From: Valdez, Veronica
Sent: Tuesday, December 10, 2019 3:57 PM
To: Correspondence@spmail.portseattle.org; White, Paul; Smith, Lauren (Commission)
Cc: Mills, Pete; Schirato, LeeAnne; Merritt, Mike; Pritchard, Aaron
Subject: FW: [EXTERNAL] Sole Sourced Contract At SEATAC.

Follow Up Flag: Follow up
Flag Status: Flagged

From: Lawrence Richards <lawrencerichards275@yahoo.com>
Sent: Tuesday, December 10, 2019 2:05 PM
To: Steinbrueck, Peter <Steinbrueck.P@portseattle.org>; Bowman, Stephanie <Bowman.S@portseattle.org>; Gregoire, Courtney <Gregoire.C@portseattle.org>; Calkins, Ryan <Calkins.R@portseattle.org>
Subject: [EXTERNAL] Sole Sourced Contract At SEATAC.

Commissioners, I write to you today regarding the Agenda Item 6H. This is a sole sourced contract that gives Siemens a blank check. By sole sourcing the public is being denied a competitive and transparent use of public monies. If you simply required the RFP to include an OPEN Source specification. The Airport and citizens of the Pugent Sound area will get a better and more competitively sourced system. I ask you to review and look at what other Airports have done. Specifically Atlanta's Hartsfiels and Minneapolis St. Paul. They have speced open source products. This allows true competition. Look at the current system iit was insatlled in the 90's by a single vendor. Service and constructions has been to a signle provider. Has that been a good use of funds. I apreciate your time and consideration.
Thanks,
Larry Richards

Commission-Public-Records

From: trent thibodeaux <trentthib@gmail.com>
Sent: Monday, December 9, 2019 2:31 PM
To: Commission-Public-Records
Subject: [EXTERNAL] facial recognition statement

I cannot be at the meeting on December 10th at noon but would like to make my statement as a concerned traveler.

To The port of Seattle Commission:

In regards to the facial recognition proposal for SEA-TAC International Airport, The Port of Seattle Commission is doing a disservice to all people who use SEA-TAC, if this facial recognition plan is pushed forward into more consideration.

These sorts of action seem relatively innocuous as a singular "precaution," but in the larger scope of "policing" it is very scary to our individual right to privacies. If airlines "aren't directly subject to any restrictions on {their} use of personal data," then they (airlines) can use that data to discriminate, racial profile, religious profile, etc etc without any consequences. This is unethical, an if not already, unlawful. As someone who travels often, this proposal makes me feel less safe to travel and offensively attacks my privacy, personal security, and civil liberties.

The only compromise to this would be an opt-out option, but mandating all travelers, domestic and international, to use facial recognition to travel is a detriment to travelers rights/freedoms. I believe it to be the airports responsibility to defend and protect those people who are using them. That is their social and ethical responsibility as a privately owned company.

As a world traveler, I ask you, Port Commission to stand up for my(our) rights to freely travel without having my(our) privacy and rights infringed upon by the use of facial recognition.

Thank you,

trent thibodeaux

Commission-Public-Records

From: Christopher Mitten <ctmitten@hotmail.com>
Sent: Monday, December 9, 2019 2:24 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial Recognition

I am 100% opposed to this facial Recognition garbage. We all know what your actual goals are and I am not for it.
This is unnecessary and will not help anyone. It will only hurt us all as you psychopaths tighten your grip on our society.
Don't you know that the pitchforks are coming? Eventually you will drive society into a corner and we will all fight back.
And by that time, there will be no words to save you.
I will be voting against anyone and everyone in favor of this.
Do some real work!

Commission-Public-Records

From: Joy Easley <jjoyeasley@gmail.com>
Sent: Monday, December 9, 2019 2:24 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial recognition

To whom it may concern:

Facial recognition is a massive violation of privacy and our rights. Washington State is one of the few states actively fighting back against the hate, fear, xenophobia, and oppression that are inexorably taking over our country. Please don't help further fascism by introducing facial recognition at Sea-Tac airport. Once one major airport gives in to it, it will sweep the country. Choose to protect the rights of citizens and reject facial recognition technology.

Thank you,

Joy Easley

Sent from my iPhone

Commission-Public-Records

From: Mariel Black <meoinii@gmail.com>
Sent: Monday, December 9, 2019 2:20 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial Recognition at Sea Tac

To the attention of the Port Commission,

The proposed facial recognition setup at SeaTac is an incredible invasion of privacy in the making. Aside from the obvious limitations of technology and the unnecessary cost involved, there is a huge security issue involving personal data and personal safety here.

In order to recognize someone's face, the system first has to have records on every single person who will pass through, obtained presumably from government records, without the consent of the person involved. It also has to store that person's personal information in some manner of database, again, without the consent of the individual, keeping a large stock of personal data that could be hugely damaging in one location. The owner of that data has no say in when, how, or where their data was collected, no say in how it is stored, and no recourse in the event that that storage is compromised. An individual who is being stalked or has an abusive partner or parent is put at much higher risk when they can be tracked from anywhere, especially when data breaches are common and security is frequently not up to the task of keeping out determined computer-savvy people. Our data is already being harvested from a multitude of sources and sold to the highest bidder. I absolutely do not feel comfortable adding a tempting target to that list.

This also fails to take into account individuals who may have limited or inaccurate government records and will not be able to use the system properly even ignoring its other problems. Those who wear religious head coverings, glasses, or have substantially changed their hairstyle or other appearance factors may not match their government ID photos closely enough for the system to recognize them. Glasses can't be worn in Driver's License photos or passport photos, nor can burqas or other veils that cover the face. Any people who don't match well enough for the algorithm to identify them will then be singled out and held up. This not only makes for a difficult and stressful travel experience for these people, but slows down the process for everyone. All of this, again, for no real benefit.

There is no reason to include invasive and potentially dangerous facial-recognition to SeaTac's security set-up. It invites additional cost and risk for no discernible benefit,and violates the privacy of every passenger who passes through.

I ask that you consider the potential consequences of this plan and make the choice to turn it down.

-Mariel Black

From: Samantha Webster <samantha.m.webster@gmail.com>
Sent: Monday, December 9, 2019 12:55 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial recognition technology Seatac

Categories: Public Comment

Hello, I have been a Seattle resident for over a decade and feel strongly opposed to the use of facial recognition tech at SeaTac.
I understand that the use of new technologies can help with security and fraud, but it is impinging on our civil liberties to have our faces catalog in a digital database without our explicit consent. This is but one step in a dangerous domino effect of politicians invading our privacy.
Please consider how dramatically unpopular this technology is going to be with your constituents.

Regards
Samantha Webster
Sent from my iPhone

From: Katherine Cleland <tkcleland@yahoo.com>
Sent: Monday, December 9, 2019 12:41 PM
To: Commission-Public-Records
Subject: [EXTERNAL] No Facial Recognition systems at SEATAC

Categories: Public Comment

I do not want to live in a dystopian system where every move is tracked by facial recognition. This technology is not appropriate for airport deployment until the legal and ethical concerns and limitations have been hammered out.

We've been thru this with the traffic cameras in Seattle, and its quite clear, the citizens of Seattle expect our government to respect our privacy.

https://www.kiro7.com/news/local/city-council-taking-closer-look-at-how-surveillance-cameras-will-be-used-in-seattle/989425808/

The program you've proposed looks to be much more intrusive. Please do NOT deploy the facial recognition program at SEATAC.

Katherine Cleland
tkcleland@yahoo.com

From: Miles Dowe <milesdowe@gmail.com>
Sent: Monday, December 9, 2019 12:34 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Regarding tomorrows discussion: facial recognition at Sea-Tac

Categories: Public Comment

To the esteemed commissioners of the Port of Seattle,

I am a resident of Lake City and I received an email about a hearing to be held tomorrow. The topic regards a proposal to use facial recognition on travelers at Sea-Tac Airport.

I am unable to attend the meeting tomorrow. However, I wanted to publicly state my opposition to the use of facial recognition. I believe it goes against the right to privacy of U.S. citizens. Facial recognition software is also far from perfect and has varying reliability across many implementations, at times resulting in high rates of false positives. According to one article from the publication *Ars Technica*:

"The Massachusetts branch of the American Civil Liberties Union [...] released the results of a test it ran on Amazon's Rekognition software, in which it mistakenly matched many New England professional athletes to mugshots from a database. The ACLU compared images of 188 athletes from the Boston Bruins, Boston Celtics, Boston Red Sox, and New England Patriots teams against a database of about 20,000 public arrest photos. The ACLU found that 27 of the athletes, more than 14%, were falsely identified in the mugshots." (Cox, 10/22/2019)

I don't feel comfortable with such a technology playing a part in the daily lives of our citizenry and individuals from around the world. I feel it is invasive and will be harmful to innocent people.

Thank you for your time in considering my comment.

Regards,

Miles Dowe

From: Andrew Kendall <kaboy4@msn.com>
Sent: Monday, December 9, 2019 12:08 PM
To: Commission-Public-Records
Subject: [EXTERNAL] In favor

Categories: Public Comment

I am in favor of facial recognition at the airport.

Andrew

From: Deyanira Taupier <flickthisspit@hotmail.com>
Sent: Monday, December 9, 2019 11:58 AM
To: Commission-Public-Records
Subject: [EXTERNAL] Completely Irresponsible

Categories: Public Comment

DO NOT USE FACIAL RECOGNITION SOFTWARE.

If you're at all informed, it would be easy to see the dangers involved. Please be diligent.

Completely unsafe practices.

Money wasting.
Imagine using resources for something actually useful, please.

If you think it doesn't affect you adversely now, you'll likely change your mind when everything goes wrong and you all get blamed.
It's honestly embarrassing this is even being considered. Wow.

From: Michelle Townsend <mtown28@hotmail.com>
Sent: Monday, December 9, 2019 11:56 AM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial Recognition at SEA TAC

Categories: Public Comment

Please do not do this!! There is no reason for the most liberal part of america to start it. Just wait. The FAA and airlines have already made travel horrible. Don't do this too.

Michelle Townsend
Seattle, WA

From: Aaron Simpson <udadni@gmail.com>
Sent: Monday, December 9, 2019 11:54 AM
To: Commission-Public-Records
Subject: [EXTERNAL] Stop Facial Recognition

Categories: Public Comment

Hello,
I am writing to oppose the use of facial recognition technology for any purpose at the SeaTac airport and any associated facilities. As an airline pilot based at SeaTac, I understand the need for proactive security measures to protect the traveling public and the workers there. I have full confidence that our colleagues at the TSA and POS Police are able to provide adequate protection without increasing the use of invasive technologies that violate the fundamental right to privacy which is one of the greatest features of our nation.

Please respect the rights of the guests and workers who use your facility.

Regards,
Aaron Simpson
Airline Transport Pilot

From: Susan Brooks-Young <sjbrooksyoung@gmail.com>
Sent: Monday, December 9, 2019 12:30 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial recognition technology at SEATAC

Categories: Public Comment

Good afternoon,

I am a resident of Bremerton and frequently fly out of SEATAC for business. I am writing today to let you know that I am adamantly opposed to use of facial recognition technology at SEATAC. This is a huge privacy concern for me.

Facial recognition technology is still in its nascent stages of development. Bias against people of color and women is currently baked into the software. In addition, certain governmental agencies have already demonstrated their willingness to trample individuals' civil rights. Employees of Google, Microsoft, and Amazon have demanded that facial recognition tools not be used for government surveillance of individuals.

This is a terrible idea. One you need to abandon immediately

Susan Young.

From: Ryan Smith <ryansmithee@gmail.com>
Sent: Monday, December 9, 2019 1:28 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Please say no to using facial recognition software at SeaTac

Categories: Public Comment

Hello,

As a local resident, I'd like to urge you against the use of facial recognition software.

As someone that was subject to using it after an international flight at another airport, I felt like my rights to privacy were being violated with no perceivable upside. Opting out would have meant missing a connecting flight so I felt coerced into using it.

Privacy is very important to me and little erosions like these become very detrimental in aggregate.

Ryan

From: Kim Berman <kim.berman@yahoo.com>
Sent: Saturday, December 7, 2019 2:27 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial recognition technology at SeaTac

Categories: Public Comment

Do not allow facial recognition technology at SeaTac. It's an invasion of privacy and not ok. Even if it did work (which it doesn't) it would not be okay.

Do not allow this to happen.

Thanks

- Kim Berman

Adam Shostack
1122 E Pike St #1299
Seattle WA 98122
917-391-2168

Comments of Adam Shostack to the Port of Seattle Commission, for its meeting of December 10, 2019, regarding policies (19-13) for automated facial recognition at Sea-Tac Airport.

Members of the Port of Seattle Commission:

Thank you for the opportunity to comment on your proposed resolution on use of automated facial recognition at the Port of Seattle. I am a recognized expert in cybersecurity. My qualifications include being the author of *Threat Modeling: Designing for Security* (Wiley, 2014), an advisor to the UK's Research Institute in the Science of Cybersecurity (RISCS), and member of the Review Board for Blackhat, the largest technical cybersecurity conference. I spent most of a decade on Microsoft's Trustworthy Computing team. I am also a board member of the Seattle Privacy Coalition, but I am, in this letter, representing only myself. Sadly, prior commitments prevent me from appearing in person at the December 10 hearing.

I have read the prepared testimony of The Identity Project and concur in its advice. Rather than re-state their excellent points, I would like to address a question which I believe may be on the minds of the Commission and its staff:

What's the harm in a photograph?

This question ties closely to the work I now do daily, as a consultant helping organizations to threat model: to understand the risks associated with technologies they are building or deploying.

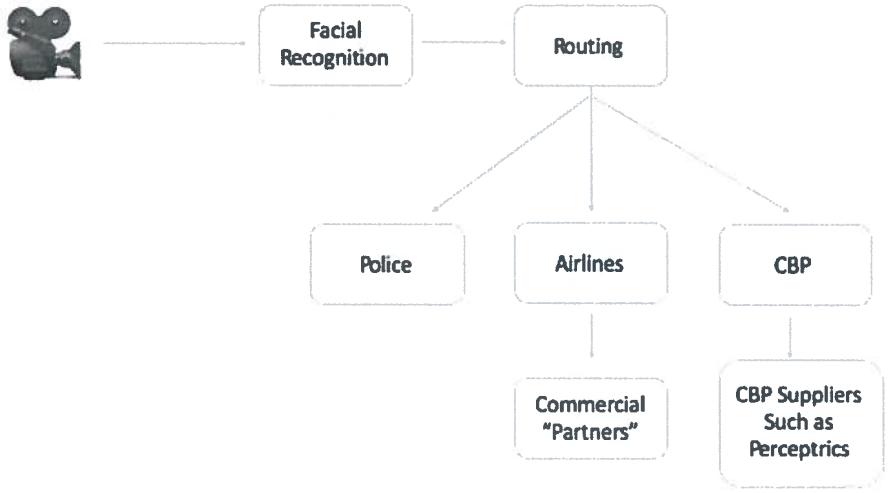
To answer the question of "what is the harm in a photograph," we should consider:

1. What are the systems being deployed?
2. What are the risks inherent in facial recognition?
3. What are the risks of facial recognition in this system?
4. Has CBP shown itself to wield its powers wisely?

1. What System Is Being Deployed?

First, we must understand that this is not simply "a photograph." The camera is a literal lens into a system of surveillance and control of the citizens of and visitors to Seattle, and the United States. That technological system includes facial recognition software, and messages sent to an unknown list of providers. For a proper security and privacy threat modeling exercise, we would have data flow diagrams of the systems provided by CBP. We do not have those, and as

such, we must hypothesize. My understanding is that the capture includes at least these elements:



In this diagram, I represent the camera as a movie camera, based on my experience at Dulles International airport, where, last month, I was told I had no right to opt-out of image capture. This personal experience is at odds with the claims of CBP, an issue to which I will return. My image was captured by a Logitech webcam, I believe it was a model 920, which is what I use at home and thus know the images it captures are of high enough quality that people routinely read titles of books on a bookshelf eight feet behind me.

The photograph is processed through a system usually referred to as "facial recognition." That term makes us think that what's happening is a nearly human process, but that belief is flawed. What happens is that a photograph is matched with millions of other photographs, and an algorithm selects the one which is the best match.

Things which we do not know include:

- Where the traveler photographs go
- Where those millions of photographs come from
- What algorithm is in use to match
- What parameters have been set
- The qualifications that make a match "best" or "sufficient" to return
- Who operates each component of the system

The question of who operates each component of the system is tremendously important. The rules of data processing may be imposed by contract across each boundary, or left open to

interpretation or even avarice. As a direct result of choices made by CBP, we have little data about who these operators are.

We can distinguish between entry tracking and exit tracking, but perhaps should not. We do not have data flow diagrams showing us where data flows, or who operates those systems.

2. What are the risks of facial recognition?

The failure of CBP to respond to the many public records requests it has received means the commission is forced, by the agency's own actions, to consider facial recognition systems at their worst. Even if additional information is provided in private briefings, the very act of hiding that information from public scrutiny means it should be, at best, discounted.

What we do know is that facial recognition is tremendously inaccurate, and its accuracy gets worse as it attempts to identify non-white populations.

When the ACLU ran an experiment with Amazon's Rekognition system, it matched 28 members of Congress to people who had been arrested for crimes.
https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Additionally, we do not know the parameters that are set, how those parameters are selected, or how they are changed. The parameters, such as "confidence level" are crucial because the lower it is set, the more the system will present false matches, rather than emit an error message.

3. What are the risks of facial recognition in this system?

So it is nearly inevitable that many people will be mis-identified, subjected to additional screening, interrogation, denial of entry into the US, revocation of visa, referral to the police with inaccurate claims that there are outstanding arrest warrants. Even if these are addressed quickly, those so mis-treated will be subjected to stress, financial costs, and possibly missed flights. But we have no reason to expect that they will all be addressed quickly. Those operating the system will be subjected to pressures to "dot every 'i' and cross every 't.' Even if those pressures are explicitly disclaimed, no one will want to be the one who lets the next 9/11 terrorist into the country. The budget of CBP is stretched by a crisis at the southern border, and staffing for review is likely not a priority.

These problems exist in any system operated by humans. However, human decisions are understood to include mistakes, and human supervisors will question and correct those faster and more capably than they will correct the decisions of "the system."

This is not an isolated incident. Bureaucratic systems defend themselves. They must assert that their systems work, for any chink in that armor threatens to disrupt the smooth flow of operations. In the normal course of operations, businesses appoint omnibudment; agencies appoint inspectors general, newspapers investigate outrages. These systems are strained by the times, and we cannot rely apon them for the timely resolution of the problems that we must expect to see.

In fact, "the system" has and will continue to aggressively and doggedly defend itself. The commission should not forget the case of Rahinah Ibrahim. After an FBI agent ticked the wrong box on a form, the FBI spent 14 years and millions of dollars to first deny its mistake, then to deny any remedy to Dr. Ibrahim. For the 9th circuit, Judge Wardlaw wrote "The government played discovery games, made false representations to the court, misused the court's time, and interfered with the public's right of access to trial. Thus, the government attorneys' actual conduct during this litigation was ethically questionable and not substantially justified." (https://www.politico.com/blogs/under-the-radar/2019/01/02/no-fly-list-terrorists-government-1078246) We have every reason to expect that such conduct continues, and the government's behavior chills attempts to use the courts to address its misbehavior.

4. Has CBP shown itself to wield its powers wisely?

This year, CBP has ripped children from the arms of their parents, caged them, and left at least one to die of a flu, rather than get them medical attention. We have many reasons to be skeptical of the agency.

Further, in this case the agency has, at the least, failed to train its front-line staff to respect opt-out requests. It has failed to publish the rules for opting out, or parameters (such as "an opt out will take no longer than our main system.") Even more, the powers that the agency seeks to grant itself will be exercised out of sight, behind a wall of public records exceptions and commercial non-disclosure agreements.

Lastly, this analysis is based on the assumption that the system operates securely, but securing computer systems is a complex task, and securing modern computer systems with their complex interactions between organizations is even harder. It is so hard that the Pentagon has recently promulgated new security standards for its contractors. (A cynic might assert that the standards ensure only the largest defense contractors can survive under the red tape.) At least one CBP contractor has failed to maintain the security of data entrusted to it. When CBP announced that breach of information, the name of the company was only released by accident, demonstrating CBP will use secrecy to inhibit analysis of what they are doing, and that these concerns are grounded. Public reporting, such as https://www.theverge.com/2019/6/10/18660382/license-plate-photos-breach-data-compromised-customs-contractor-leak indicates that "it wasn't until May 31st that the agency learned that a contractor had copied CBP files to its own network, a violation of data security

policies that enabled the breach." This statement indicates that CBP had failed to "trust but verify" by specifying and monitoring data flows from its own networks.

It is my hope that we can thus see that the harm from "just a photograph" is much greater than might otherwise be expected. Facial recognition represents a magic box, which will arbitrarily pull victims into a nightmare of red tape. The Commission should investigate the technology, its parameters, and its management

In a world, it is entirely reasonable to assume that a photograph can do a great deal of harm, and that the Commission should act to protect the public from these intrusions.

I would be happy to speak further by phone or in person when I return to Seattle.

Thank you again for the opportunity to comment on these matters.

I remain,

/s/ Adam Shostack

From: Valdez, Veronica
Sent: Tuesday, December 10, 2019 7:58 AM
To: Merritt, Mike; Schinfeld, Eric; Mills, Pete; Schirato, LeeAnne; Pritchard, Aaron; White, Paul; Smith, Lauren (Commission)
Subject: FW: [EXTERNAL] Port of Seattle meeting agenda, item 8a re using biometric technology

Follow Up Flag: Follow up
Flag Status: Flagged

FYI~

From: Bernedine Lund <philandbernedine2002@yahoo.com>
Sent: Monday, December 9, 2019 11:20 PM
To: Bowman, Stephanie <Bowman.S@portseattle.org>; Calkins, Ryan <Calkins.R@portseattle.org>; Felleman, Fred <Felleman.F@portseattle.org>; Gregoire, Courtney <Gregoire.C@portseattle.org>; Steinbrueck, Peter <Steinbrueck.P@portseattle.org>
Subject: [EXTERNAL] Port of Seattle meeting agenda, item 8a re using biometric technology

Hello, Commissioners,

I'm not able to come to tomorrow's meeting so am sending you a short comment on the use of biometric technology.

Using biometric technology, more commonly known as facial recognition, creates more problems than it solves. It may seem like it adds security, but it creates a loss of privacy for people. One article stated that facial recognition can be at best 50% accurate when it is scanning unknown people, though it does keep improving. It does work well for security for closed groups, like employees, where all the faces are known but not as well on the general population.

Here are some quotes from a Forbes magazine dated Aug. 8, 2019, describing some problems with facial recognition: (https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#459497011 4d1).

"The biggest drawback for facial recognition technology in most people's opinions is the threat to an individual's privacy. In fact, several cities have considered or will ban real-time facial recognition surveillance use by law enforcement, including San Francisco, Cambridge, Massachusetts, and more. These municipalities determined the risks of using the technology outweighed the benefits....

The technology isn't as effective at identifying people of color and women as it is white males....

Another potential downside is the storage of sensitive personal data and the challenges that come with it. Just last week, we have had the news that a database containing facial scans used by banks, police forces, and defense firms where breached."

I found the information and references below unsettling and wonder why the Port of Seattle is being one of the first to develop policies for using in on the general public. the quotes below are from Alex Marthews, Restore The Fourth via ActionNetwork.org as pointed out by The Identity Project, which brought this to his attention.

"Travelers have a "public right of transit" by air; there's no federal law that requires airlines to require their passengers to identify themselves; and the state of Washington successfully sued the Federal government to prevent restrictions on travel to the US from Muslim-majority countries, on the grounds of freedom of movement and association of Washington residents....

DHS plans to expand its collection of mug shots of travelers to include passengers on domestic as well as international flights, and still hopes to make submission to facial imaging mandatory for US citizens. Airlines also have a dismal track record of deliberate disregard for the norms of data security in their storage and sharing of personal data about travelers, and DHS has given them a financial incentive to collaborate in DHS surveillance of travelers, by giving airlines free use of its automated facial recognition Traveler Verification Service (TVS) on a software-as-a-service basis for airline business process automation purposes, in exchange for airlines installing and operating cameras at departure gates and sending the digital photos of travelers to the DHS...."

Besides the references above, I found articles showing a bipartisan letter to DHS head from senators angry about the issue, another article about possible lawsuit, and strong opposition from the ACLU. There is more information available but this message already got longer than I had planned. The Port has many issues with the issue of growth and pollution and emissions that you don't need to be the "beta tester: for this technology.

Please put this motion on hold. I urge you not so step any further into this quagmire until more issues have been resolved.

Bernedine Lund

From: Oliver Hansen <oliver.hansen@gmail.com>
Sent: Tuesday, December 10, 2019 7:38 AM
To: Commission-Public-Records
Subject: [EXTERNAL] Comment on facial recognition technology at SeaTac

Follow Up Flag: Follow up
Flag Status: Flagged

Hello,

Unfortunately I am unable to attend in person so please accept this comment via written correspondence.

Increasing privacy-invasive technology such as facial recognition in public places like the SeaTac airport will only increase the profits of the tech companies making these products and not safety.

Additionally, surveillance has been abused to track non-criminal dissent and legal protest (https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/) specifically against black and other non-white groups. This is not a new phenomenon but continued for many decades and included Dr King (https://www.eff.org/deeplinks/2014/11/fbis-suicide-letter-dr-martin-luther-king-jr-and-dangers-unchecked-surveillance). Imagine how such a technology like facial recognition would be abused to the detriment of the citizens you represent.

Once a technology like this is implemented the impacts are felt for a long time. I encourage you to consider other, less invasive forms of security for the port and keep your citizens in mind.

Respectfully,

Oliver Hansen

From: Madeline Burns <madelineburns0321@gmail.com>
Sent: Monday, December 9, 2019 8:59 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Save Public Privacy! NO Facial Recognition at Sea-Tac Airport

Follow Up Flag: Follow up
Flag Status: Flagged

To the commission of public records :

I, Madeline Burns, a lifelong Tacoma Washington resident, US citizen, and customer of the Sea-Tac International Airport, state my disapproval regarding the consideration of facial recognition technology at the Sea-Tac International Airport.

The implementation and use of facial recognition technology would eliminate public privacy to patrons, employees, vendors, customers, etc. of the Sea-Tac Airport and would prove extremely expensive- as with all new technology infrastructure- which is not at all necessary.

Most certainly ANY funds to be used for facial recognition could be better saved or spent for improvements to airport infrastructure regarding building code & safety, environmental protection efforts, reduction of pollution and noise pollution, reduction of taxes to those impacted by the neighboring Sea-Tac airport, or even sending these funds to support Homeland Security - if you are truly concerned about who is in the airport.

Have the members of this commission not given their focus any attention to the recent events in Hong Kong with the massive public protest? Where facial recognition is a part of their daily lives, have they paid any attention in particular to those who were arrested and persecuted for covering their faces with masks while seeking refuge at the college campus? Or in China were hundreds of thousands of citizens were prevented from taking public transportation after the implementation and use of facial recognition led to a social scoring system?

That is some scary, real life that some people have to live every day.

The United States of America has already embarked down a dark path but to move towards the evasion of public privacy in a place of business is a step we should be conscious of so as not to make that decision lightly.

I completely disagree and I would also vote and pay for a big, fat NO no this idea.

I wish I could attend this hearing so I can hear the arguments/points of proposal from the commission but I have to be present at my place of employment instead.

- Madeline E. Burns
Tacoma, Wa, USA
Sent from my iPhone

From: Kendra J Hoffman <kendrahoffman@icloud.com>
Sent: Monday, December 9, 2019 8:27 PM
To: Commission-Public-Records
Subject: [EXTERNAL] I oppose the use of facial recognition at SEA-TAC

Follow Up Flag: Follow up
Flag Status: Flagged

Hello,

I'm a resident of Sammamish and do a lot of business and family travel. I use TSA precheck and don't have anything to hide. But I strongly oppose the use of facial recognition at SEA-TAC.

Facial recognition technology has been proven time and again to be just as biased as humans, just as racist. Sometimes worse. Coming from a machine does not magically make it objective.

On top of that, it is horrifying to think that Seattle, one of the last bastions of civil rights and caring for minorities and the underserved in this country, would actually help start a sweep of this horrific, 1980-style Big Brother surveillance through our nation's airline system.

Travelers do not have the option to go somewhere else. Most cities only have one major airport. The potential positive uses are far outweighed by the damage to privacy, the addition to harassment of minorities, and the abuses that technology like this would be subject to.

In the strongest terms, I urge you not to implement technology that is this biased, this flawed, and this invasive at the airport.

Sincerely,

Kendra Hoffman
952-215-4790

From: Joe Mabel <jmabel@joemabel.com>
Sent: Monday, December 9, 2019 4:55 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Facial recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Public Comment

Given the enormous tendency for facial-recognition software to show false positives, especially for non-white people, I strongly urge the Port Commission **not** to introduce facial-recognition technology at SeaTac Airport, or anywhere else. It is unlikely to make anyone safer, and it is a lawsuit waiting to happen.

JM

From: Hank <suntourhank@aol.com>
Sent: Monday, December 9, 2019 8:13 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Proposed deployment of facial recognition technology at SEA-TAC

Follow Up Flag: Follow up
Flag Status: Flagged

Remember that **Benjamin Franklin** once said: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

This technology is not proven to be even close to reliable and effective and it's another insidious invasion of privacy.

We pride ourselves on our liberty and the fact that this is the Land of the Free.

The progressive City of Seattle has a chance to say NO to Big Brother.

From: Conor Curtis <conor.curtis@gmail.com>
Sent: Monday, December 9, 2019 4:47 PM
To: Commission-Public-Records
Subject: [EXTERNAL] Fwd: Facial Recognition

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Public Comment

Commissioners and staff,
I am aware that SeaTac is considering implementing facial recognition technology in the airport. I would ask that you abandon this proposal. We live in a world that is increasingly saturated with surveillance technology, and lacking of privacy. While I understand that passenger safety is a concern, I do not believe that facial recognition will assist with this fight in a way that overrides the privacy concerns of citizens.

We should have an inherent mistrust of those in the position of power to use surveillance. Past abuses require this mistrust. When you consider that this is almost undoubtedly intended to 'creep' from border control, to domestic flights, and into an interagency database, these fears appear valid. Making facials recognition mandatory is a gross violation of human rights (see Xinjiang, China) and I am loathe to see it expanded here. I do not believe that this erosion of privacy rights is satisfactorily offset by any safety concerns. I value my privacy and currently feel more than safe enough while flying.

I read just yesterday that an American journalist at the border was not allowed to opt out of facial recognition, despite signs stating that she held that right. How does the port intend to address Americans being denied their rights?

Furthermore, I object to providing my information to private parties (i.e. airlines) without my consent. Aside from being subject to advertising, 'personal pricing,' and other business practices from airlines, I am concerned about their ability to protect my information securely. Providing this information to airlines also exposes that information to foreign governments who may compel the airlines to comply, whether or not I am traveling outside of the USA.

The Port has an obligation to protect its customers from the more likely threats than the unlikely and ephemeral. Without guarantees protecting Americans' right to opt out, you must opposed facial recognition and protect American rights to privacy and free assembly.

Please forgive the haphazard manner in which I feel this email is composed. I am trying to write it in the middle of my workday and just recently found out SeaTac would be participating in the initial phase of facial recognition. I would refer you to The Identity Project's written statement for further (and more cogent) reading, which have provided to the Port already.

Thank you,
Conor Curtis

From: Jann Werner <jwerbus@gmail.com>
Sent: Monday, December 9, 2019 2:46 PM
To: Commission-Public-Records
Subject: [EXTERNAL] We do not want facial recognition technology in our state

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Public Comment

To the Port Commission:

Ubiquitous facial recognition technologies create a world where there is literally NO privacy. Not only has facial recognition technology been proven to be unreliableIf and inaccurate, if this technology is deployed in our airports my right to privacy will be violated.
As a resident and tax payer in Seattle, I expect you to defend my right to travel freely and that you will not approve this technology in Washington State.

Thank You
Jann Werner

Commission-Public-Records

From: Yen Baynes <yenjourneys@gmail.com>
Sent: Tuesday, December 10, 2019 11:06 AM
To: Commission-Public-Records
Subject: [EXTERNAL] NO to facial recognition at SeaTac

Hello,

I live in Seattle and use the airport to travel many times a year. In fact, in the past year, I have come or gone from SeaTac no less than 12 times. I am outraged that the commission would even consider this invasive inaccurate facial recognition technology even as Seattle voted against anything of the sort with our police force. DO NOT allow facial recognition tech in our airport. I will remember this decision next election and plan to vote against any one of you that votes for this. I will also be sure to tell my neighbors and friends.

Thanks,

Yen Baynes

Commission-Public-Records

From: Geoff Froh <geoff.froh@densho.org>
Sent: Tuesday, December 10, 2019 10:15 AM
To: Commission-Public-Records
Subject: [EXTERNAL] Public comments regarding Sea-Tac facial recognition program
Attachments: 20191210-DenshoPublicComment-SeatacFacialRecognition.pdf

To the Commissioners of the Port of Seattle:

Please find attached Densho's comments in opposition to the proposed facial recognition pilot at Sea-Tac airport. Thank you for your consideration of our remarks.

Respectfully,

Geoff Froh

--
Geoff Froh (he,him)
Deputy Director

Densho
1416 S. Jackson St.
Seattle, WA 98144
US
(v) 206-320-0095 x105
(f) 206-320-0098
(w) www.densho.org

DENSHŌ

December 10, 2019

To Seattle Port Commissioners:

Densho (www.densho.org) is a Seattle-based nonprofit that has spent the last two decades documenting and sharing stories of Japanese American WWII incarceration in order to promote equity and justice today. One of these stories is the decade-plus of government surveillance of Japanese immigrant communities that preceded World War II — and how that surveillance, along with then-cutting edge data collection tools, were used to carry out the unconstitutional exile and imprisonment of more than 120,000 innocent Japanese Americans.

We have interviewed hundreds of WWII incarceration survivors who tell stories of witnessing fathers arrested without due process in the days and weeks following the attack on Pearl Harbor — men who were blacklisted as potential spies because of government surveillance and, in many cases, did not see their families again for months or even years.

In the decades since WWII, surveillance technology has been used to criminalize many more marginalized communities. The specter of data being shared with U.S. Customs & Border Protection and Immigration & Customs Enforcement is particularly dangerous for immigrants and refugees today, who face detention, deportation, and family separation.

For these reasons, we are deeply concerned to learn that not only is Delta Air Lines proposing to implement facial recognition for international travelers at its gates in Sea-Tac by year-end, but CBP plans to soon begin using this technology to identify all travelers entering the country.

There are too many unanswered questions about the disproportionate impact that facial surveillance will have on immigrants, refugees, people of color, queer and trans individuals, and other marginalized communities to allow this policy to move forward. We therefore urge you to halt further action on this proposed program until those most impacted by increased surveillance can air concerns and ask questions in a public hearing.

Respectfully,

Geoff Froh
Densho Deputy Director