BIOMETRICS FOR TRAVELER FUNCTIONS BY PORT EMPLOYEES OR NON-AIRLINE, PRIVATE SECTOR TENANTS POLICY

12/17/21

EX-28 As of 12/17/21

I. BACKGROUND

Biometrics is the use of technology to identify an individual through analysis of that person's physical and behavioral characteristics. 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 has been a significant increase in public-facing biometric technology deployment by public and private sector users in aviation and maritime settings. 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. These functions are driven entirely by perceived business advantages, customer convenience or public health benefit, and not required by any local, state, or federal government regulation. The COVID-19 pandemic may spur additional attention toward potential applications of biometric technology so as to avoid direct interactions that could spread the virus.

Other than airline use of biometrics for traveler functions and U.S Customs and Border Protection's (CBP) Biometric Entry and Biometric Exit programs (which are both covered under separate executive policies), there are only a few current applications of biometrics for this kind of use at Port facilities, most notably CLEAR at Seattle-Tacoma International Airport (SEA), which allows travelers to use fingerprint and iris scans as identity verification to advance to the front of U.S. Transportation Security Administration (TSA) checkpoints. While private, proprietary biometric technologies may be utilized by different tenants and operators at the airport, some tenants and operators may utilize CBP's existing TVS system, as part of their boarding, bag-check, and other operations. Examples of potential future biometric (including facial recognition) applications for traveler functions at Port facilities could include:

- Boarding of departing cruise ships;
- Ticketing and bag-check for cruise ships;
- Access to a rental car at the Port's rental car facility;
- Use of biometrics for payment at airport restaurants or retail stores in lieu of credit card or cash; or
- Use of biometrics to inform dynamic signage targeting information or advertisements to travelers.

Many members of the public and various advocacy organizations have expressed concerns about the rapidly expanding use of facial recognition and other public-facing biometrics. These stakeholders have raised issues around privacy, equity, and civil liberties, as well as the potential for unregulated "mass

surveillance." To that end, the Port Commission passed Motion 2019-13 on December 10, 2019 which instituted guiding principles for the public-facing use of biometric technology at Port facilities.

After more than a year and a half of work and approximately twenty public meetings, Port staff developed policy recommendations to operationalize the guiding principles. To implement those recommendations, the Commission passed Order 2021-XX, which directs the Executive Director to create an executive policy regulating the use of public-facing biometrics for traveler functions. Again, the policies below are specific to Port staff or non-airline tenants and operators since airline use and federal government use of public-facing biometrics at Port facilities are covered under separate executive policies.

II. POLICY STATEMENT

The following policies will be implemented by the Port of Seattle as directed by the Port of Seattle Commission to regulate the use of public-facing biometric technology for traveler functions at Port facilities by Port staff as well as private sector tenants and operators other than airlines (hereinafter, "Port tenants"):

Policy 1 – Creation, and Role of, a Technology Ethical Advisory Board:

- By January 2022, the Port will form a Technology Ethical Advisory Board to advise on the ethical issues raised by implementation of biometric technology and other innovations.

- This Board will be composed of no more than five members – appointed by the Commission President. Members of the Board should be technology experts with specific expertise in the field of biometrics, academic researchers will expertise in biometric technology and/or technology ethics, and/or policy professionals who have experience with regulating technology to balance practical benefits with ethical and equity concerns. Members will serve three-year terms, and can be nominated for an unlimited number of consecutive terms.

- The Board will meet as requested by Port staff, to help advise on the issues listed below. The Board will not take votes or have direct decision-making authority, but rather provide their advice for consideration. While Board advice is non-binding, its recommendations must be shared with Commissioners and the Executive Director as part of any approval process for new public-facing biometric technology.

- Until January 2022, the input already received by the Biometrics External Advisory Group will count in lieu of feedback from the Technology Ethical Advisory Board.

Policy 2 – Application to the Managing Director:

- Port staff or Port tenants who wish to implement public-facing biometric technology for traveler functions at Port facilities must submit a request to the relevant Port Managing Director (i.e. aviation or maritime). The Managing Director will seek feedback from the Technology Ethical Advisory Board and then consider the following criteria in deciding whether or not to approve the additional implementation:
    - Demonstrated operational benefit, which is defined as increased efficiency or effectiveness in passenger processing vs existing manual processes;
    - Compliance with all Port Biometrics principles and policies;

- Compliance with all relevant state and federal laws, including privacy and discrimination laws;
- If relevant, compliance with all CBP requirements, such as documentation that the proposed process has been approved by CBP, and is in compliance with CBP's Biometric Air Exit Requirements and TVS application programming interface (API) specifications;
- Alignment with the Port's Equity, Diversity and Inclusion standards; and
- Net benefit-cost to travelers – both overall and for specific subsets of travelers – of the added customer facilitation versus potential privacy and other risks, with also due consideration for the Port's own airport and cruise logistical and operational considerations. If the risks are deemed significant, then the Managing Director should deny the application regardless of the net-benefit calculation; "significant risk" should be clearly defined in partnership with the Technology Ethical Advisory Board, to include harms based on equity impacts.

- If the request is for implementation of public-facing biometrics for marketing or advertising purposes, the Managing Director should only approve the application if:
  - The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose;
  - The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent; and
  - The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment.

- Any Port tenant using public-facing biometric technology for traveler functions at Port facilities prior to the passage of Order 2021-XXXX will be required to comply with the Port's public-facing biometrics policies as part of its next lease or contract. At least six months in advance of the expiration of its existing agreement, Port staff will be responsible for notifying the operator of the need to include these provisions in its new agreement, as well as additional information about the biometrics approval process and all associated policies.

Policy 3 – Notification to Port Leadership Regarding a Private Sector Application:

- If the request is by a Port tenant and the Managing Director plans to approve the request after considering all the above criteria, they must first notify the Port Executive Director and the Port Commission at least three (3) weeks before providing that formal approval to the private sector applicant. The purpose of this notification is to provide public transparency and to allow the Executive Director and/or Commission to ask additional questions, request a delay in approval until additional information is received, and/or reject the Managing Director's recommendation for approval. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies, or 2) multiple violations of Port policies as identified through performance evaluation.

Policy 4 – Notification to Port Leadership Regarding a Port Staff Application:

- If the request is by Port staff and the Managing Director plans to approve the request after considering all the above criteria, 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, such as the name of the service, vendor, and version; a description of its general capabilities and limitations; the type or types of data

inputs that the technology uses; how that data is generated, collected, and processed; a description of the purpose and proposed use of the technology, including what decision or decisions will be used to make or support it; a clear use and data management policy; any complaints or reports of bias regarding the service received by the vendor; testing procedures; information on the service's rate of false matches; a description of any potential impacts of the service on civil rights and liberties; and procedures for receiving feedback from individuals affected by the use of the service and from the community at large.

Prior to finalizing the accountability report, the Port must – in compliance with state law – allow for a public review and comment period; hold at least three community consultation meetings; and consider the issues raised by the public through the public review and comment period and the community consultation meetings. The final adopted accountability report must be clearly communicated to the public at least ninety days prior to the Port putting the service into operational use, and be posted on the Port's website.

- After the accountability report process is completed as described above, if the proposed implementation of biometrics for traveler functions by Port staff does not require a Commission authorization, the Managing Director must notify the Port Executive Director and the Port Commission at least three (3) weeks before the technology is procured. The purpose of this notification is to allow the Executive Director and/or Commission to ask additional questions, request a delay in approval until additional information is received, and/or reject the Managing Director's recommendation for approval. Approvals, once provided, are ongoing, unless there is 1) a substantial change in operations that impacts the operator's compliance with Port policies, or 2) multiple violations of Port policies as identified through performance evaluation.

- If the requested implementation of biometrics by Port staff does require a Commission authorization, then the Commission memo must include the final accountability report, an explanation of how the proposal complies with the Port's Biometric Principles and policies, a recommendation from the relevant Managing Director on how and why this request meets the Justified principle and any feedback from the Technology Ethical Advisory Board.

Policy 5 – Port Procurement Process:

- If the proposed implementation of biometrics for traveler functions by Port staff requires a procurement, the request for proposals must include 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.

Policy 6 – Port Definition of a Voluntary, "Opt-in" System:

- Unless there is a legal mandate, such as from a federal agency or a public health entity, all proposed applications of public-facing biometrics for traveler functions must be voluntary and individuals must "opt-in" – both opting-in to the overall system as well as actively choosing to participate in the system at the point of service. For the purposes of this policy, opt-in is further defined as:

- The system only includes the biometric data of those individuals who have actively opted-in to the system for that explicit purpose, other than systems like CBP's TVS that use passport or visa application data submitted to and held by the federal government;
- The system does not include biometric data purchased from a third-party without the individual's explicit consent, nor biometric data collected from publicly available galleries (such as social media sites) without the individual's explicit consent;
- The system only scans those individuals who have actively opted-in and only when they are purposefully and actively participating in that particular moment;
- Comprehensive, clear, and accessible notice is provided at the time of enrollment (i.e. – "informed consent") for individuals to know exactly what they are opting-in for, how their data will be handled and protected and their rights to remove their data from the system;
- There are clear standards for how to cancel a subscription or other voluntary commitment such that an individual's biometric data is removed from the system;
- Standards are in place to avoid unintended image capture, such as by positioning a 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;
- Standards are in place to handle biometric data accidentally collected by unintended capture, including immediate deletion; and
- The system does not operate by scanning large groups of people who have not opted-in in order to identify those individuals who have opted in.

Policy 7 – Port Standards for Unintended Image Capture and Operator Training:

- The Port will develop standards to avoid unintended image capture if facial recognition (or a similar image-based biometrics system) is implemented (such as by positioning a 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), as well as standards for how to handle biometric data accidentally collected by unintended capture, including immediate deletion.

- The Port will 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. The training should also include standards for minimizing mismatch likelihood, such as lighting, image capture angles and camera quality.

- The Port will require all Port staff operating the technology at Port facilities 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 Port will also – to the extent allowable – have non-Port personnel operating at Port facilities be trained to the Port's standards – either using the Port's curriculum or a comparable alternative.

Policy 8 – Port Standards for Data Privacy:

- The Port will develop minimum biometric data security and privacy standards for biometrics for traveler functions at Port facilities. Those standards should address data privacy protections at the point of service as well as throughout the proprietary system, such as potential data breach and data sharing. The standards should include requirements that any data collected should be used only for those purposes explicitly communicated to those individuals who participate in the

biometric process, and that unauthorized third parties will not have access to or be sold any such data. These guidelines should be based – to the extent possible – on national and global standards already developed for evaluating the security of these technologies.

- Within the limitations of its ability to do so, the Port will require that all approved public-facing biometric technology for traveler functions at Port facilities meet or exceed the Port's minimum biometric data security and privacy standards.

- For any proposed implementations of biometrics for traveler functions that have obligations related to U.S. Transportation Security Administration security and data privacy regulations, the proposal must demonstrate full alignment with all of the Port's Air Security Program rules and requirements.

Policy 9 – Port Standards for Accuracy:

- Within the limitations of its ability to do so, the Port will require that all approved public-facing biometric technology for traveler functions at Port facilities must be verified to demonstrate 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.
    - "High levels of accuracy" is defined not only relative to correctly matching the person with their image but also as an accuracy rate that is at least as good as human review. Port staff should include in their disclosure of accuracy rates the specific device and system settings – such as similarity thresholds – that maximize accuracy and provide the proper balance of accuracy, equity, and security.

- Within the limitations of its ability to do so, the Port will require that approved public-facing biometric technology must 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. Making an application programming interface (API) or other technical capability does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data; providers bear the burden of minimizing these risks when making an application programming interface or other technical capability available for testing. This requirement does not apply to applications using the CBP TVS system, since the federal government cannot be compelled to comply with this requirement; however, the user should provide the Port any publicly available information about the TVS system's compliance with these goals.

Policy 10 – Port Standards for Disclosure of Biometric Data:

- Port staff may not disclose personal data obtained from biometric technology to a federal or law enforcement agency, except when such disclosure is:
    - Pursuant to the consent of the consumer to whom the personal data relates;
    - Required by federal, state, or local law or in response to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer or grand jury;
    - Necessary to prevent or respond to a national security issue or an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the operator; or

- To the national center for missing and exploited children, in connection with a report submitted thereto under Title 18 U.S.C. Sec.2258A.

- To the extent permissible by state and federal law, the Port will request that Port tenants abide by these standards as part of their deployment at Port facilities.

Policy 11 – Public Disclosure Requests:

- The Port will seek clarification from the State of Washington Attorney General as to 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.

Policy 12 - Port Communications and Transparency Efforts:

- If the Port approves any implementation of biometrics for traveler functions at Port facilities, Port staff must develop and implement a comprehensive communications plan that notifies the general public of the implementation and all related information, including information pertaining to traveler rights with regard to the program, how to remove themselves from the program if possible, and avenues of potential recourse in case of violations of those rights and/or data breaches. The communications plan should include specific communications on-site, including announcements, signage, flyers, and web content. The communications plan should include effort to reach local immigrant and refugee communities – in multiple languages and in culturally appropriate ways; languages should be determined based on the most common ones spoken by airport and/or cruise passengers.

- If the Port approves any implementation of biometrics for traveler functions at Port facilities, Port staff must work with the Technology Ethical Advisory Board (once formed) to produce an annual accountability report that includes all approved, publicly available information on topics such as:
  - A description of the biometrics being used, including the name of the biometric vendor and version;
  - The system's general capabilities and limitations;
  - How data is generated, collected, and processed;
  - A description of the purpose and proposed use of the biometrics, and its intended benefits, including any data or research demonstrating those benefits;
  - A clear use and data management policy, including protocols for:
    - How and when the service will be deployed or used and by whom including, but not limited to, the factors that will be used to determine where, when, and how the technology is deployed, and other relevant information, such as whether the technology will be operated continuously or used only under specific circumstances.
    - Any measures taken to minimize inadvertent collection of additional data beyond the amount necessary for the specific purpose or purposes for which the service will be used;
    - Data integrity and retention policies applicable to the data collected using the service, including how the operator will maintain and update records used in connection with the service, how long it will keep the data, and the processes by which data will be deleted;
  - The Port and the Port tenant's privacy guidelines, as well as CBP's privacy guidelines if relevant;
  - Information pertaining to traveler rights with regard to the biometric system;

- The Port's biometric training guidelines;
- The operator's testing procedures, including its processes for periodically undertaking operational tests of the service;
- A description of any potential impacts of the service on civil rights and liberties, including potential impacts to privacy and potential disparate impacts on marginalized communities, and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use of the service;
- Procedures for receiving feedback, including the channels for receiving feedback from individuals affected by the use of the service and from the community at large, as well as the procedures for responding to feedback;
- Any known or reasonably suspected violations of the Port's and the operator's rules and guidelines, including complaints alleging violations;
- Any publicly available data about the accuracy and effectiveness of the system, including accuracy overall as well as accuracy for specific demographics; and, where possible, any specific device and system settings – such as similarity thresholds – that speak to how the operator is balancing accuracy, equity and security.
- Benchmarking data against the operational results of the biometric system at other ports;
- An assessment of compliance with the Port's Biometrics Principles and policies, as well as CBP's Biometric Air Exit Requirements, if relevant;
- Any Port conducted performance evaluations, as well as any publicly available CBP audits of the biometric air exit system, if relevant;
- 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, if relevant; and
- Any Port tenant's disclosure of individuals' biometric data, within the limitations of the Port to access and disclose law enforcement activity.

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

Policy 13 – Compliance with Port Policies:

- Within the limitations of its authority, the Port should periodically conduct performance evaluations to ensure that Port staff and/or Port tenants are following all relevant Port policies, including those related to privacy, customer service, communication, and unintended image capture. In particular, the Port should ensure that images are retained no longer than necessary, and used only for their intended purpose. The Port will limit its performance evaluation of private sector implementations of public-facing biometrics for traveler functions at Port facilities only to those areas for which the Port has legal and/or contractual ability to review and enforce.

- If a Port tenant is found to have repeatedly violated the Port's policies after more than two notifications asking for corrective action, the Port reserves the right to withdraw its approval of the biometric implementation.

Policy 14 – Port Advocacy Efforts:

- The Port will work with Port tenants and other stakeholders to advocate for state and federal laws and regulations that codify the goals of the Port's biometric principles.

Policy 15 – Port Outreach Efforts:

- The Port will 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 information pertaining to traveler rights – in multiple languages and in culturally appropriate ways.

- The Port will 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.

III. PROCEDURES FOR NOTICE

- The Port will inform employees about this policy by posting it online at: http://compass.portseattle.org/corp/legal/Pages/PoliciesandProcedures.aspx#exec
- The Port will train relevant Port employees and other associated corporate staff on this policy.
- The Port will communicate this policy directly to Port tenants and federal agencies operating at Port facilities through existing communication channels.
- The Port will communicate this policy to all relevant external stakeholders, elected officials and impacted community organizations through existing communication channels.

The Executive Director will work with Port staff to develop any necessary rules and regulations as necessary to implement the policies set forth herein.

IV. VIOLATIONS

In accordance with the Port of Seattle's Standards of Performance and Conduct, Corrective Action and Discipline policy (HR-18), employees who violate this policy may be subject to disciplinary action, up to and including termination.

All employees have a responsibility for ensuring that this policy is followed. Concerns and potential violations should be reported to the Workplace Responsibility Officer, or anyone identified in the "Reporting Concerns Violations" policy.

The Port of Seattle strictly prohibits retaliation against any employee for making a good faith report of any potential or suspected violation of this policy or for cooperating in any investigation of such violation.

For further information contact Eric Schinfeld.