BIOMETRIC MASS SURVEILLANCE POLICY

EX-24 As of 12/17/21

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 airport and seaport settings – specifically the use of facial recognition biometrics for boarding and disembarkation of international flights and cruises, and for traveler functions such as ticketing and bag check. In fact, 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 – because of the potential for a faster and more efficient travel experience, a more accurate security process and the public health benefits of moving to a "touchless" system.

At the Port of Seattle's aviation and maritime facilities, examples of biometric technology implementation include 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) use of U.S. Customs and Border Protection's (CBP) Traveler Verification System (TVS) at Seattle-Tacoma International Airport (SEA) to validate arriving and departing international traveler identities via facial recognition; and 3) use of CBP's TVS 66 to validate the identities of disembarking passengers from Norwegian Cruise Line ships docked at Pier.

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, Commission Motion 2019-13 explicitly prohibits – to the greatest extent permissible by state and federal law – mass surveillance using public-facing biometric technology at Port facilities.

In order to ensure that this ban on mass surveillance using public-facing biometric technology is applied in a comprehensive way at Port facilities and in relation to all Port-controlled activities, the Commission passed Order 2021-XX, which directs the Executive Director to implement an overarching ban on the use of biometric technology for mass surveillance.

II. POLICY STATEMENT

The following policies will be implemented by the Port of Seattle as directed by the Port of Seattle Commission to prohibit – to the greatest extent permissible by state and federal law – the use of public-facing biometric technology for mass surveillance:

Policy 1 – Definitions:

- The Port will define "using public-facing biometric technology for mass surveillance" as any real time or near-real time use of biometric technology to identify individuals without both their awareness and active participation.

- The Port will define "public-facing" as any areas of Port facilities where visitors, travelers and other non-employees might reasonably be.

- This definition applies both to:
  - The direct use of biometric technology at Port facilities, such as a facial recognition camera capturing the identities of travelers at the airport without their awareness and active participation; and
  - The use of biometric technology by Port employees in any other setting, such as a Port Police Department mutual aid deployment.

Policy 2 – Prohibitions:

- Port employees are prohibited from purchasing, using, or assisting in the use of public-facing biometric technology for mass surveillance, unless required to do so by state or federal law.

- To the extent permissible by state or federal law, the Port prohibits the use of public-facing biometric technology for mass surveillance by any tenant or other non-Port entity operating at Port facilities. In situations for which the Port cannot prohibit such use – such as a deployment by federal law enforcement with a court order to do so – it will share its preference that the deployment be limited in time and scope and that every effort be taken to minimize the potential impact to unrelated individuals using Port facilities.

Policy 3 – Port Standards for Voluntary, Opt-in System:

- To the greatest extent permissible by state and federal law, the Port will strive to ensure that all uses of public-facing biometric technology at Port facilities be voluntary and "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 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.

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 private sector 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.