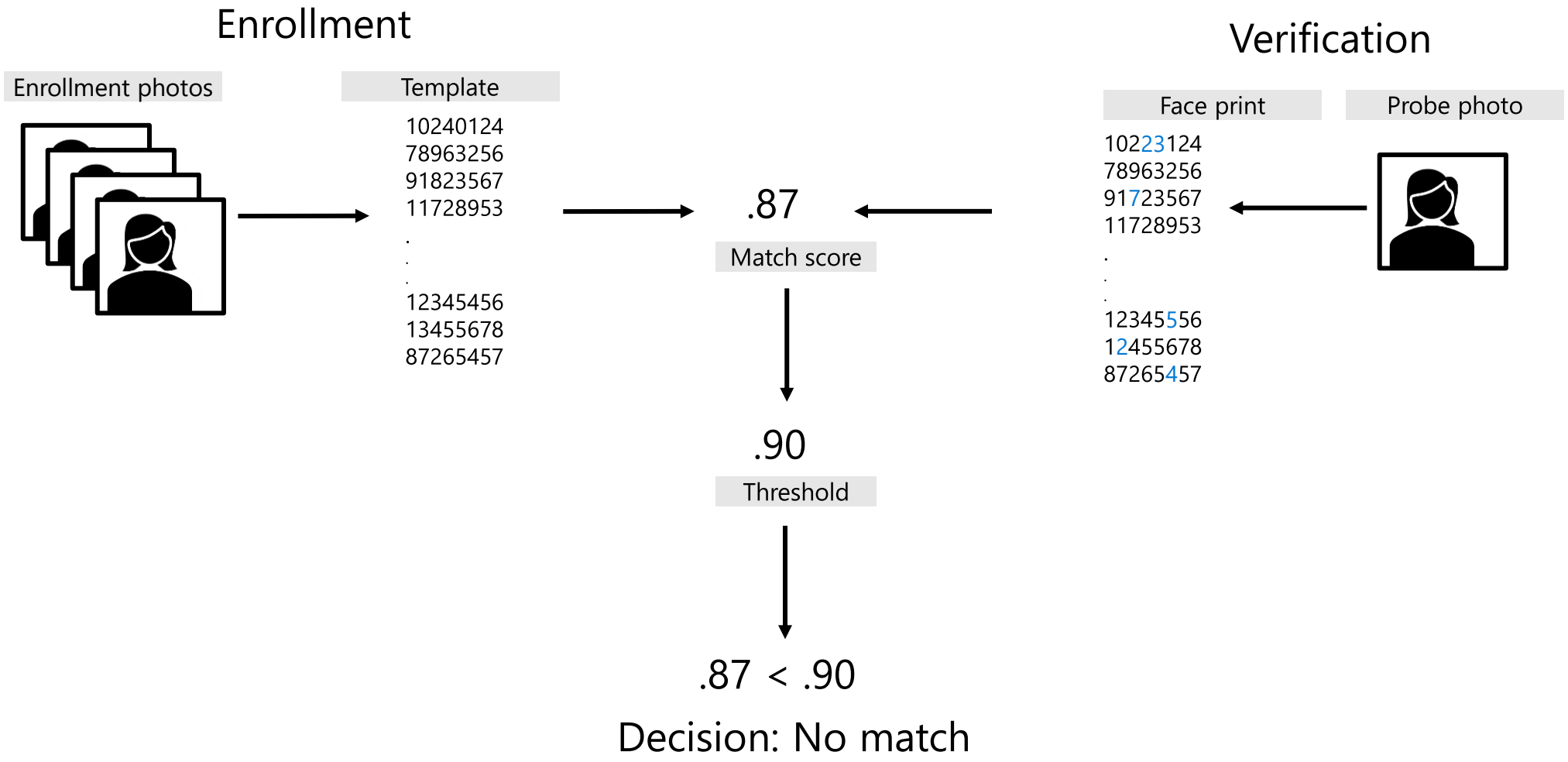
Microsoft

Facial Recognition Overview

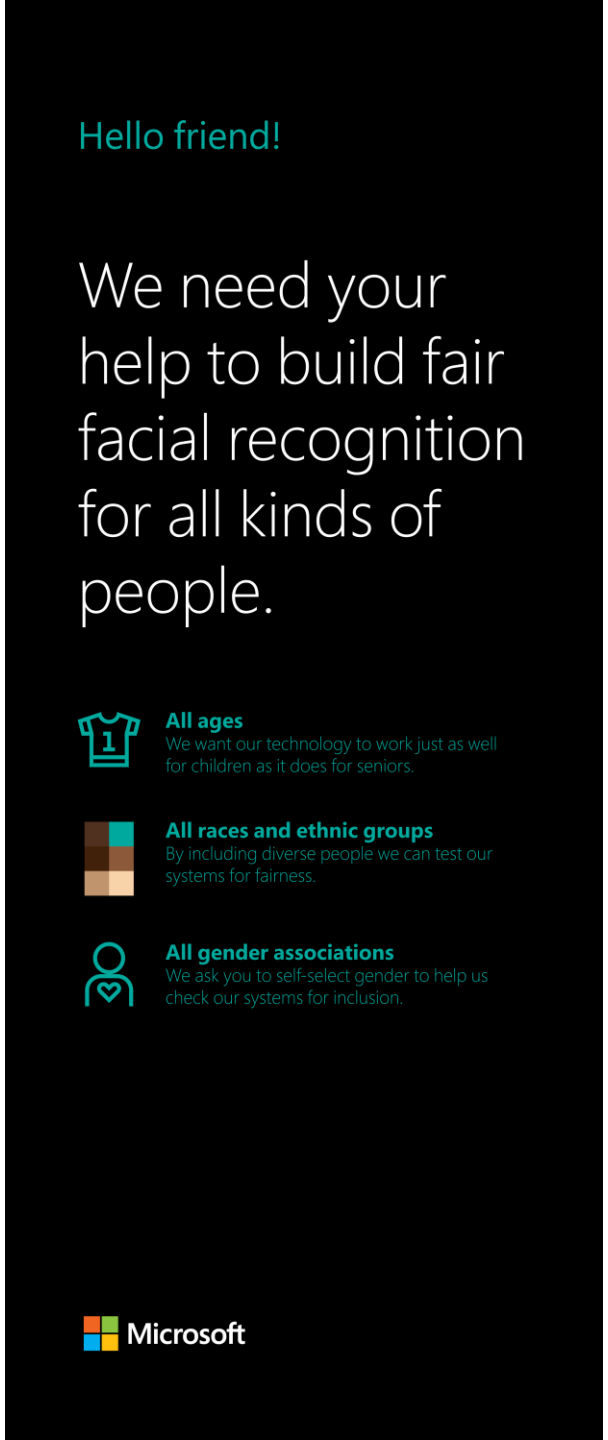
September 2019

Port of Seattle Biometrics Study Session

Facial Recognition: A type of Computer Vision



The importance of inclusive data

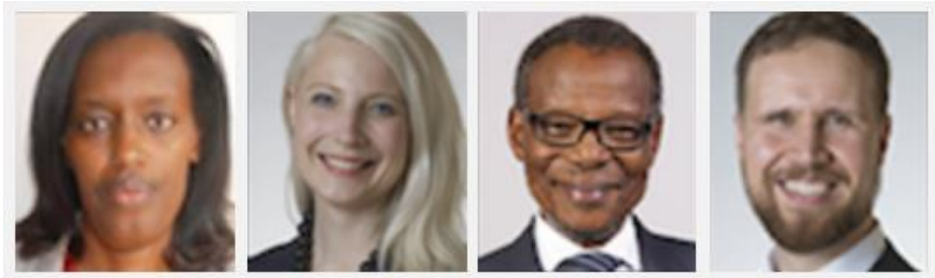


Studying gender classifiers: Gender Shades

Joy Buolamwini, MIT

Dr. Timnit Gebru, Google

Gender Shades: Microsoft Face API results



	Woman Dark Skin	Woman Light Skin	Man Dark Skin	Man Light Skin
2018 MS Face API Error Rate	20.8%	1.7%	6.0%	0.0%

Buolamwini & Gebru, 2018

2019 MS Face API Error Rate	1.5%	0.3%	0.3%	0.0%

Raji & Buolamwini, 2019

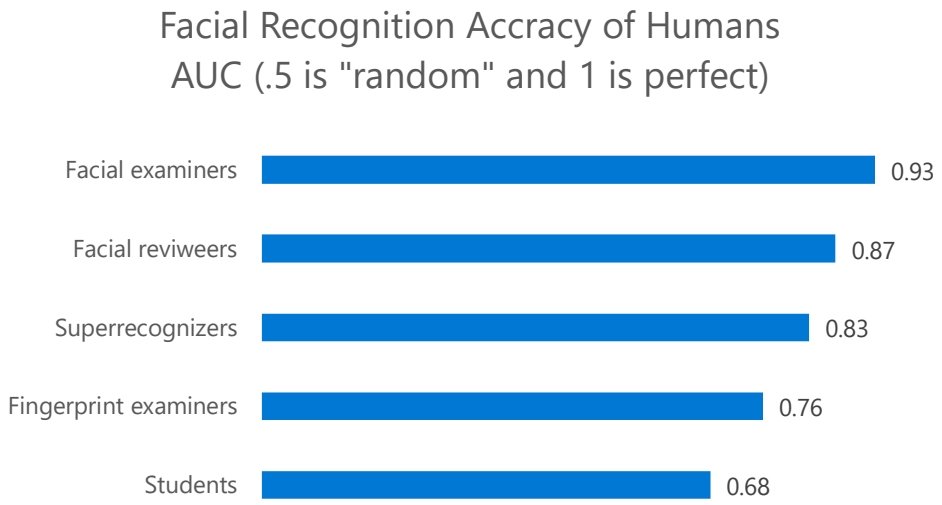
Change in evaluations for women with darker skin

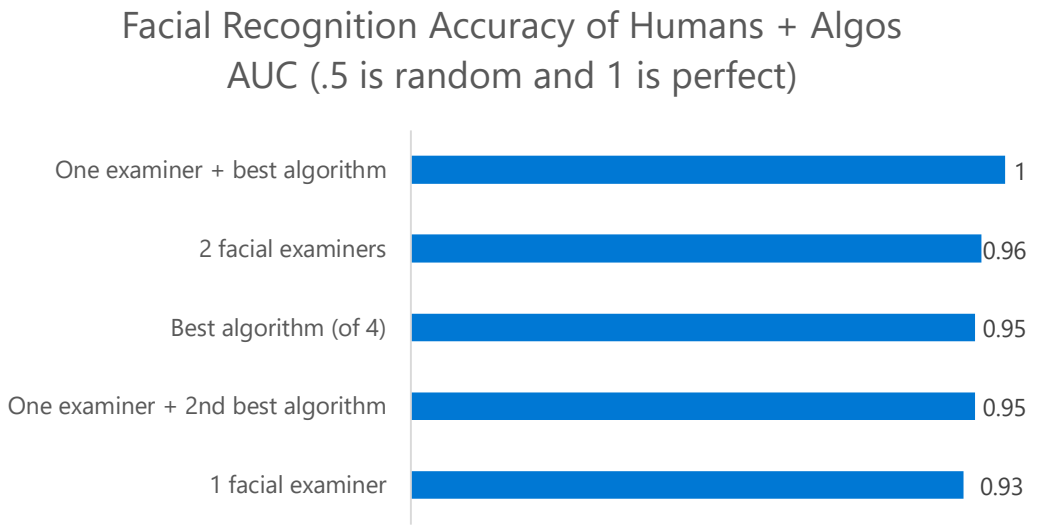
	Microsoft	IBM	Face++
Error rate: Buolamwini & Gebru, 2018	20.8%	34.7%	34.5%
Error rate: Buolamwini & Raji, 2019	1.52%	16.97%	4.1%
Change (ppts)	-19.28	-17.73	-30.4

"By highlighting the issue of classification performance disparities and amplifying public awareness, the study was able to motivate companies to prioritize the issue and yield significant improvements within 7 months." Raji & Buolamwini, 2019

Facial Recognition System

Best Solution: People plus facial recognition





Facial examiner: Extensive training, rigorous and time-consuming process, decisions can be presented to support legal action, prosecution, and expert testimony in court

Facial reviewer: Perform faster and less rigorous identification to assist in generating leads in criminal cases

Superrecognizers: High performance on facial recognition tasks
Fingerprint examiner: professional trained forensic examiners

Students: Undergraduate students

From: *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms*, Phillips et al., 2018

CBP Case Study

- Part of boarding procedure, *in addition to* staff reviewing passport photo, providing good data for evaluation (ground truth data)
- Compared live image to passport photos of passengers on the manifest for the specific flight
- 10 international flights per day across 9 airports
- 5 months of results
- Officers receive one of the following:
  - Green – match
  - Yellow- poor photo quality, retake photo
  - Red – no match, please review
- 97.3 to 99.3 “technical accuracy rate”

CBP Pilot Case Study: Example of solid evaluation

Table 3: CBP Biometric Air Exit Pilot Goals and Outcomes (As of January 2018)

Mission Tasks	Goals	Outcomes
1. Facial Photograph Availability	• Demonstrate that CBP can locate and retrieve photos for every departing passenger to use for exit processing. • Demonstrate that the photos are sufficient for automated matching.	• Approximately 99% of passengers' photos were located.[13] • Photos were considered adequate.
2. Technical Match Rate	Demonstrate that a live traveler photo, searched against a gallery of photos from existing CBP data sources, will yield sufficient accuracy.	Average technical match rate of 98% in December 2017.
3. Scalability	Confirm whether facial identification is feasible as an end-state solution for large-scale exit processing, where real-time match results are required.	Potential for TVS to support 50% of the biometric processing at 20 airports expected to enter the program by January 2021.
4. Boarding Process Impacts	Identify the impacts of facial recognition technology on the boarding process.	TVS' match response rate was reported as 1 second.
5. Match Performance Trade-offs	Identify operational and technical trade-offs between the frequency of mistakenly matching individuals to the wrong passengers in the same gallery (false positive rates) and the frequency of correctly matching individuals to their photos stored in the digital gallery (true match rates).	False positive rate of .03% and false reject rate of .5% in December 2017

Source: OIG-generated from CBP data

Image Quality Guidance from the Transparency Note

Meet image quality specifications

Image quality is critical to quality facial recognition so you should ensure that both the images used to enroll people and the probe images meet the following specifications:

- ☑ Full-frontal head and shoulder view without obstruction.
- ☑ Face size is at least 200x200 pixels with at least 100 pixels between eyes. Faces are detectable when their size is as small as 36x36 pixels, but for best performance Microsoft recommends a minimum size of 200x200 pixels when using Face API.

Control image capture environment

Lighting and camera calibration

Pay attention to how well the detail of people's faces can be seen in images taken with the camera you are intending to use in the locations where you will use it. Face API uses RGB images.

- ☑ Capture images in appropriate lighting conditions. Is the lighting too bright, too dark? Are faces backlit? Is there too much light from one side and not enough from the other? When possible, place sensors away from areas with extreme lighting.
- ☑ Is the lighting adequate to accurately capture the details of people's faces with different skin tones?

Backgrounds

- ☑ Strive for neutral, non-reflective backgrounds. Avoid backgrounds containing faces, for instance where there are pictures of people displayed, or where people other than the person to be recognized are prominent in the photo.

Sensor placement and maintenance

- ☑ Position sensors at face-level to best capture images that meet the quality specifications.
- ☑ Ensure sensors are regularly checked for dust, smudges, and other obstructions.

Plan for variations in subject appearance and behavior

Facial occlusions

Facial recognition works best when the person's entire face is visible. Faces may be partially or entirely occluded for a variety of reasons, including:

- Religion: Headwear that covers or partially obscures faces.
- Weather: Garments like scarves wrapped across the face.
- Injury: Eye patches or large bandages.
- Vision Disability: Very opaque glasses and pinhole glasses (other glasses and lenses should be fine).
- Personal style: Bangs over eyebrows, baseball caps, large facial tattoos, etc.

It is not always possible to avoid occlusions: removing glasses may be unsafe and requiring removal of religious headwear may be impermissible. In addition to sensor placement, the following actions can help to address occlusion challenges:

- ☑ A fallback method, such as a non-biometric alternative, is critical. For some people, the fallback may be the option they consistently use.
- ☑ Pay attention to challenges that people face during evaluation and deployment to identify remediations that work best for your environment.

Microsoft Facial Recognition Principles

1. **Fairness.** We will work to develop and deploy facial recognition technology in a manner that strives to treat all people fairly.
2. **Transparency.** We will document and clearly communicate the capabilities and limitations of facial recognition technology.
3. **Accountability.** We will encourage and help our customers to deploy facial recognition technology in a manner that ensures an appropriate level of human control for uses that may affect people in consequential ways.
4. **Non-discrimination.** We will prohibit in our terms of service the use of facial recognition technology to engage in unlawful discrimination.
5. **Notice and consent.** We will encourage private sector customers to provide notice and secure consent for the deployment of facial recognition technology.
6. **Lawful surveillance.** We will advocate for safeguards for people's democratic freedoms in law enforcement surveillance scenarios and will not deploy facial recognition technology in scenarios that we believe will put these freedoms at risk.