. Performance data should be a key aspect of the Port's review of biometric air exit implementation, and publicly verified and approved findings should be made public.

2. Working Group Recommendations

"Transparent" recommendations at a glance		
Port	Airline	Federal
If port *approves* biometric air exit program implementation or CBP implements, the Port should produce: a) a comprehensive communications plan b) an accountability report each of which should be shared publicly through all Port communication channels. Each report should include all available information released by CBP.	If port *approves* biometric air exit program implementation, airlines should cooperate with the Port on communications and accountability reports.	The port cannot require CBP to share information.

If procurement process is required, request information on alignment with transparency protections		

For Port

Recommendation 17: If the Port approves an implementation of biometric air exit by Port staff that requires a procurement, the vendor proposal must include an explanation of how it will support efforts to meet the Port's biometric Transparent principle. In addition, once the procurement contract is awarded, the vendor must support efforts to develop performance reports on a regular basis.

Recommendation 18a: If the Port approves the implementation of biometric air exit by either Port staff or an airline or CBP implements biometric air exit by exercising its federal jurisdiction, the Port should develop a comprehensive communications plan that notifies the general public of the implementation and all related information, including their rights with regard to the program and recourse in case of violations of those rights and/or data breaches. The communications plan should include specific communications within the airport, including announcements, signage, flyers and web content.

Recommendation 19a: If the Port approves the implementation of biometric air exit by Port staff or an airline or CBP implements biometric air exit by exercising its federal jurisdiction, the Port should produce an annual accountability report – in multiple languages – that includes all approved, publicly available information on topics such as:
- A description of the biometric air exit program;
- Its general capabilities and limitations;
- How data is generated, collected, and processed;
- CBP's privacy guidelines;
- Traveler rights with regard to the biometric air exit system;
- The Port's biometric air exit training standards;
- Other relevant data, including any publicly available data shared by CPB about the accuracy and effectiveness of its system;
- Benchmarking data against the operational results of other airports' biometric air exit systems;
- An assessment of compliance with the Port's Biometrics Principles, CBP's Biometric Air Exit Requirements, and the Biometric Air Exit Policy approved by the Commission;
- Any Port conducted performance audits, within the limitations of CBP's federal jurisdiction, verifying the results of CBP audits.
- Any known or reasonably suspected violations of those rules and guidelines, including complaints alleging violations;
- Feedback about the public's experience, sought proactively in customer surveys, including whether travelers believe that they fully understand the information about the system;
- Any available information on data sharing within the U.S. Department of Homeland Security, such as what data is requested and by whom, within the limitations of the Port to require this information from CBP;
- Any airline disclosure of individuals' biometric data, within the limitations of the Port to access and disclose law enforcement activity; and
- Any publicly available CBP audits of the biometric air exit system.

This accountability report should be shared publicly through appropriate Port communications channels.

Recommendation 20: The Port should periodically conduct its own performance evaluation, within the limitations of CBP's federal jurisdiction, to attempt to verify CBP's audit results and ensure that airline staff are following all Port policies, including those related to privacy, customer service, traveler communication and unintended image capture.

For Airlines
Recommendation 18b: If the Port approves the implementation of biometric air exit by an airline for use at SEA, it should partner with that airline on implementation of the Port's biometric air exit communications plan.

Recommendation 19b: If the Port approves the implementation of biometric air exit by an airline for use at SEA, it should work with the airline to share the Port's annual accountability report through relevant airline communications channels. The airline should also disclose to the Port as part of that annual reporting an assessment of compliance and any known or reasonably suspected violations, including complaints alleging violations and any disclosure of an individual's biometric data.

For CBP
The Port does not have jurisdiction over CBP's transparency procedures. However, CBP does provide notice to travelers at SEA and other the designated ports of entry through physical signage, verbal announcements and/or flyers with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the program. As stated above, the Port can implement additional signage and communications on this topic.

As it relates to evaluation of the technology's accuracy and effectiveness, the Port cannot require CBP to share this information, but it can request and help publicize CBP-provided performance data and any publicly-available audits.

Recommendation 19c: The Port should include in its communications plan and accountability reports all available and approved information publicly released by CBP about the biometric air exit program, including data on privacy, accuracy, audits, and other program details.

3. Stakeholder Concerns
External Advisory Group members raised the following concerns:
- The Port should seek greater clarity from CBP on data sharing within the U.S. Department of Homeland Security, such as what data is requested and by whom, within the limitations of CBP's federal jurisdiction. Similarly, airlines should disclosure any data sharing that occurs of individuals' biometric data.
  - Port response: Added to the requirements of the accountability report, under Recommendation 19a and 19b.

- The Port should include in the Accountability Report any feedback about the public's experience. This should be proactive information gathering rather than simply reactive to complaints. The public should be asked whether they fully understand the information about the system.
  - Port response: Added to the requirements of the accountability report, under Recommendation 19a.

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.
  - Port staff response: For this section, edited recommendations 18a and 19a to make it clear that they would happen in all scenarios.

f. Lawful

The Port Commission's Biometrics Motion states that:

> *Use of biometric technology and/or access to associated biometric data collected should comply with all laws, including privacy laws and laws prohibiting discrimination or illegal search against individuals or groups.*

1. Key Issues to address

The Lawful principle essentially speaks to the legal justification for CBP's biometric air exit program. As discussed above, CBP has stated that the biometric entry/exit program is based on several Congressional (Intelligence Reform and Terrorism Prevention Act of 2004; FY 2013 Consolidated and Further Continuing Appropriations Act; FY 2016 Consolidated Appropriations Act) and Administration (Executive Order 13769) authorizations.

There are several active conversations in Congress regarding the need for additional regulation of the federal government's use of biometrics and facial recognition technology, but no clear direction as of yet. Similarly, there are several conversations in the Washington State Legislature regarding regulation of biometrics and facial recognition. Airlines and the Port may be subject to state and local law to the extent they voluntarily deploy TVS in support of CBP's biometric air exit initiatives.

This is a rapidly evolving area of the law and the extent to which biometric air exit may be further regulated is not yet clear.

2. Working Group Recommendations

"Lawful" recommendations at a glance		
Port	Airlines	Federal
Port staff should comply with existing laws, and actively advocate for additional state and federal biometric regulations If the Port approves the implementation of biometric air exit by Port staff or an airline or CBP implements biometric air exit by exercising its federal jurisdiction, Port staff should develop a comprehensive understanding of how local, state and federal data breach statutes would apply to a biometric air exit data breach,	Airlines should engage with port in tracking and advocating state and federal biometric regulations	CBP is subject to all federal law and regulations

and what recourse travelers would have in those situations. This information should be shared as part of the Port communications plan.		

For Port
Recommendation 21a: If the Port approves the implementation of biometric air exit by Port staff or an airline, it must comply with all state and federal laws including privacy and discrimination laws.

Recommendation 21b: If the Port approves the implementation of biometric air exit by Port staff or an airline or CBP implements biometric air exit by exercising its federal jurisdiction, Port staff should develop a comprehensive understanding of how local, state and federal data breach statutes would apply to a biometric air exit data breach, and what recourse travelers would have in those situations. This information should be shared as part of the Port communications plan.

Recommendation 22a: Port staff should actively track and work with stakeholders to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.

For Airlines
Recommendation 22b: The Port should engage its airline partners in its advocacy for state and federal laws and regulations that codify the goals of the Port's biometric principles.

For CBP
CBP is subject to applicable federal law and regulations.

3. Stakeholder Concerns
External Advisory Group members raised the following concerns:
- The Port should address what tools and/or recourse exists for travelers in case of a data breach, and specifically the Port's role in that situation.
    - Port response: Added data breach recourse into its communications plan under Recommendation 18a. Added data breach research as recommendation 21b.

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.
    - Port staff response: For this section, nothing would change. The Port is going to pursue recommendation 22a regardless.

g. Ethical
The Port Commission's Biometrics Motion states that:

> *The port and its partners should act ethically when deploying biometric technology or handling biometric data. Ethical behavior means actions which respect key moral principles that include honesty, fairness, equality, dignity, diversity and individual rights. In particular, use of biometrics at port facilities should comply with Resolution No. 3747, establishing the port's Welcoming Port Policy Directive to increase engagement with, and support for, immigrant and refugee communities.*

1. Key Issues to address

As mentioned by several of the Port's external stakeholders, the Ethical principle is an important complement to the Lawful principle, because of the current lack of comprehensive state and federal laws governing facial recognition technology.

Several of the recommendations on this topic are covered under other principles like Equity (treating people fairly and with dignity), Privacy (protecting individual rights) and Justified (no "mass surveillance"). However, the most tangible aspect of this principle is alignment with the Port's "Welcoming Port Policy" (Resolution 3747).[11]

The Welcoming Port Policy commits the Port to "to foster a culture and environment that make it possible for our region to remain a vibrant and welcoming global gateway where our immigrant communities, refugee residents, and foreign visitors can fully participate in – and be integrated into – the social, civic, and economic fabric of our region." To the extent consistent with federal laws and obligations, the practical applications of this policy include not denying anyone services based on immigration status; prohibiting any Port employees, including law enforcement officers, from unnecessarily asking about citizenship or immigration status; and taking tangible steps to make all visitors to its facilities to feel welcome and safe. As it relates to immigration enforcement, the policy includes calls for the Port – within the restrictions of federal law – to "defer detainer requests from ICE"; restrictions on "providing federal immigration agents with access to databases without a judicial warrant"; and restrictions on carrying out "a civil arrest based on an administrative warrant."

The biometric air exit program generally provides CBP with information that it already has: CBP already compiles galleries of travelers' facial biometrics from photos that travelers are required to submit (i.e., passport or visa application pictures). The airline also already provides CBP with passenger manifests and traveler data through the Advance Passenger Information System (APIS) system. That is why CBP refers to biometric air exit as an "automation of an existing system" rather than a new border security measure.

2.   Working Group Recommendations

"Ethical" recommendations at a glance		
Port	Airlines	Federal
If port approves biometric air exit program implementation or CBP implements, then engage (along with relevant partners) with local immigrant and refugee communities in multiple languages and culturally appropriate such that they can a) be educated b) share concerns about incidents The Port should form a Technology Ethical Advisory	*If port approves* biometric air exit program implementation, then airlines should work with the Port to educate local immigrant and refugee communities	CBP is bound by all relevant federal laws as referenced above – including anti-discrimination and civil liberties statutes.

[11] https://www.portseattle.org/sites/default/files/2018-05/2018_05_08_SM_8a_reso.pdf

Board to advise on the ethical issues raised by implementation of biometric technology and other innovations		

For Port

Recommendation 23: If the Port approves the implementation of biometric air exit for use at SEA or CBP implements biometric air exit by exercising its federal jurisdiction, the Port should develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about the biometric air exit program. Specifically, the Port should ensure that these communities are fully informed about the program, the technology and their rights – in multiple languages and in culturally appropriate ways.

Recommendation 24a: If the Port approves the implementation of biometric air exit for use at SEA or CBP implements biometric air exit by exercising its federal jurisdiction, the Port should work with local jurisdictions, nonprofit organizations and others to inform local immigrant and refugee communities – in multiple languages and in culturally appropriate ways – about resources for sharing concerns about any incidents in which they do not feel they have been afforded their full legal rights and/or their treatment has not been fully respectful.

Recommendation 25: The Port should form a Technology Ethical Advisory Board – composed of community stakeholders, academics, technology experts and other key stakeholders – to advise on the ethical issues raised by implementation of biometric technology and other innovations. This advisory board should be consulted on a regular basis to ensure that Port technology implementation – specifically new biometrics programs – are fully aligned with this principle.

For Airlines

Recommendation 24b: If the Port approves the implementation of biometric air exit for use at SEA or CBP implements biometric air exit by exercising its federal jurisdiction, the Port should work with participating airlines to inform local immigrant and refugee communities – in multiple languages and in culturally appropriate ways – about resources for concerns about any incidents in which they do not feel they have been afforded their full legal rights and/or their treatment has not been fully respectful.

For CBP

CBP is bound by all relevant federal laws as referenced above – including anti-discrimination and civil liberties statutes. The best way to ensure ethical behavior is to enshrine it in statute, which relates back to the advocacy recommendations above. In addition, the Port will continue to engage regularly with CBP to share our expectations that all individuals traveling through our facilities have full access to their legal rights and are receiving appropriate treatment.

3. Stakeholder Concerns
External Advisory Group members raised the following concerns:
- The Port should explicitly include opt-out procedures in its public outreach.
    - Port responses: Added to the communications plan under Recommendation 18a.

- This document should explicitly articulate which of the Port recommendations will still be implemented if CBP – not the Port or airlines – implement biometric air exit.

- Port staff response: For this section, edited recommendations 23, 24a and 24b to reflect that these would happen in any implementation scenario.

APPENDIX

o Appendix A – Port Biometrics Working Group

- Matt Breed, Chief Information Officer
- Julie Collins, Director, Customer Experience
- Commander Lisa Drake, Port of Seattle Police Department
- Laurel Dunphy, Director, Airport Operations
- Marie Ellingson, Manager, Cruise Operations
- Eric ffitch, Manager of State Government Relations, External Relations
- Bookda Gheisar, Senior Director, Office of Equity, Diversity and Inclusion
- James Jennings, Director, Airline Relations
- Ron Jimerson, Chief Information Security Officer
- John McLaughlin, Senior Port Counsel
- Anne Purcell, Senior Port Counsel
- Russ Read, Manager, Maritime Security
- Wendy Reiter, Director, Aviation Security
- Kathy Roeder, Director of Communications, External Relations
- Eric Schinfeld, Senior Manager of Federal Government Relations, External Relations
- Deputy Chief Mark Thomas, Port of Seattle Police Department
- Veronica Valdez, Commission Specialist
- Todd VanGerpen, Manager, Aviation Innovation
- Dave Wilson, Director, Aviation Innovation

○ **Appendix B – Port Biometrics External Advisory Group**

- Ian Baigent-Scales, Airport Customer Development Manager - Airport Operations, Virgin Atlantic Airways
- Sasha Bernhard, Legislative Assistant, Office of US Representative Suzan DelBene
- Dana Debel, Managing Director, State and Local Government Affairs, Delta Air Lines
- Adele Fasano, Director, Field Operations, Seattle Field Office, US Customs & Border Protection
- Eric Holzapfel, Deputy Director, Entre Hermanos
- Suzanne Juneau, Executive Director, Puget Sound Business Travel Association
- Scott Kennedy, State and Local Government Affairs Manager, Alaska Airlines
- Jennifer Lee, Technology & Liberty Project Director, ACLU
- Maggie Levay, Director Guest Port Services, Royal Caribbean
- McKenna Lux, Policy Manager, CAIR-WA
- Yazmin Mehdi, Outreach Director, Office of US Representative Pramila Jayapal
- Nina Moses, Stakeholder Relations Manager, US Transportation Security Administration
- Irene Plenefisch, Government Affairs Director, Microsoft Corporation
- Sheri Sawyer, Senior Policy Advisor, Office of Washington State Governor Jay Inslee
- Victoria Sipe, Director Shore Operations, Holland America Group
- Rich Stolz, Executive Director, One America
- Elizabeth Tauben, Manager Port Guest Services & Clearance, Norwegian Cruise Line Holdings
- Jennifer Thibodeau, Public Policy Manager - Western States, Amazon Web Services
- Jevin West, Director, Center for an Informed Public, University of Washington

o **Appendix C – Commission Biometrics Motion**

MOTION 2019-13:
A MOTION OF THE PORT OF SEATTLE COMMISSION

adopting guiding principles for the public-facing use of
biometric technology at Port of Seattle maritime and
aviation facilities; establishing a working group to
develop policy recommendations governing public-
facing biometric use at the port; and establishing
deadlines for further actions.

AMENDED AND ADOPTED
DECEMBER 10, 2019

INTRODUCTION

Biometrics is the measurement and analysis of physical and behavioral characteristics that are used to identify individuals through technology. An example of a physical characteristic includes the unique features of an individual's face or their fingerprint. An example of a behavioral characteristic includes an individual's voice, signature, or how they walk.

The Port of Seattle has long used various forms of biometrics at its aviation and maritime facilities – for access control and verification of employee, contractor, vendor, and consultant identity. However, biometric technology – particularly facial recognition – is increasingly being deployed on the customer-facing side of airport and cruise operations, as both an identity validation and a customer facilitation tool to speed up check-in, boarding, and screening processes.

As with any developing technology, public sector leaders have an obligation to ensure appropriate and responsible use of not only the technology itself, but the related data that is generated. The port commission believes proper biometric policy should balance operational needs, business priorities, and regulatory mandates with protections for the interests and rights of passengers, employees, and other visitors to our facilities.

TEXT OF THE MOTION

Port of Seattle Principles for Public-Facing Biometric Technology
The commission hereby adopts the following principles to guide the use of public-facing biometric technology at Port of Seattle facilities:

(1) **Justified:** Biometric technology at port facilities should be used only for a clear intended purpose that furthers a specific operational need. The port does not condone biometrics for "mass surveillance" – for example, use of facial recognition on large groups of people without a lawful purpose, rather than single-use for travelers.

(2) **Voluntary:** The use of biometrics to identify and validate travelers through port facilities should be voluntary, and reasonable alternatives should be provided for those who do not

wish to participate – through a convenient "opt-in" process where possible or "optout" process if "opt-in" is not possible, except in specific situations authorized by the port or required by federal law such as U.S. Customs and Border Protection's (CBP) entry and exit requirements for non-U.S. citizens. Unintended capture of data by biometric technology from those travelers opting out of such biometric data collection, or of any non-travelers or other visitors at the airport, should be prevented; any unintended capture of this data should not be stored.

(3) **Private:** Data collected by biometric technology at port facilities or by port employees from travelers through port facilities should be stored only if needed, for no longer than required by applicable law or regulations, and should be protected against unauthorized access. The port opposes this data being sold or used for commercial purposes unrelated to processing travelers at port facilities without their clear and informed consent. Individuals should be provided a process to challenge instances where they feel their rights have been violated.

(4) **Equitable:** The port opposes discrimination or systemic bias based on religion, age, gender, race, or other demographic identifiers. Biometric technology used at port facilities or by port employees should be accurate in identifying people of all backgrounds, and systems should be in place to treat mismatching issues with proper cultural sensitivity and discretion.

(5) **Transparent:** Use of biometric technology for passenger processing at port facilities should be communicated to visitors and travelers. Individuals should be notified about any collection of their biometric data to facilitate travel at port facilities, and how that data may be used, in easily understood terms. Reports on the performance and effectiveness of the technology should also be made public to ensure accountability.

(6) **Lawful:** Use of biometric technology and/or access to associated biometric data collected should comply with all laws, including state and federal privacy and consumer data protection laws and laws prohibiting discrimination or illegal search against individuals or groups.

(7) **Ethical:** The port and its partners should act ethically when deploying biometric technology or handling biometric data. Ethical behavior means actions which respect key moral principles that include privacy, honesty, fairness, equality, dignity, diversity, and individual rights. In particular, use of biometrics at port facilities should comply with Resolution No. 3747, establishing the port's Welcoming Port Policy Directive to increase engagement with, and support for, immigrant and refugee communities.

These principles will apply until a more comprehensive policy is put in place, through the working group process laid out below.

Biometric Working Group
Through this motion, a port working group is established to develop further recommendations governing port policy related to use of public-facing biometric technology, which shall be submitted to the commission by the end of the first quarter of 2020. Issues to be addressed by this working group include the following:
- the strategic use and objectives of biometrics;
- procurement;

- transparency and accountability for biometric implementation;
- auditing of this technology to ensure compliance and accuracy, and auditing prior to approval of expansion of technology;
- commitments or agreements with airlines, cruise operators, and other port tenants and users;
- handling biometric data collected and stored from the technology;
- protection of personally identifying information;
- data security protocols and protection from unlawful or unauthorized access;
- alignment with the port's Welcoming Port Policy;
- state and federal policy priorities;
- outreach and public awareness strategy to prepare travelers and community members;
- and any other relevant topics that arise.

In addition, the working group should develop a comprehensive list of known public-facing biometric implementation being planned at port facilities over the next five years.

The working group will include, but not be limited to, representatives from the following port departments: Aviation Security; Aviation Operations; Airport Innovation; Maritime Security; Maritime Operations; Commission Office; Office of Equity, Diversity, and Inclusion; Information and Communications Technology; Information Security; Government Relations; Legal; and Police. The working group shall also engage active participation from an advisory group comprised of community partners, travelers, maritime and aviation industry partners, and other impacted stakeholders. The working group shall meet at least once a month. The policy recommendations shall be delivered to commission by the end of the first quarter of 2020. The commission may create a special committee (an ad hoc, limited term commission committee) to oversee these efforts and expects a policy governing the use of public-facing biometric technology to be delivered to the commission by the end of the second quarter of 2020.

Implementation of Public-Facing Biometric Technology at Port facilities
Upon adoption of the port's policy by the end of the second quarter of 2020, public-facing biometric technology may be implemented at port facilities if it demonstrates alignment with biometric principles and meets the port's operational requirements. Port leadership will implement an approval process for any proposals for new or expanded use of public-facing biometric technology to ensure alignment with these principles. Any proposal for new or expanded use of public-facing biometric technology will be communicated in advance directly to the port commission and through the port's external communications channels. The use of public-facing biometric technology at port facilities is subject at all times to the port's requirements. The port's biometric policies should be incorporated into commitments or agreements governing the use of biometric technology at port facilities.

Because the port does not have jurisdiction over the use of biometrics by the federal government at our facilities, the port will communicate these principles to CBP and other federal partners such as the U.S. Transportation Security Administration (TSA) and U.S. Coast Guard. We will not only notify them of our desired standards, but also work with these agencies and Congress to ensure that federal programs in place at port facilities are aligned as closely as possible with port policy regarding utilization of public-facing biometric technology.

<div align="center">**STATEMENT IN SUPPORT OF THE MOTION**</div>

Due to technological advances, perceived customer benefits, and federal requirements, there will be a significant increase in public-facing facial recognition technology deployment by public and private sector users over the next few years, including in airport and seaport settings that will impact travelers and other visitors to our facilities. In advance of this expansion, the port commission believes that it has an obligation to institute proper policy frameworks and clear guidelines to reduce potential misuse and abuse, while improving public understanding of the benefits and risks. Specifically, the port must ensure individual privacy, civil liberties, and equity, and that biometric technology and use of the associated data is aligned with state and federal laws intended to protect those rights.

Biometrics are used in various forms at the port's aviation and maritime facilities:
- Across the port, port-issued identification cards currently utilize fingerprint biometrics to access secure or restricted areas or to permit authorized personnel access to port facilities outside of normal business hours or in locations where there is no other monitoring of access. In addition, many port employees are issued iPhones with fingerprint and facial recognition as an alternative to password protection, and facial recognition is also used on Microsoft Windows 10.
- At Seattle-Tacoma International Airport (SEA), airport employees are required to scan their fingerprint at many secure doors throughout the facility. SEA also offers travelers the option of using CLEAR to validate the identity of a traveler as they process through TSA checkpoints using biometric technology instead of using traditional identification and validation methods.
- On the maritime side, biometric data is required by federal regulation for issuance of TSA-issued Transportation Worker Identification Credential (TWIC) smart cards that are required to access maritime facilities regulated by the U.S. Coast Guard and cruise terminal operational areas. In addition, the cruise industry is increasingly taking advantage of biometrics as a passenger facilitation tool; for example, Norwegian Cruise Line and CBP have partnered for use of facial recognition for disembarkation of guests at Pier 66.

One of the leading drivers of the expected deployment of public-facing biometrics over the next few years is implementation by CBP of a Congressionally mandated biometric exit-entry screening process for international air passengers. SEA's International Arrivals Facility will incorporate facial recognition for almost all arriving passengers (other than those U.S. citizens who opt out), and CBP is working with the port and its airline partners to incorporate this technology into departing international passenger processes.

Facial recognition is also increasingly being utilized by the port's private sector partners. Delta Air Lines opened the first full biometric airport terminal in Atlanta in November 2018, and is working to bring aspects of their "curb to gate" experience to SEA. Similarly, many of the port's cruise partners are working to streamline the check-in and boarding process for their travelers through facial recognition.

Some members of the public and various advocacy organizations have expressed concerns about the rapidly expanding use of facial recognition. These stakeholders have raised issues around privacy, equity, and civil liberties, although their main focus has been on broad law enforcement use of this technology for "mass surveillance" rather than the kind of customer facilitation uses that are being considered at port facilities. They view the use of appropriate regulation to ensure protections against abuse, discrimination, and unintended consequences to be a condition for approval of the use of these technologies.

○ **Appendix D – CBP Letter to the Port**

1300 Pennsylvania Avenue NW
Washington, DC 20229

**U.S. Customs and
Border Protection**

Port of Seattle Commission
2711 Alaskan Way
Seattle, WA 98121

Dear Commissioners,

U.S. Customs and Border Protection (CBP) is in possession of a draft copy of the Port of Seattle's proposed document concerning the principles for use of biometric technology at Seattle port facilities, and is aware that this motion will be considered at a Commissioners meeting on December 10, 2019.

This letter is to confirm CBP's agreement with the principles outlined in the motion and to commend the Port of Seattle Commission on its efforts regarding adoption of biometric technology at its facilities. CBP agrees with the Port of Seattle's biometric principles and finds they align fundamentally with CBP's mission and approach to better secure our nation by incorporating biometrics into its comprehensive entry-exit system.

In support of the motion, CBP provides the following explanation on how CBP lives by these principles today in application of facial recognition technology in its biometric matching service, the Traveler Verification Service (TVS).

Seattle Port Principle & CBP Alignment

1) **Voluntary:** *The use of biometrics to identify and validate travelers through Port facilities should be voluntary, and reasonable alternatives should be provided for those who do not wish to participate – through a convenient "opt-in" or "opt-out" process, except in specific situations authorized by the Port or required by federal law such as U.S. Customs and Border Protection's (CBP) entry and exit requirements for non-U.S. citizens. Unintended capture of data by biometric technology from those travelers opting out of such biometric data collection, or of any non-travelers or other visitors at the airport, should be prevented; any unintended capture of this data should not be stored.*

   CBP Alignment: U.S. citizens are not within the scope of CBP's biometric entry-exit program, and those who do not wish to have a photo taken may request alternative processing, which typically involves a manual review of their travel documents. CBP posts information on opt-out procedures near the point of departure or arrival into the United States.

2) Private: *Data collected by biometric technology at Port facilities or by Port employees from travelers through Port facilities should be stored for no longer than required by applicable law or regulations, and should be protected against unauthorized access. The Port opposes this data being knowingly sold or used for commercial purposes unrelated to processing travelers at Port facilities without their clear and informed consent.*

> **CBP Alignment:** As outlined in the TVS Privacy Impact Assessment (*DHS/CBP/PIA-056 Traveler Verification Service – November 2018[1]*), once a match is made, U.S. citizens' photos are retained for no more than 12 hours in the TVS cloud for disaster recovery purposes, then deleted. CBP retains only a confirmation of the crossing and the associated biographic information. No photos of U.S. citizens are retained under this process.

> Facial images for arriving and departing foreign nationals are retained by CBP for up to two weeks, not only to confirm travelers' identities but also to assure continued accuracy of the algorithms. As always, facial images of arriving and departing foreign nationals are forwarded to the U.S. Department of Homeland Security Automated Biometric Identification System (IDENT) system for future law enforcement purposes, consistent with established DHS processes and regulations[2].

> CBP's Business Requirements do not allow its approved partners such as airlines, airport authorities, or cruise lines to retain the photos taken under this process for their own business purposes. The partners must immediately purge the images following transmittal to the TVS, and the partner must allow CBP to audit compliance with this requirement.

3) Equitable: *The Port opposes discrimination or systemic bias based on religion, age, gender, race or other demographic identifiers. Biometric technology used at Port facilities or by Port employees should be reasonably accurate in identifying people of all backgrounds, and systems should be in place to treat mismatching issues with proper cultural sensitivity and discretion.*

> **CBP Alignment:** CBP is fully committed to the fair, impartial and respectful treatment of all members of the trade and traveling public. CBP has rigorous processes in place to review data and metrics associated with biometric entry and exit facial comparison performance. Significant variance in match rates that can be attributed to demographic variables have not been detected. Additionally, CBP is partnering with the National Institute of Standards and Technology (NIST) to conduct a comprehensive analysis of facial comparison technology used in CBP's biometric entry-exit efforts, in order to improve data quality, integrity, and accuracy.

4) Transparent: *Use of biometric technology for passenger processing at Port facilities should be communicated to visitors and travelers. Individuals should be notified about any collection*

---

[1] DHS/CBP/PIA-056 Traveler Verification Service - November 2018 is available at: https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service-0.

[2] DHS/OBIM/PIA-001 Automated Biometric Identification System is available at: https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

of their biometric data to facilitate travel at Port facilities, and how that data may be used, in easily understood terms.

> **CBP Alignment:** CBP strives to be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). CBP works closely with partners to post the required privacy notice on signs for impacted travelers and the public in close proximity to the cameras and operators, whether the cameras are owned by CBP or the partners. In addition, tear sheets are available as requested.
>
> When airlines or airports are partnering with CBP on biometric air exit, the public is informed. We provide notice to travelers at the designated ports of entry through both printed and electronic signs, LED message boards, and verbal announcements to inform the public that photos will be taken for identity verification purposes and of their ability to opt-out of having their photo taken.

5) **Lawful:** *Use of biometric technology and/or access to associated biometric data collected should comply with all laws, including privacy laws and laws prohibiting discrimination or illegal search against individuals or groups.*

> **CBP Alignment:** CBP is committed to ensuring that our use of technology sustains and does not erode privacy protections. We take privacy obligations very seriously and are dedicated to protecting the privacy of all travelers. CBP complies with all federal legal requirements, including under the Privacy Act of 1974, as well as all DHS and government-wide policies. In accordance with DHS policy, CBP uses the Fair Information Practice Principles (FIPPs)[3] to assess the privacy risks and ensure appropriate measures are taken to mitigate any risks from the use of biometrics. As CBP is bound by the above mentioned privacy laws and policies and data collection requirements, partnering stakeholders are also held to the same standards, which ensures accountability with the public on how both government and the private sector use biometrics.

6) **Ethical:** *The Port and its partners should act ethically when deploying biometric technology or handling biometric data. Ethical behavior means actions which respect key moral principles that include honesty, fairness, equality, dignity, diversity and individual rights. In particular, use of biometrics at Port facilities should comply with Resolution No. 3747, establishing the Port's Welcoming Port Policy Directive to increase engagement with, and support for, immigrant and refugee communities.*

> **CBP Alignment:** CBP is fully committed to the fair, impartial and respectful treatment of all members of the trade and traveling public.

7) **Justified:** *Biometric technology at Port facilities should be used only for a clear intended purpose that furthers a specific operational need. The Port does not condone biometrics for*

---

[3] The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security is available at: https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf.
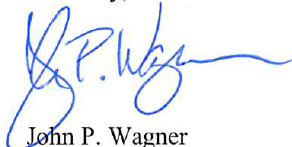
"mass surveillance" – for example, use of facial recognition on large groups of people without a lawful purpose, rather than single-use for travelers.

CBP Alignment: CBP TVS matches travelers to their travel documents only. It is not a surveillance program. CBP introduced the use of facial recognition technology into an already established process that requires the verification of an individual's identity when entering or exiting the United States. CBP is simply replacing the current manual travel document comparison with facial comparison technology.

As outlined in the TVS PIA, CBP and partners inform travelers of the process through signage and announcements describing how a photo is taken and submitted to the TVS; this photo is used solely for the purpose of matching the traveler to the travel document and ensuring that the travel document being presented belongs to the bearer of the document.

Again, CBP strongly supports the list of principles outlined by the Port of Seattle. We look forward to working with the Port of Seattle Commission on the use of facial comparison technology in Port of Seattle facilities.

Sincerely,

John P. Wagner
Deputy Executive Assistant Commissioner
U.S. Customs and Border Protection, Office of Field Operations