Committee Meeting Date: December 11, 2020

Policy Recommendations for Public-Facing Biometrics at Port Facilities

Eric Schinfeld, Sr. Manager, Federal Government Relations

Veronica Valdez, Commission Specialist

Port of Seattle®

Purpose

1. To transmit policy recommendations developed by the Port working group and reviewed by the Biometrics External Advisory Group to the Biometrics Special Committee for the following use cases:
   - Biometrics for Traveler Functions Using Private, Proprietary Systems
   - Biometrics for Traveler Functions Using Government Systems
   - Biometrics for Air & Cruise Entry

2. To receive Biometrics Special Committee feedback on the recommendations and potential process/timeline/format for Commission consideration

3. To receive a recommendation from the Biometrics Special Committee to the Commission with regards to the recommendations

BACKGROUND

Biometrics Motion 2019-13 (Adopted 12/10)

1. **Adopted seven (7) guiding principles** for public-facing biometrics at Port facilities: 1) Justified, 2) Voluntary, 3) Private, 4) Equitable, 5) Transparent, 6) Lawful, 7) Ethical
2. **Established a Port working group** to translate guiding principles into tangible & enforceable policy recommendations by the end of Q1 2020, for Commission passage by Q2 2020
3. **Established an external advisory group** to provide feedback on proposed Port working group policy recommendations
4. **Recommended the creation of an ad hoc, limited term commission committee** to oversee these efforts (Special Biometrics Committee)
5. **Put a hold on any new or expanded uses of biometrics at Port facilities until after Commission approves of policy recommendations and adopts policies**

Key Dates

- **Commission Engagement:**
  - Two (2) Commission Study Sessions: Sep 10, 2019 and Oct 29, 2019
  - Commission Action adopting Motion: Dec 10, 2019
  - Commission Briefing: Feb 25, 2020
  - Commission Actions: Mar 10, 2020 and Apr 14, 2020
- **Development/Review of Recommendations:**
  - Port Working Group meetings/review: Dec 2019 – Aug 2020
  - Eight (8) External Advisory Group Meetings facilitated by consultants: Jan 17, 2020 – Sep 25, 2020
- **Biometrics Special Committee:**
  - Three (3) Commission Biometrics Special Committee: Feb 18, 2020; Mar 31, 2020; and Oct 8, 2020

Process

1. **Policy recommendations by "use case" rather than one comprehensive policy**
2. **Port Working Group identified five "use cases"** for public-facing biometrics at Port facilities and **drafted policy recommendations** for each use case:
   - Biometric Air Exit (Submitted and Approved)
   - Biometrics for Law Enforcement & Security Functions (Tabled, Moratorium)
   - Biometrics for Traveler Functions Using Private, Proprietary Systems
   - Biometrics for Traveler Functions Using Government Systems
   - Biometrics for Air & Cruise Entry
3. **External Advisory Group reviewed policy recommendations for each use case and provided feedback during facilitated meetings**
4. **Biometrics Special Committee reviewed policy recommendations for each use case**

Observations

- Not “consensus” recommendations
  - All stakeholder concerns are being submitted along with the staff recommendations to provide full transparency
  - Offered opportunity to advisory group members to submit letters outlining their concerns
- As per Motion 2019-13, these 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 if the Commission decides it is appropriate.

USE CASES

Law Enforcement & Security Functions

- Use of biometrics, including facial recognition, to perform public-facing law enforcement and security functions at Port facilities.
  - On July 14, 2020, the Port Commission extended its moratorium on these uses as part of its motion on assessing Port policing.
  - Therefore, staff did not vet its policy recommendations with the Biometrics External Advisory Group, and is not transmitting those recommendations to Commission.
  - If and when the Commission wishes to revisit the issue, Port staff will vet its draft policy recommendations with external stakeholders at that point.

Air and Cruise Entry

- **CBP's** use of biometrics, specifically facial recognition, utilizing their TVS to confirm the identities of **arriving international passengers as they exit aircraft or cruise ships**.
  - Entry into the United States is a federally regulated process, and all persons arriving at a port-of-entry to the United States are subject to inspection by CBP before entering the country.
  - The Port has no jurisdiction over these activities, but can still play an important transparency and accountability role.

Traveler Functions Using Private, Proprietary Systems

- Use of biometrics for traveler functions by **private-sector entities using proprietary systems**. For example:
  - Current use: CLEAR
  - Potential future use:
    - Boarding of departing cruise ships or domestic flights
    - Ticketing and bag-check for airlines or cruise lines
    - Access to tenant-controlled facilities e.g. airline passenger lounge
    - Access to a rental car at the Port's rental car facility;
    - Payment at airport restaurants or retail stores in lieu of credit card or cash.

Traveler Functions Using Government Systems

- Use of biometrics for traveler functions where a **private sector entity might wish to use an existing government biometrics system**. For example:
  - An airline using CBP's Traveler Verification System for international departing passenger ticketing or bag check
  - The Port could use biometrics for access to its parking garage
  - Any Port use of biometrics utilizing a Port-controlled system is by definition a use of a government system, and therefore included in this use case.

RECOMMENDATIONS

Biometrics for Traveler Functions (Private Sector)

- The Port ***should not allow*** private sector entities to implement public-facing biometrics at Port facilities unless:
  - The relevant Managing Director first seeks feedback from the Technology Ethical Advisory Board and considers set criteria in deciding whether or not to approve the implementation.
  - The Managing Director has notified the Port Executive Director and the Port Commission at least three (3) weeks before providing formal approval to the private sector applicant.
  - The proposed application is "opt-in", both in terms of opting-in to the overall system as well as actively choosing to participate in the system at the point of service.
  - The private sector operator agrees to the Port's standards and training protocols regarding avoiding unintended image capture.
  - The proposed usage does not scan individuals or groups without their knowledge and active participation.
  - The proposed technology meets and/or exceeds the Port's minimum biometric data security and privacy standards.
  - Those staff operating the technology agree to be trained to the Port's standards on how to deal with mismatching issues with sensitivity and discretion, and how to minimize mismatch likelihood, such as lighting, image capture angles and camera quality.
  - The private sector operator verifies that their technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington State definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions.
  - The private sector operator agrees to make available an application programming interface (API) or other technical capability, to enable legitimate, independent, and reasonable tests of those biometric technologies for accuracy and unfair performance differences across distinct subpopulations.
  - The proposed usage complies with all relevant state and federal laws, including privacy and discrimination laws.
  - The private sector operator agrees not to disclose personal data obtained from a biometric system to a federal or law enforcement agency, except when such disclosure is legally required.

Biometrics for Traveler Functions (Private Sector)

- If the Port approves such an application, it should:
  - Form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations.
  - 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, how to remove themselves from the program, and recourse in case of violations of those rights and/or data breaches.
  - Work with the Technology Ethical Advisory Board to produce an annual accountability report that includes all approved, publicly available information.
  - Conduct performance evaluations to ensure that Port staff and/or private sector operators are following all Port policies, including those related to privacy, customer service, communication and unintended image capture.
  - Actively track and work with stakeholders, including private sector operators at Port facilities, to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.
  - Develop biometric training guidelines for personnel who will be administering the facial recognition technology on travelers, including the capabilities and limitations of facial recognition, and how to deal with mismatching issues with sensitivity and discretion.
  - Develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about that biometric 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.
  - 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.

Biometrics for Traveler Functions (Public Sector)

- *The Port **should not allow** Port employees to implement public-facing biometrics at Port facilities – or private sector entities to implement public-facing biometrics for traveler functions using CBP's system – unless*:
  - The relevant Managing Director first seeks feedback from the Technology Ethical Advisory Board and considers set criteria in deciding whether or not to approve the implementation.
  - The Managing Director has notified the Port Executive Director and the Port Commission at least three (3) weeks before providing formal approval to the private sector applicant.
    - If the request is for implementation of biometrics for travel functions using CBP's TVS system, the Managing Director should only consider the request if a Biometric Exit program has already been implemented and if all of CBP's Biometric Requirements regarding encryption and other security standards are complied with.
    - If Port staff receive approval from the Managing Director, they must then submit a notice of intent to the Port Commission and commence an accountability report process as defined in state law that publicizes key aspects about the biometric technology.
  - The proposed application is "opt-in", both in terms of opting-in to the overall system as well as actively choosing to participate in the system at the point of service.
  - The operator agrees to adhere to the Port's standards and training protocols regarding avoiding unintended image capture.
  - The proposed usage does not scan individuals or groups without their knowledge and active participation.
  - The proposed technology meets and/or exceeds the Port's minimum biometric data security and privacy standards.
  - Those staff operating the technology agree to be trained to the Port's standards on how to deal with mismatching issues with sensitivity and discretion, and how to minimize mismatch likelihood, such as lighting, image capture angles and camera quality.
  - The operator verifies that their technology demonstrates high levels of accuracy both overall and between various characteristics – particularly those relevant to biometric identification – as identified under the Washington State definition of "protected class." These demonstrations of accuracy must result from testing in operational conditions.
  - The operator agrees to make available an application programming interface (API) or other technical capability, to enable legitimate, independent, and reasonable tests of those biometric technologies for accuracy and unfair performance differences across distinct subpopulations.
  - The proposed usage complies with all relevant state and federal laws, including privacy and discrimination laws.
  - The operator agrees not to disclose personal data obtained from a biometric system to a federal or law enforcement agency, except when such disclosure is legally required.

Biometrics for Traveler Functions (Public Sector)

- *If the Port approves such an application, it should:*
  - Form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations.
  - Include in the vendor solicitation document – if the proposed implementation of biometrics for traveler functions by Port staff requires a procurement – a request for explanation of how the vendor's technology will comply with the Port's Biometric Principles and policies; how its technology can help minimize the unintended capture of images of nontravelers or visitors, if an image is used as part of the biometrics; how the technology solution will meet the Port's biometric Privacy principles and policies, including by providing relevant privacy policies, data collection and storage practices, and cybersecurity practices; how it will meet the Port's Equity principle and policies; and how their equipment and services enhance accuracy levels in identifying peoples of all backgrounds, gender, and age.
  - Seek clarification from the State of Washington Attorney General whether Port collection and transmission of biometric data at Port facilities is exempt from state public disclosure requirements, so as to protect personally identifying information from release.
  - Request updated accuracy rates from CBP – including a request for any available data segmented by key traveler characteristics – before approving any proposed use of biometrics for traveler functions that would use the CBP system.
  - 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, how to remove themselves from the program, and recourse in case of violations of those rights and/or data breaches.
  - Work with the Technology Ethical Advisory Board to produce an annual accountability report that includes all approved, publicly available information.
  - Develop biometric training guidelines for personnel who will be administering the facial recognition technology on travelers, including the capabilities and limitations of facial recognition, and how to deal with mismatching issues with sensitivity and discretion.
  - Conduct performance evaluations to ensure that Port staff and/or private sector operators are following all Port policies, including those related to privacy, customer service, communication and unintended image capture.
  - Actively track and work with stakeholders, including private sector operators at Port facilities, to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.
  - Develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about that biometric 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.
  - 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.

CBP Use of Biometric Entry

- If CBP implements biometric entry at the Port's airport or cruise facilities, the Port should:
  - Develop recommendations to CBP for their consideration regarding ways to avoid unintended image capture at Port facilities.
  - Continue to pursue whether opt-out is an option for biometric entry at Port facilities.
  - Design training guidelines to help cruise line employees educate disembarking passenger about CBP rules regarding opt-out.
  - Request biometric program accuracy rates from CBP on an annual basis, including a request for any available data segmented by key traveler characteristics.
  - Request that CBP make available an application programming interface (API) or other technical capability, to enable legitimate, independent, and reasonable tests of those biometric technologies for accuracy and unfair performance differences across distinct subpopulations.
  - Develop suggested biometric training guidelines for personnel who will be administering the facial recognition technology on travelers, including the capabilities and limitations of facial recognition, and how to deal with mismatching issues with sensitivity and discretion.
  - Share its training guidelines, specifically related to "cultural sensitivity and discretion", with CBP and cruise lines for their voluntary adoption.
  - Develop a comprehensive communications plan that notifies the general public of the implementation and all related information.
  - Produce an annual accountability report that includes all approved, publicly available information on related topics.
  - Request CBP audit reports on biometric entry systems on a regular basis and include appropriate information in the annual accountability report.
  - Include the specific federal laws and statutes that allow CBP to implement biometrics at Port facilities in the annual accountability report.
  - Actively track and work with stakeholders to advocate for federal laws and regulations that support the Port's biometric principles.
  - Develop an engagement plan with local jurisdictions, nonprofit organizations and others to educate local immigrant and refugee communities about the biometric entry 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.
  - 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.

Questions?

Public-Facing Biometrics Guiding Principles

Justified	Should be used only for a clear and intended purpose and not for surveillance on large groups without a lawful purpose
Voluntary	Should be voluntary and reasonable alternatives should be provided for those who not wish to participate through an opt-in or opt-out process
Private	Should be stored for no longer than required by applicable law or regulations, and should be protected against unauthorized access
Equitable	Should be reasonably accurate in identifying people of all backgrounds, and systems should be in place to treat mismatching issues
Transparent	Should be communicated to visitors and travelers
Lawful	Should comply with all laws, including privacy laws and laws prohibiting discrimination
Ethical	Should act ethically when deploying technology or handling biometric data

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

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 Medhi, 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

Biometric Air Exit

- Use of biometrics, specifically facial recognition technology, to verify the identity of **departing international air passengers** using US Customs & Border Protection's (CBP) Traveler Verification System (TVS).
  - First use case reviewed
  - Policy recommendations were reviewed by the Biometrics Special Committee on Feb 18, 2020
  - Policy recommendations were approved by the Commission on Mar 10, 2020
  - Executive Policy developed EX-22 on Apr 3, 2020
  - Review by the External Advisory Group was expedited due to Commission Action in March. Some stakeholders felt they did not have enough time to fully vet the recommendations