

**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 “opt-out” 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.

STATEMENT IN SUPPORT OF THE MOTION

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-Tac), airport employees are required to scan their fingerprint at many secure doors throughout the facility. Sea-Tac 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-Tac'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-Tac. 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.