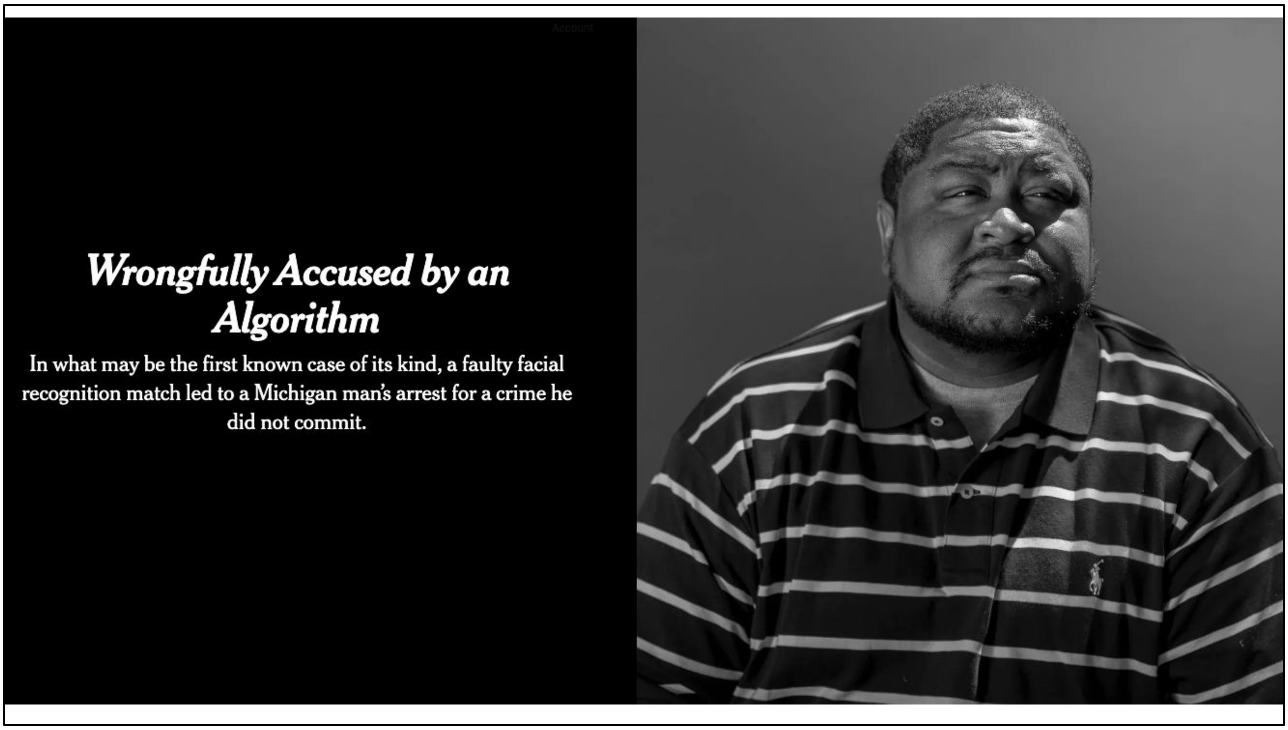
The Ethical Dilemma of Using Facial Recognition

Marisa Shuman & Marieke Thomas

CSCI 77800

Final Project Presentation



Wrongfully Accused by an Algorithm

In what may be the first known case of its kind, a faulty facial recognition match led to a Michigan man's arrest for a crime he did not commit.

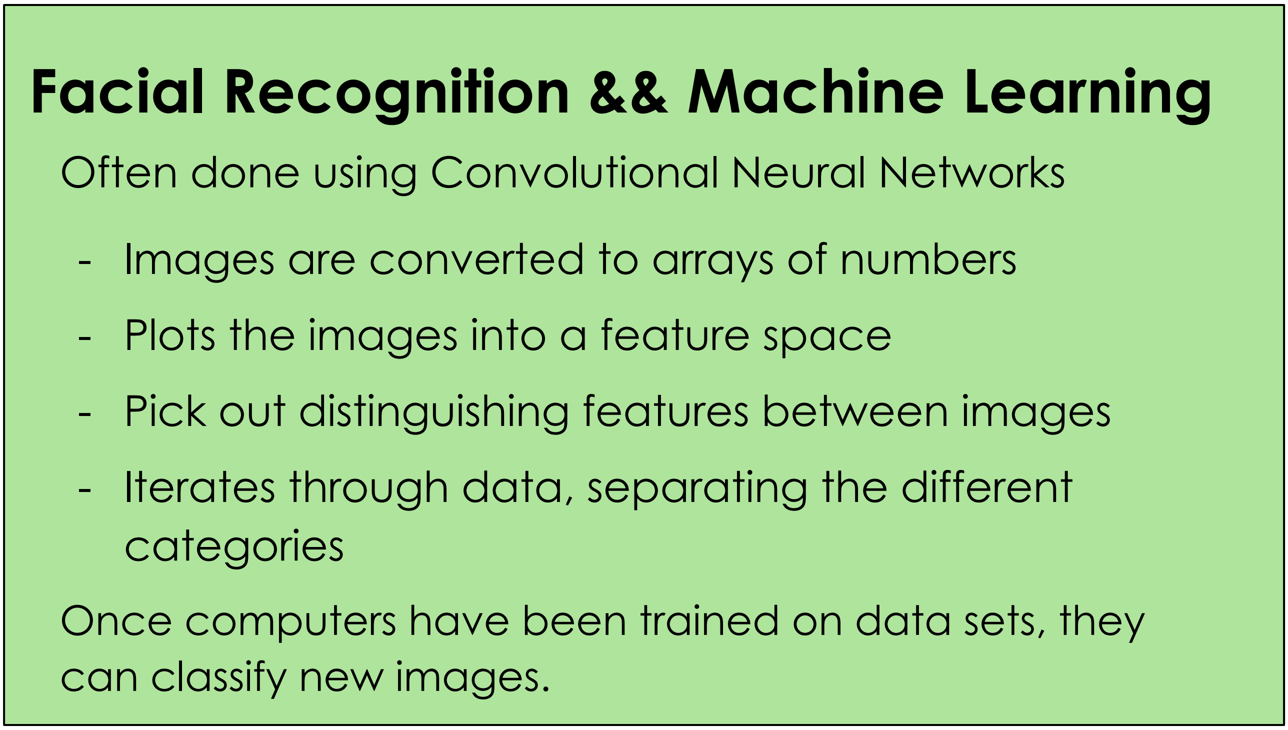
Story: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

How would you feel if you were arrested for a crime you didn't commit simply because a computer thought you looked like the perpetrator?

Robert Julian-Borchak Williams was wrongfully arrested after facial recognition software incorrectly matched him to security footage of a robbery. DataWorks Plus, the facial recognition software used, was paid by the Michigan police department. This software runs unofficial checks but there is no formal, scientific measure of its accuracy. In a federal study of facial recognition algorithms, including the DataWorks one, it was shown that African American faces were far more likely to be falsely matched than white faces.

Areas of Use

- Facebook tagging
- Biometric phone unlocking
- Airports & security
- Law enforcement
- Tracking individuals in protests
- Surveillance



Facial Recognition && Machine Learning

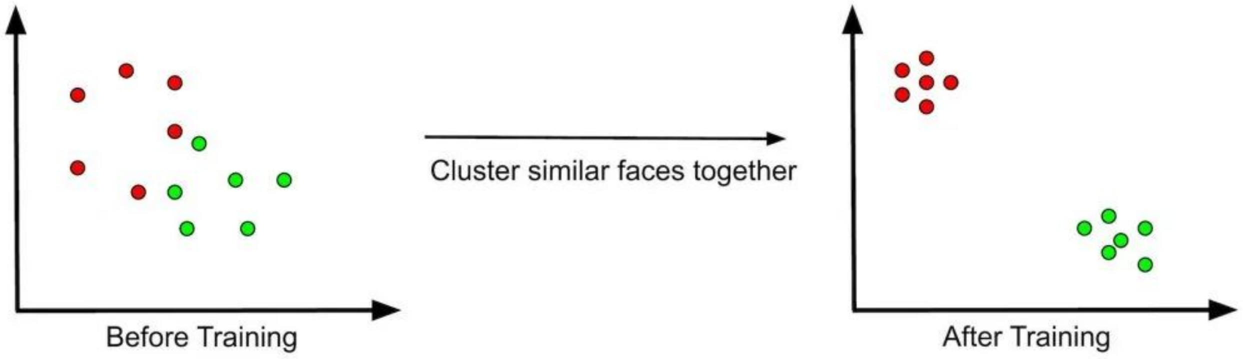
Often done using Convolutional Neural Networks

- Images are converted to arrays of numbers
- Plots the images into a feature space
- Pick out distinguishing features between images
- Iterates through data, separating the different categories

Once computers have been trained on data sets, they can classify new images.

- Training data set classified and fed into the computer
- CNNs pick out distinguishing features
- Images are split into arrays of numbers
- Each image is embedded into a feature space (plotting as a point on a graph)
- Computer iterates through the data, and eventually groups some images closer together (this is done by changing the weights on different criteria until like images are clustered and different images are separated)
- Note that for the specific API that we used, the neural network is already mostly trained to distinguish features between photographs more generally. We are essentially adding in the last layer of the neural network, which specifically classifies the images based on the categories chosen (in our case, male and female)

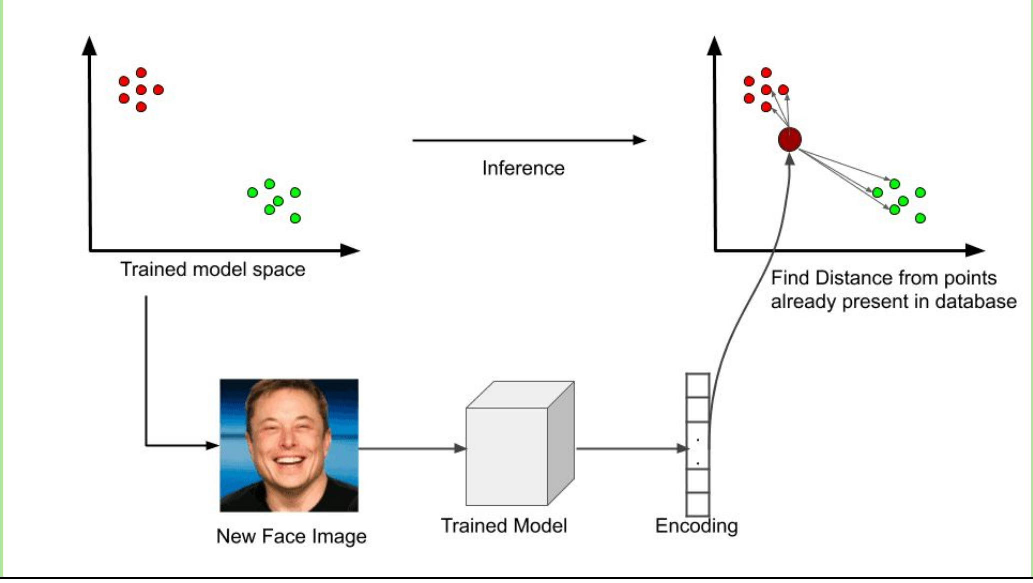
Training the Model



- Computer iterates through the data, and eventually groups some images closer together (this is done by changing the weights on different criteria until like images are clustered and different images are separated)

Image from: https://learnopencv.com/face-recognition-an-introduction-for-beginners/

Using the Trained Model

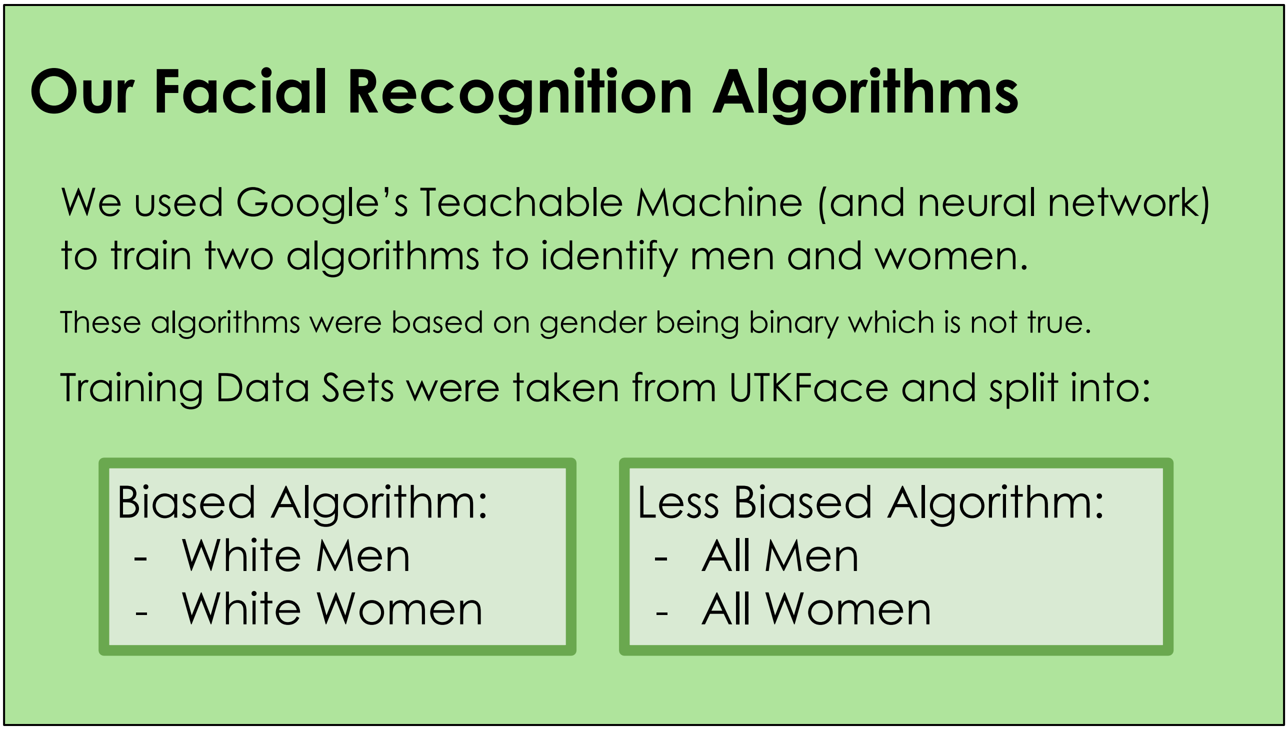


Once computers have been trained on data sets, they can classify new images.

Image from: https://learnopencv.com/face-recognition-an-introduction-for-beginners/

Flaws in Facial Recognition

- Necessity of large data sets
- Data sets are often disproportionately full of White or Asian male faces
- Leads to greater accuracy when classifying White/Asians and lowest accuracy when classifying Black people



Our Facial Recognition Algorithms

We used Google's Teachable Machine (and neural network) to train two algorithms to identify men and women.

These algorithms were based on gender being binary which is not true.

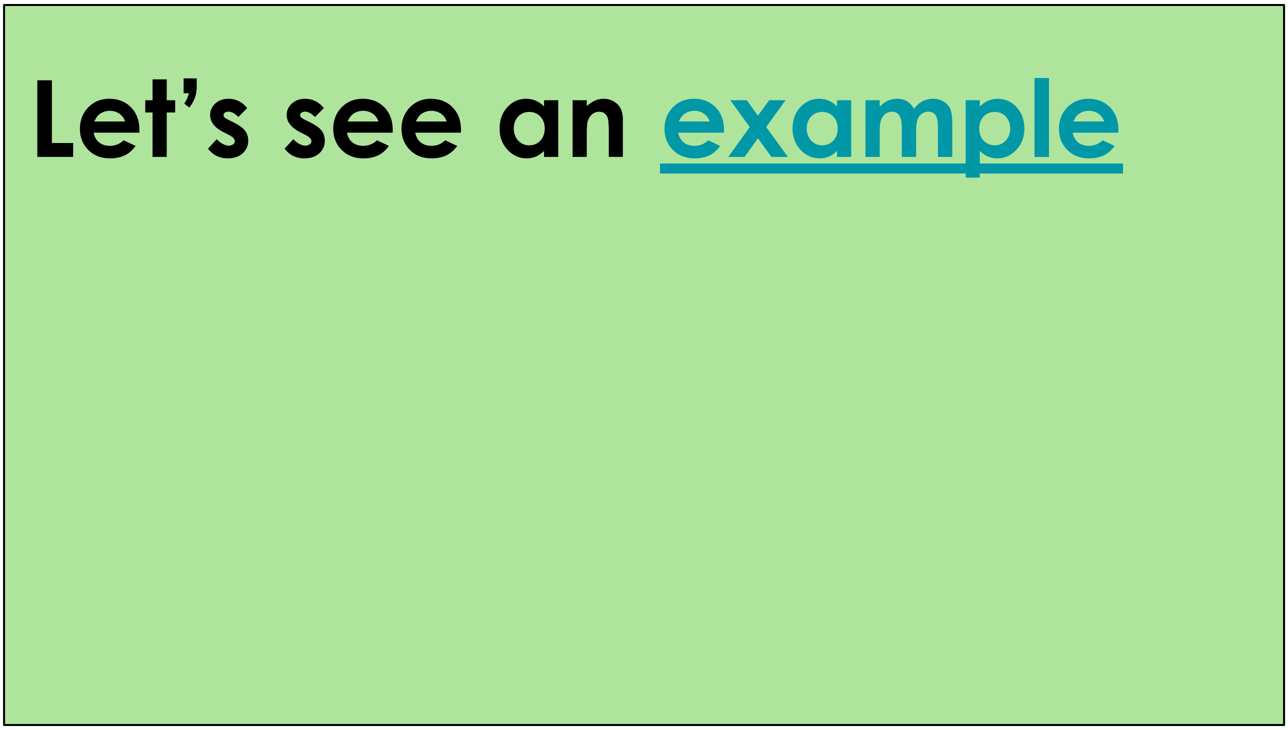
Training Data Sets were taken from UTKFace and split into:

Biased Algorithm:
- White Men
- White Women

Less Biased Algorithm:
- All Men
- All Women

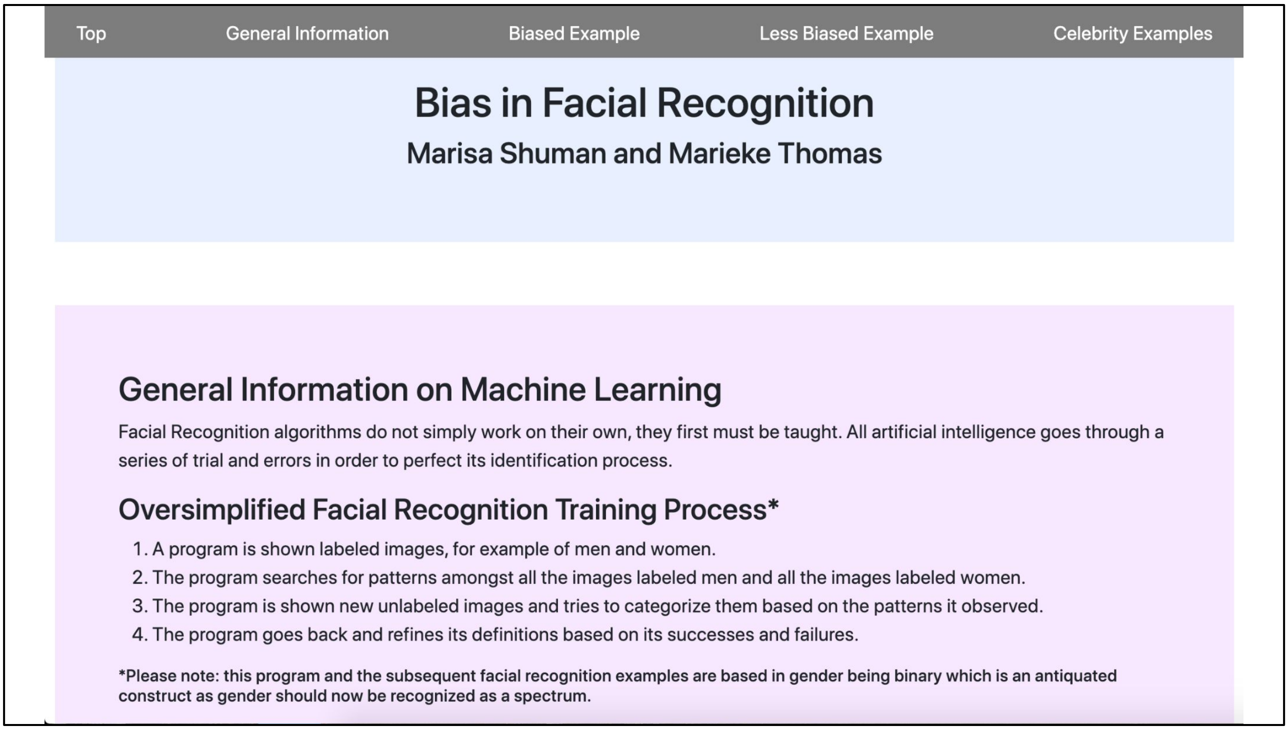
We did two algorithms to demonstrate the bias that already exists in most facial recognition algorithms.

Data sets that are trained mostly on white male faces are more likely to have difficulty identifying people of color and women.



Let’s see an example

https://replit.com/@mshuman8/FacialRecWebsite#style.css



Bias in Facial Recognition

Marisa Shuman and Marieke Thomas

General Information on Machine Learning

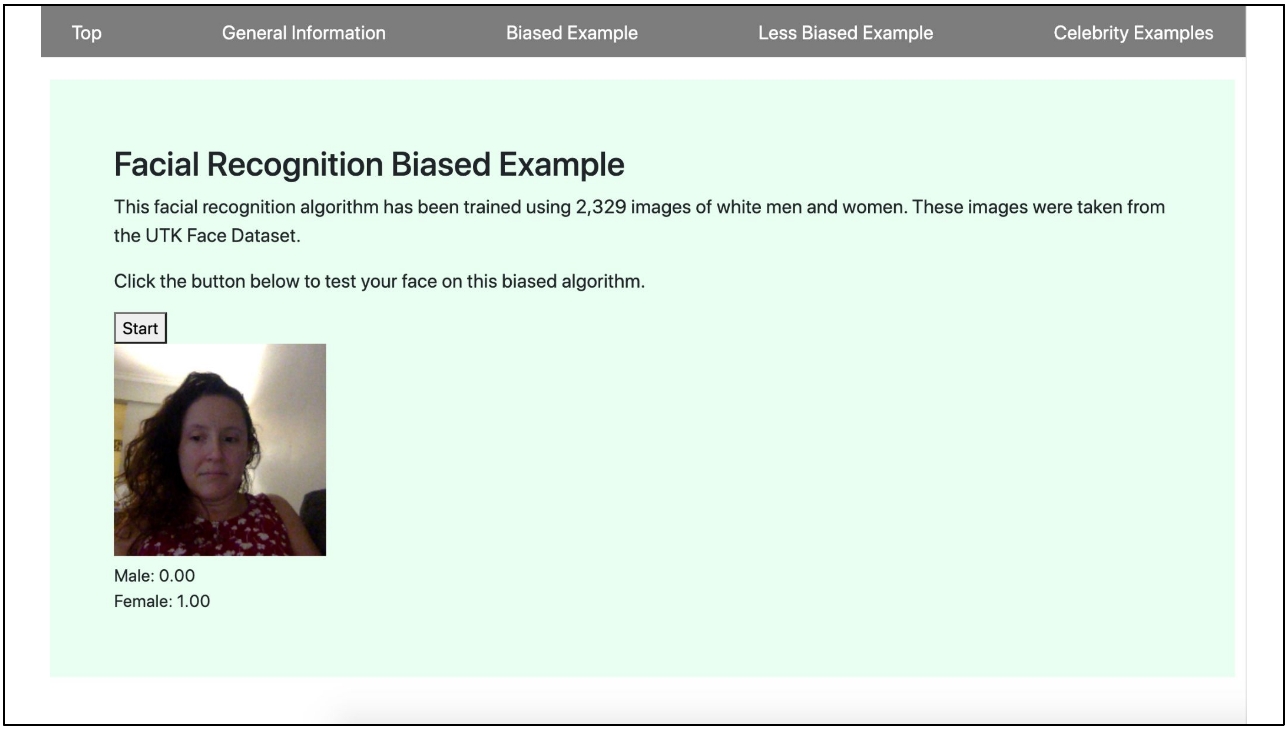
Facial Recognition algorithms do not simply work on their own, they first must be taught. All artificial intelligence goes through a series of trial and errors in order to perfect its identification process.

Oversimplified Facial Recognition Training Process*

1. A program is shown labeled images, for example of men and women.
2. The program searches for patterns amongst all the images labeled men and all the images labeled women.
3. The program is shown new unlabeled images and tries to categorize them based on the patterns it observed.
4. The program goes back and refines its definitions based on its successes and failures.

***Please note: this program and the subsequent facial recognition examples are based in gender being binary which is an antiquated construct as gender should now be recognized as a spectrum.**

General info



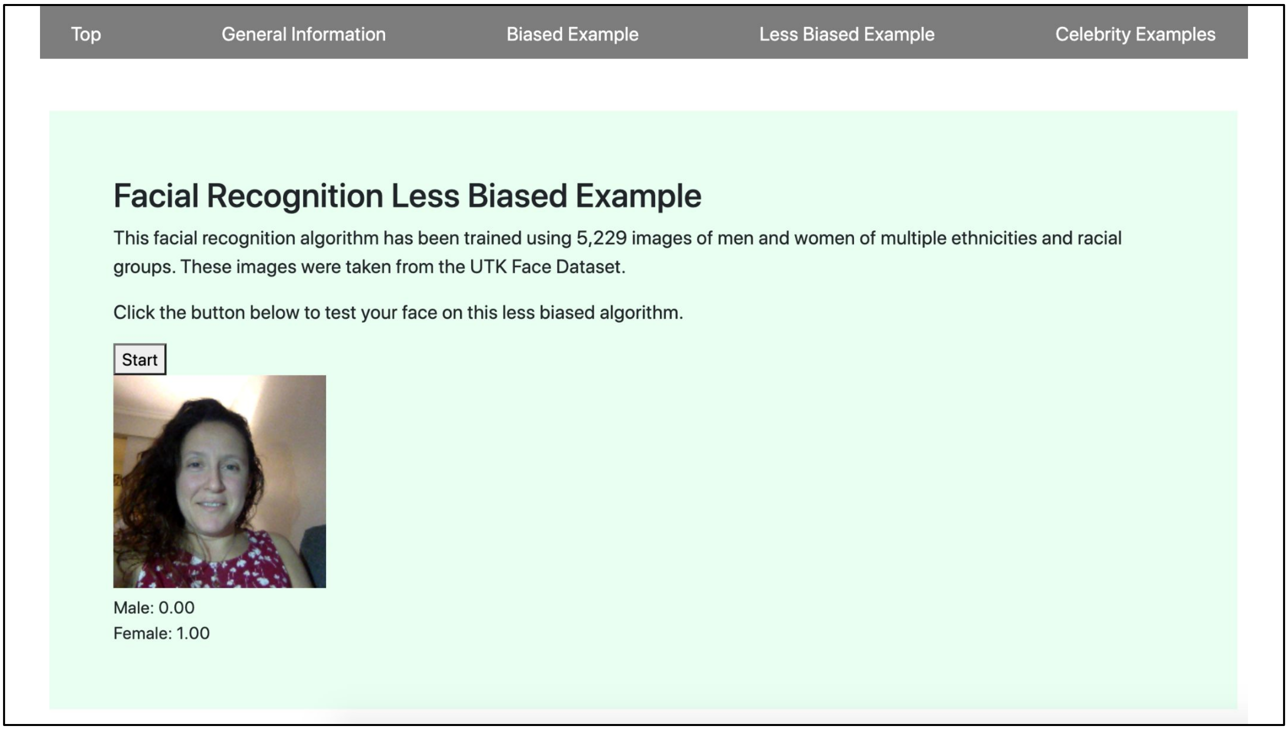
Facial Recognition Biased Example

This facial recognition algorithm has been trained using 2,329 images of white men and women. These images were taken from the UTK Face Dataset.

Click the button below to test your face on this biased algorithm.

Male: 0.00
Female: 1.00

This is our algorithm that has been trained on a variety of different faces (white) -- press start to see the camera and then it uses the computer's webcam as input and the algorithm is used on it to determine gender.



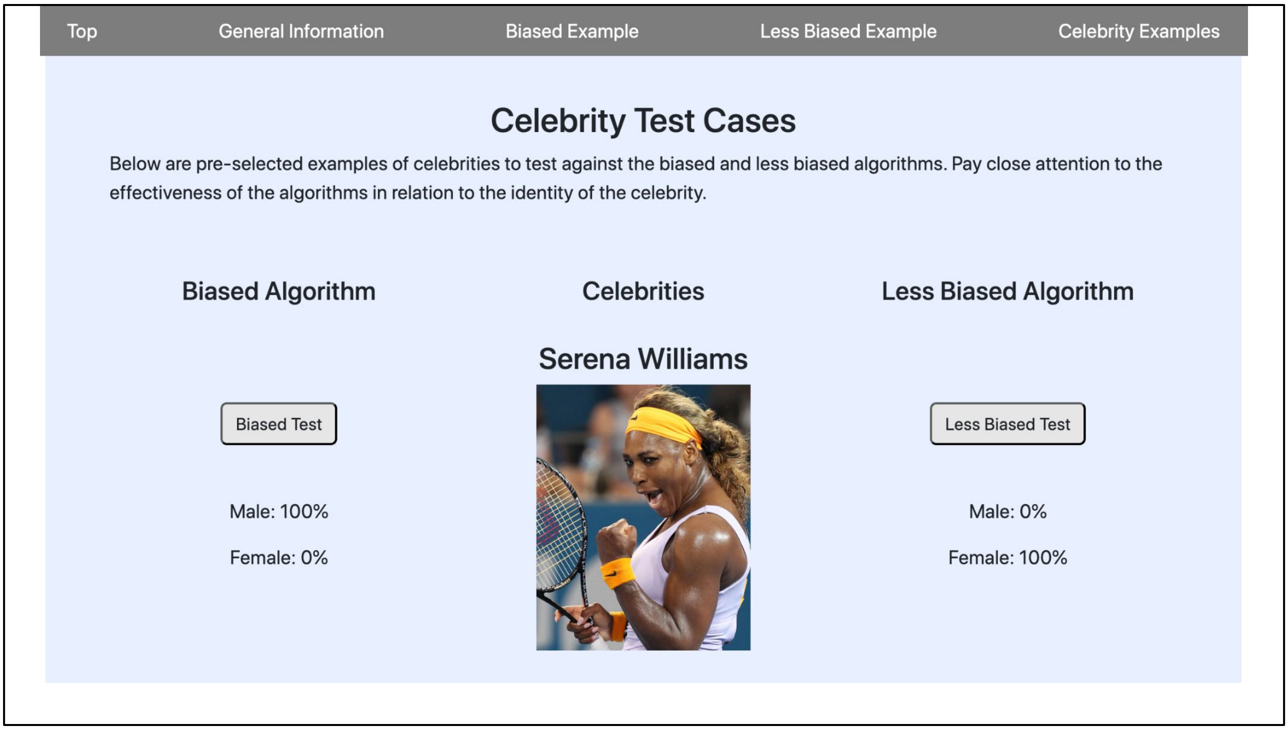
Facial Recognition Less Biased Example

This facial recognition algorithm has been trained using 5,229 images of men and women of multiple ethnicities and racial groups. These images were taken from the UTK Face Dataset.

Click the button below to test your face on this less biased algorithm.

Male: 0.00
Female: 1.00

This is our algorithm that has been trained on a variety of different faces (of all ethnicities) -- press start to see the camera and then it uses the computer's webcam as input and the algorithm is used on it to determine gender.

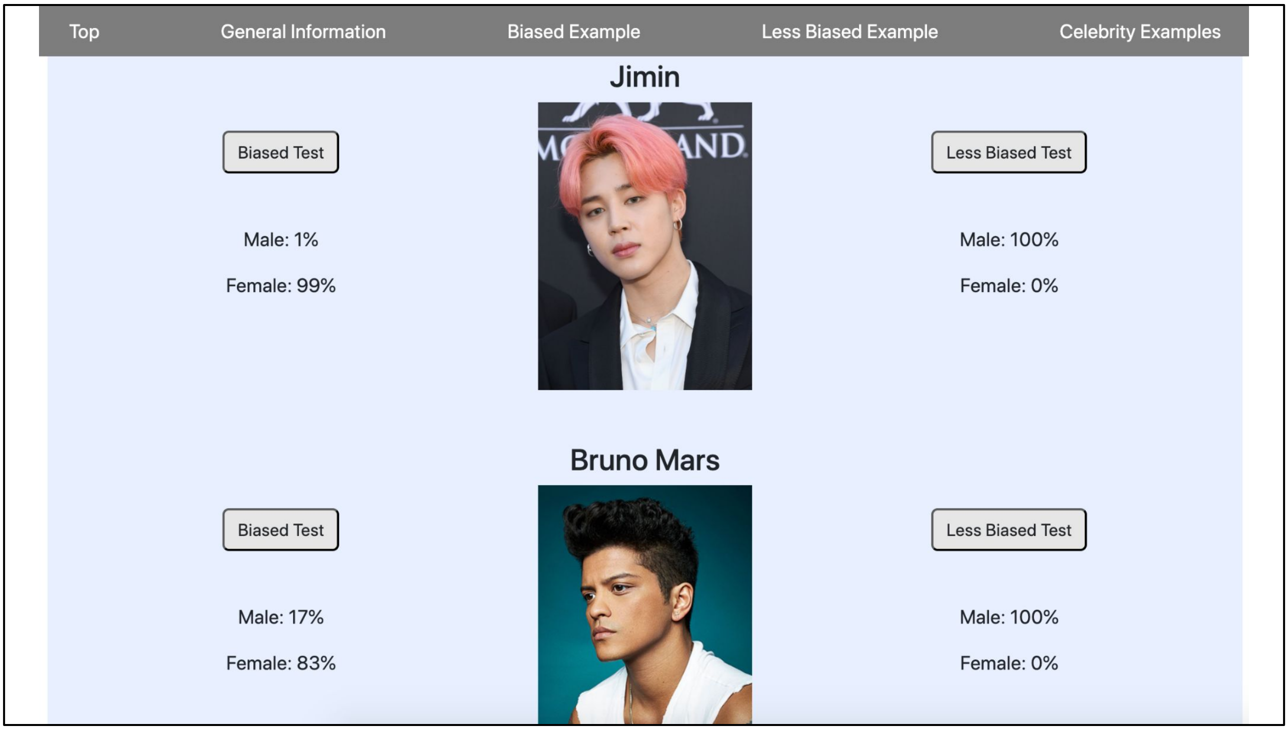


Celebrity Test Cases

Below are pre-selected examples of celebrities to test against the biased and less biased algorithms. Pay close attention to the effectiveness of the algorithms in relation to the identity of the celebrity.

Biased Algorithm	Celebrities	Less Biased Algorithm
	Serena Williams	
Male: 100%		Male: 0%
Female: 0%		Female: 100%

Serena Williams was incorrectly identified in the biased test as a man but this was rectified in the less biased tests.



Jimin

Male: 1%

Female: 99%

Male: 100%

Female: 0%

Bruno Mars

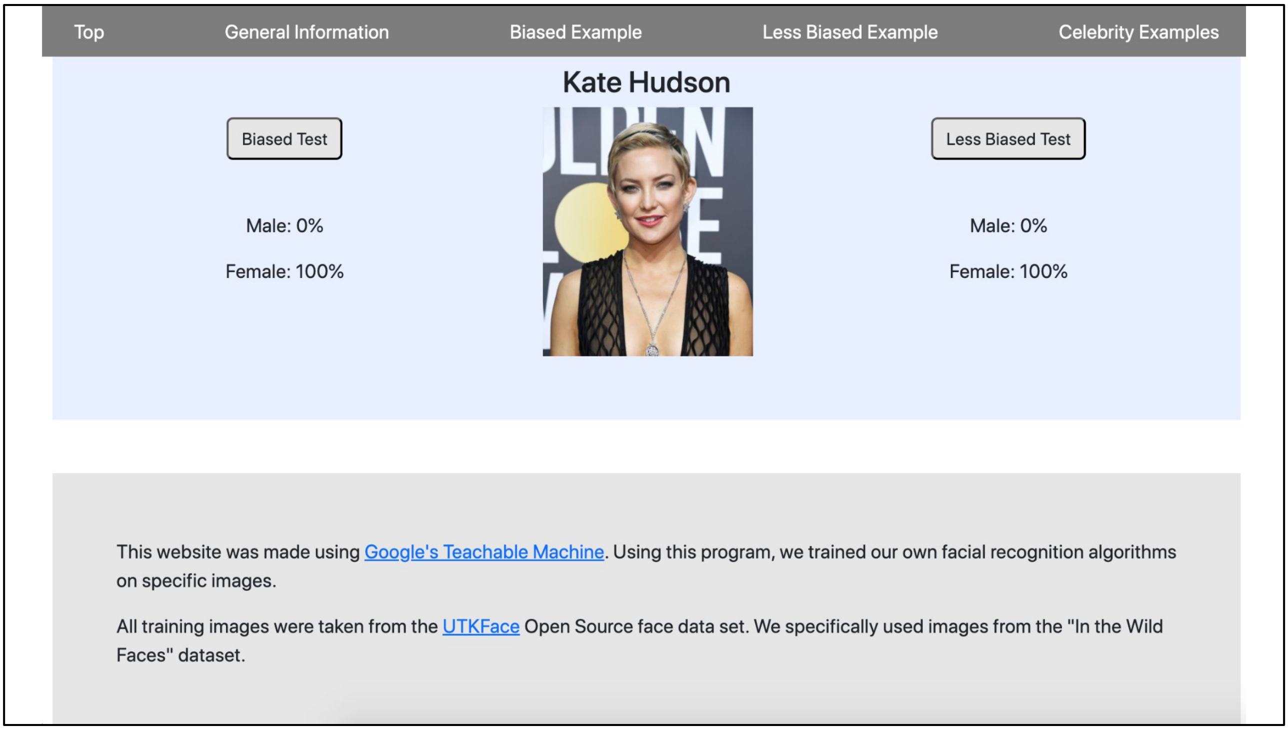
Male: 17%

Female: 83%

Male: 100%

Female: 0%

Both Jimin and Bruno Mars were incorrectly identified as female in the Biased tests but this was corrected in the less biased tests.



Kate Hudson

Male: 0%

Female: 100%

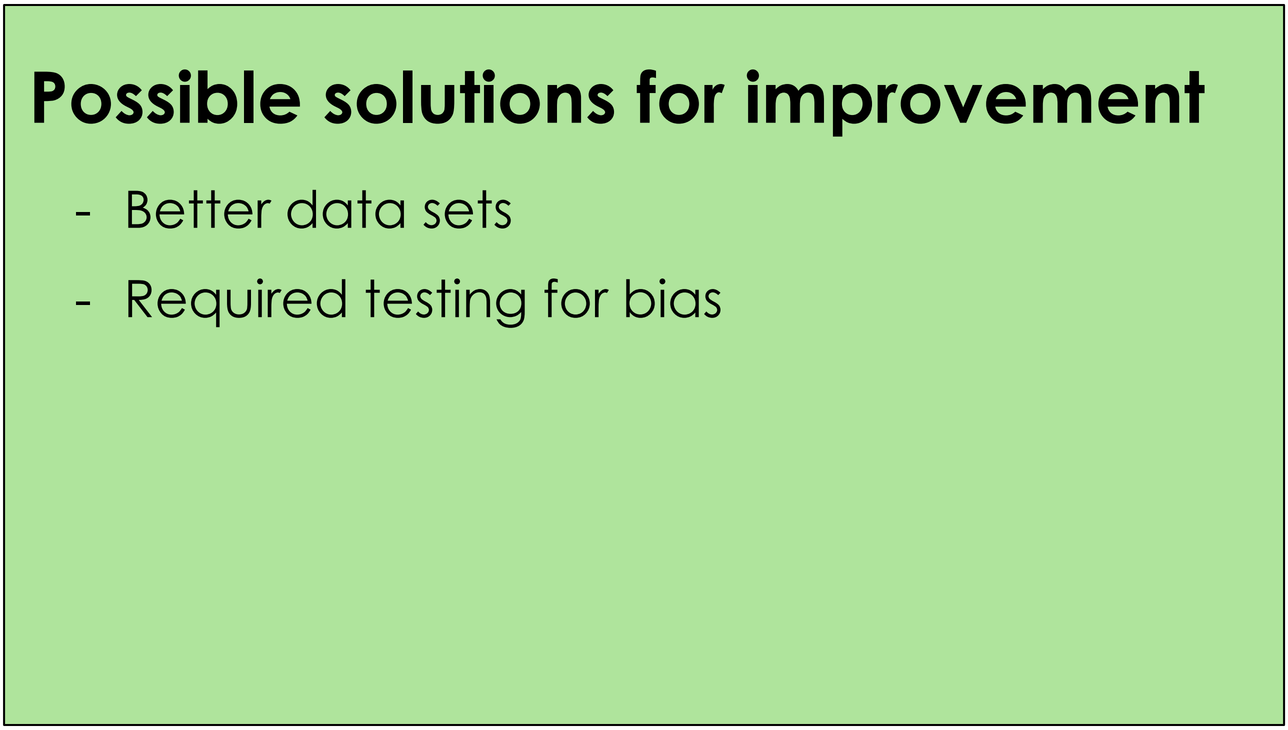
Male: 0%

Female: 100%

This website was made using Google's Teachable Machine. Using this program, we trained our own facial recognition algorithms on specific images.

All training images were taken from the UTKFace Open Source face data set. We specifically used images from the "In the Wild Faces" dataset.

Kate Hudson was a control -- she is white and was accurate in both situations.



Possible solutions for improvement

- Better data sets
- Required testing for bias

- **Better Data Sets:** need to be fully representative of all groups and all people
- **Require Testing for bias:** all algorithms should be fully tested before being implemented in the real world. Standards should be set for how successful it needs to be.

Given that we know this technology has flaws, should it be used in its current state?

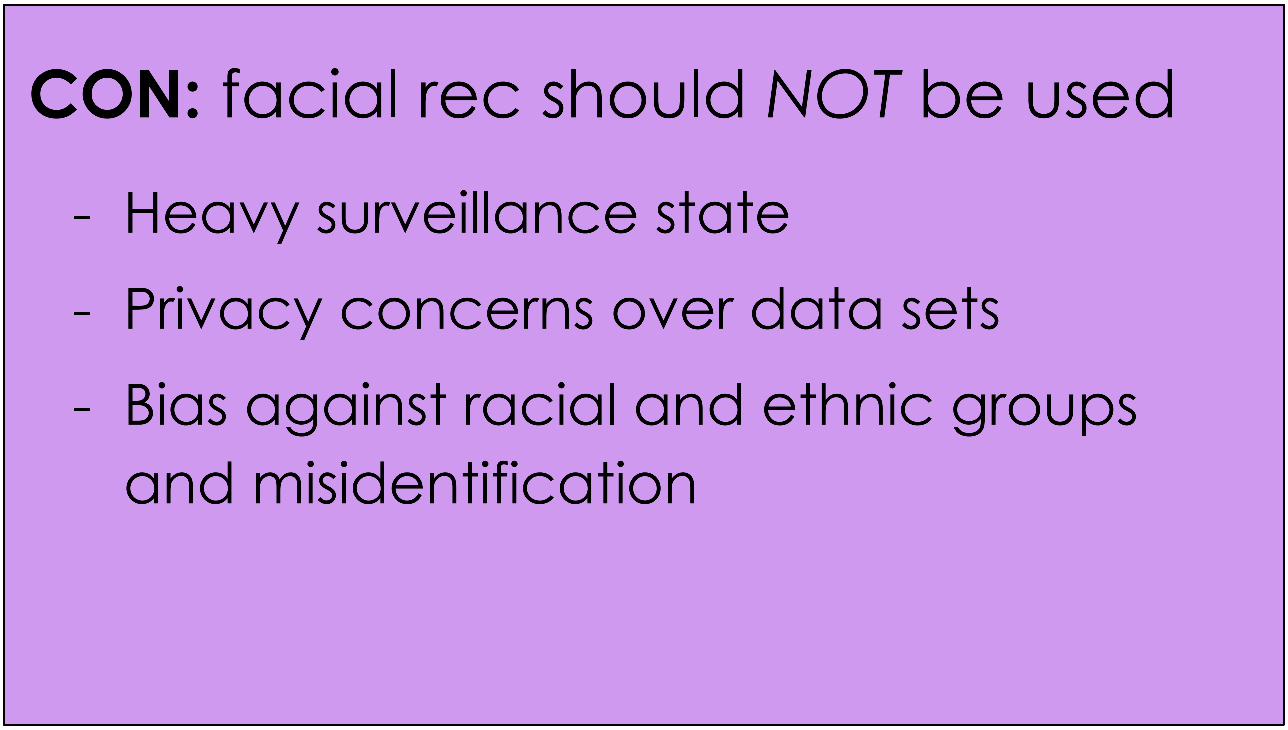
PRO: we *should* be using this technology in its flawed state.

PRO: facial rec should be used

- Convenient & useful
- Quick criminal and missing person identification
- You are already publicly viewable
- We must use it to know its flaws

- Biometric unlocking is super strong in conjunction with 2 factor authentication
    - Great as long as there is opt in
- Image tagging -- Facebook
    - Could lead you to determine if someone posted an image of you without your consent
- Speed up criminal investigations
    - Focus in on possible suspects rather than trying to broadly canvas
    - Great if used in conjunction with proper police training
- Child Trafficking
    - Compares pictures of online sex ads and checks for matches against photos of missing children
    - Helped identify 17,092 chidr3en.

CON: we *should not* be using this technology in its flawed state.



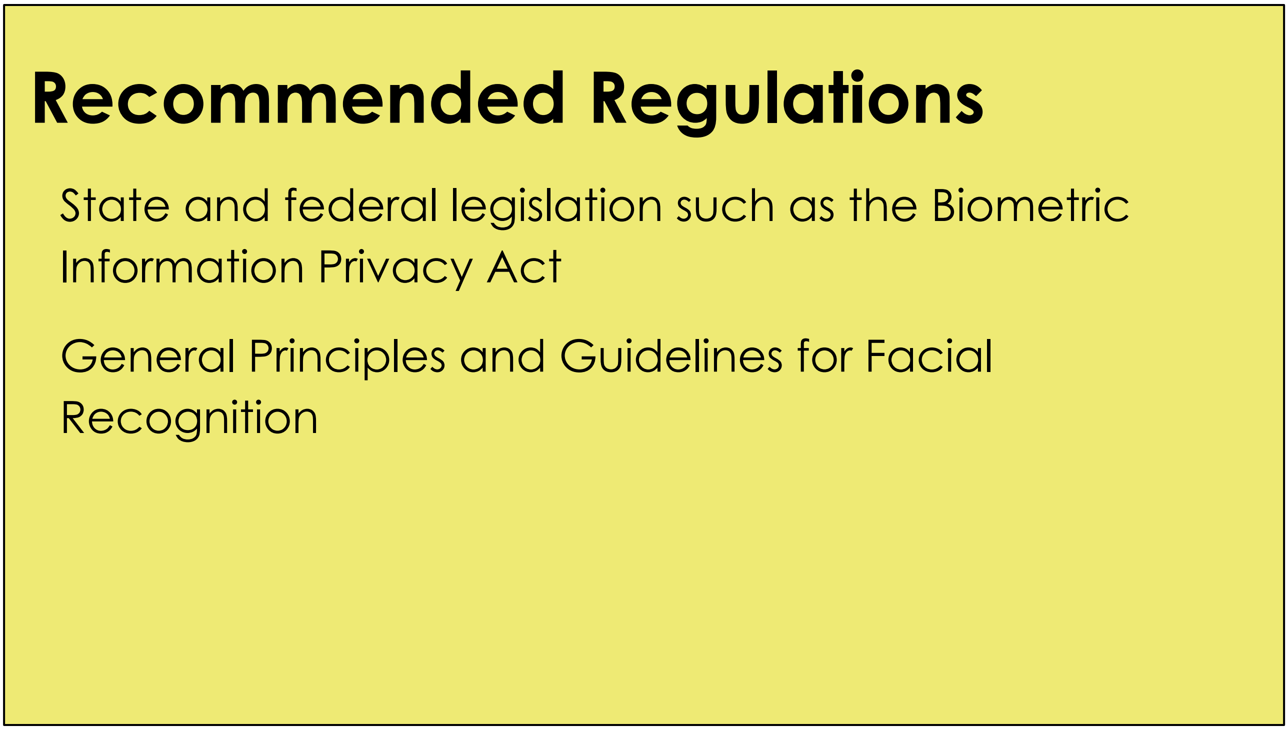
CON: facial rec should *NOT* be used

- Heavy surveillance state
- Privacy concerns over data sets
- Bias against racial and ethnic groups and misidentification

- Increased surveillance != increased safety
  - Decreased crime in Stockholm after cameras were added
  - Increased crime in MTA in NYC
- Protests:
  - BLM and Hong Kong, compiling lists of participants for future matching
  - Hong Kong -- figuring out ways to counteract surveillance (masks, lasers, etc)
- ICE: tracking immigrants in US (including with DMV and utility bills)
- Continued Bias: NYPD says they use a photo of a person committing a crime and try to match it on mug shots (which are BIPOC)
  - If they are matching with people already convicted then they are more likely to accuse someone of recommiting crime
- Privacy Concerns:
  - Stanford University public webcam and Duke University
  - Facial Recognition Verification Testing program run by National Institute of Standards and Technology -- uses images of:
    - children from child pornography
    - former convicts (alive and dead)
    - Potential US visa applicants

Our position

This technology should be allowed for recreational uses but has no place in law enforcement and government in a democratic and free state.



Recommended Regulations

State and federal legislation such as the Biometric Information Privacy Act

General Principles and Guidelines for Facial Recognition

BIPA - Passed in the Illinois legislature in 2008.

- protects the biometric data of an individual and
- prohibits its collection and use unless a company alerts the individual in writing about their intents, purpose and storage
- receives written consent.

General guidelines include:

- Protecting privacy and data of population
- consent
- Transparency
- Data security
- accountability