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.

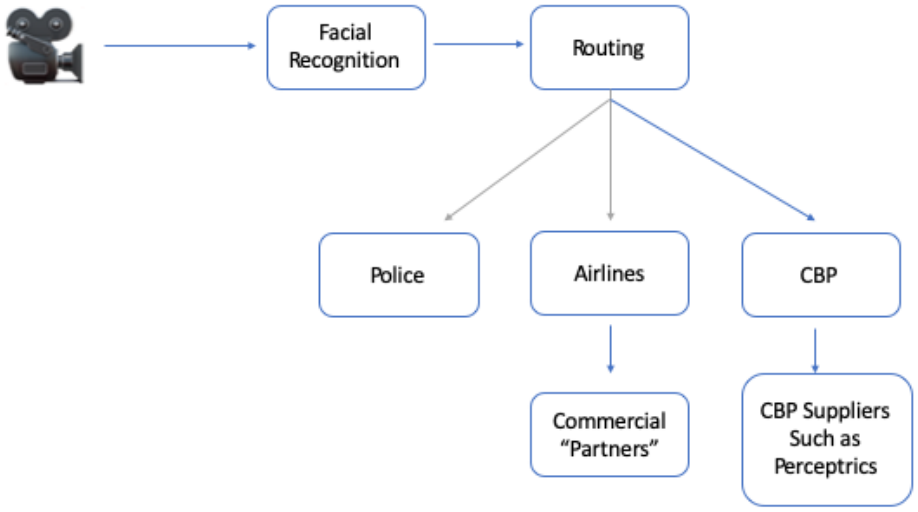
To answer the question of "what is the harm in a photograph," we should consider:

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