

CMSC 304 Computer Ethics

Dr. Cynthia Matuszek

1

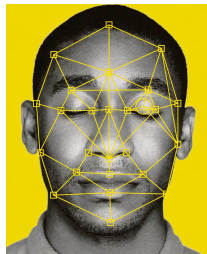
Bookkeeping

- EA4 is out
 - China's Social Credit scoring system
 - Please make sure to find additional background information
- Topics due tonight (individually or in pairs)
 - Description in paper guidelines
- Today: facial recognition
- Thursday: self-driving cars

2

Facial recognition

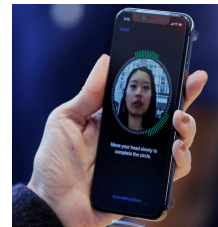
- Build a large model on a dataset of faces
- Identify the existence of a face (detection)
- Evaluate key points on that face and compare to the model
- Draw broad conclusions about that person, e.g., gender (analysis)
- Connect that face to a particular individual in a dataset (recognition)



3

Benefits: Convenience and Security

- Tagging photos
- Securing devices
- Helping the visually impaired
- Finding missing children
- ID'ing unknown civil war soldiers
- Identifying rare genetic conditions
- Simplifying access control
- Law enforcement use
- Fraud protection (e.g. ATMs)
- Loyalty cards/customer tagging



4

Disadvantages and Concerns

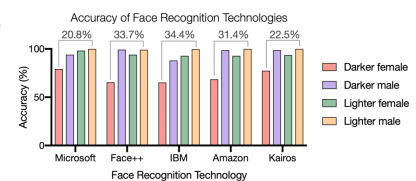
- High error rates
- Inequitable performance
- Opaque algorithms
- Inappropriate uses
 - E.g., 'personality trait' analysis
- Surveillance potential



5

Inequitable performance

- Historically, facial recognition works less well on certain groups
- Women
- Non-binary people
- BIPOC
- Especially, intersections of these groups



6

High error rates

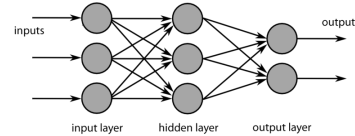
- “NIST’s most recent test, which largely relies on a database of high-quality mugshot photos, found that even the best algorithms can be wrong **more than 20 percent of the time**.”^[1]
- Generally defeated by masks
- Perform worse for older people, BIPOC, non-binary, women
- Depends heavily on quality of source images
- What’s the failure result of a false positive? A false negative?

[1] <https://www.wired.com/story/face-recognition-is-broken/>

7

Opaque algorithms

- Generally uses AI algorithms trained on large corpora of data
 - Typically neural, sometimes deep learning
- Such algorithms can produce very good results, *but...*
- Typically “black box” learning



<https://www.ibm.com/cloud/learn/neural-networks>

8

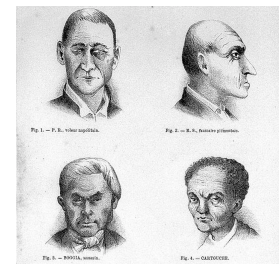
Surveillance potential

- Very large-scale matching can be performed
 - E.g., run everyone at the Super Bowl looking for criminal suspects
 - E.g., constantly run surveillance on Baltimore streets
- Governments: where are citizens and what are they doing?
- Law enforcement: who’s attending certain activities?
- Commercial: who buys what and doesn’t buy what, when?
- Other figures: landlords, schools, family, ...
- Protected activities can become part of surveillance

9

Inappropriate uses

- Sometimes faces are ‘analyzed’ for...
 - Criminal tendencies
 - Homosexuality
 - Personality traits
 - Hiring decisions
 - Test proctoring
 - **We just don’t know how to do this**



<https://www.fbi.gov/newsroom/special-operations/1976-faces-1-4>

10

Facial recognition and law enforcement

- Can be useful to identify suspects
- Can be used to locate missing persons and children
- Can be used to find suspected criminals

But...

- Is used to track protesters
- Is used to compare suspect pictures to ID cards
- Is used on inappropriate media, e.g., sketches
- Is used for large-scale surveillance

11

Facial recognition and arrests

- Faulty arrests can lead to serious consequences even when acquitted
- Causal role of facial recognition is frequently obscured
- Frequently the ‘top’ match is not the one charged
- Right now, few legal bars requiring transparency
- Combination of technical flaws and opaque use of the technology inevitably leads to seriously flawed results
- Currently publicized cases are all Black

12

A final note

- “I think people sometimes feel a sense of ease, like ‘That would never happen to me because I’m not somebody who has had a lot of interactions with the police,’” Jackson says. “But no one can guarantee that you don’t look a lot like somebody who committed a crime. Nobody is safe from poor facial recognition technology.”



www.wired.com/story/hidden-role-facial-recognition-tech-arrests
images: www.bbc.com/news/technology-20160712 you-can-surprisingly-like-to-have-a-facial-recognition

13

Facial recognition and hiring

- Screen for ‘friendliness,’ ‘customer facing,’ ‘comfort,’ ...
 - Exact details are proprietary – we don’t know what’s being screened
- Accuracy of face recognition technology
 - Race, color, gender, glasses, ...
- Accuracy of screening
 - Are we measuring what we think?
- Digital divide issues
- Perpetuation of existing biases
 - Systems are typically trained on existing employees

Problems

14

Facial recognition and hiring

- Lets you make quick decisions about applicants, *but...*
- Three tests for a hiring tool:
 1. Is it reliable (gives the same performance for the same person)?
 2. Is it valid (predicts employee performance successfully)?
 3. Does it treat all applicants fairly regardless of characteristics?
 - Including traits protected by federal law, including gender, race and age
- Facial analysis fails on all counts

www.nytimes.com/2016/07/12/us/politics/facial-recognition-arrests.html

15

Facial recognition and test proctoring

- Facial recognition and analysis-based proctoring software
- Tries to determine if:
 - You are who you say you are
 - You are consistently sitting in the field of view
 - You are not wearing a hat (or hijab!)
 - You are not fidgeting

16

ACLU’s Ethical Framework

- Collection: An entity must receive informed, written, and specific consent from an individual before enrolling them in a face recognition database.
- Use: An entity must receive informed, written consent from an individual before using a facial recognition system or faceprint in a manner not covered by existing consent.
 - An entity may not use a face recognition system to determine an individual’s race, color, religion, sex, national origin, disability or age.
- Sharing: A faceprint or any information derived from the operation of a face recognition system may not be sold or shared except with the informed, written consent of the individual whose information is being sold or shared.
- Access: An individual must have the right to access, correct, and delete his or her faceprint information.

17

Discussion

- There are few laws governing facial recognition technology, which is widely used in Maryland.
- What policies should exist for law enforcement?
 - A complete ban?
 - Requiring a warrant?
 - Disclosure of use to courts/attorneys?
 - Use only in limited situations?
- How do those policies work with the ACLU’s ethical framework?

<http://tiny.cc/facial-rec>

18