Should facial recognition systems be regulated?

What is facial recognition

- A first algorithm is presented with pictures of faces in known positions. Through training, the accuracy with which it can detect the faces increases. A second neural network learns how to tell the faces apart. This second neural network outputs a vector of numbers for each face, allowing the network to recognise unique faces. The combination of these two neural networks allows for rapid facial detection and recognition in real time.

Where is it currently used?

- In London the Metropolitan Police implemented live facial recognition 10 times between 2016 and 2019.
- The FBI has roughly 36.4 million photos of faces stored, which can be matched against in order to identify suspects.
- Retail and banks have incorporated facial recognition technology.
- Even celebrities have used this technology.

The current issues

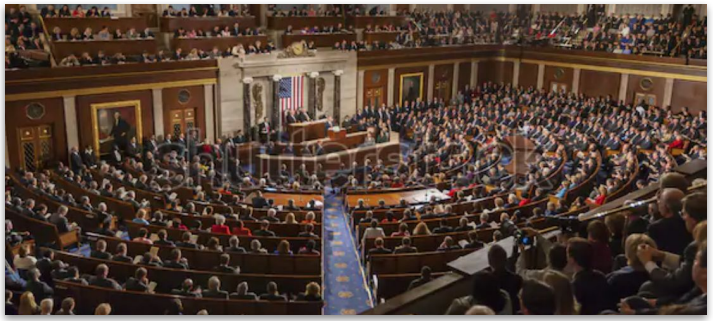
- The concern is that while identifying a few people associated with a crime, millions of unsuspecting people have their face and identity stored in databases.
- The Facial Recognition Vendor test found the error rate of identification of one algorithm was 0.1% when using good quality photos, but increased to 9.3% when presented with photos of people in public.
- In a simple test of identifying gender, 95.9% of errors by a facial recognition technology from Face++ were female subjects.
- Commercial facial recognition technology falsely identified African American and Asian faces 10 to 100 times more than white faces.

Positive uses of facial recognition technology

- It can help keep people safe by matching the face of someone caught on camera committing a crime, to an identity stored in a database of known or suspected offenders.
- Facial recognition can keep crowds safe by filtering out those who may be flagged or known to the police in real time.
- It can be useful for simple things like tagging friends in photos online.
- This technology makes life quicker and easier for people, for example unlocking their phones or easily accessing online banking.

The ‘Rekognition’ incident

- The American Civil Liberties Union instructed Rekognition to compare 2500 mugshots to photos of members of congress.
- 28 of the members of congress were wrongly identified as criminals.
- 39% of false matches were people of colour, however people of colour only make up 20% of congress.
- It is a cause for concern, considering Rekognition could be implemented in police surveillance, which would result in false matches more frequently for people of colour given the evidence above.



How could the flaws be addressed

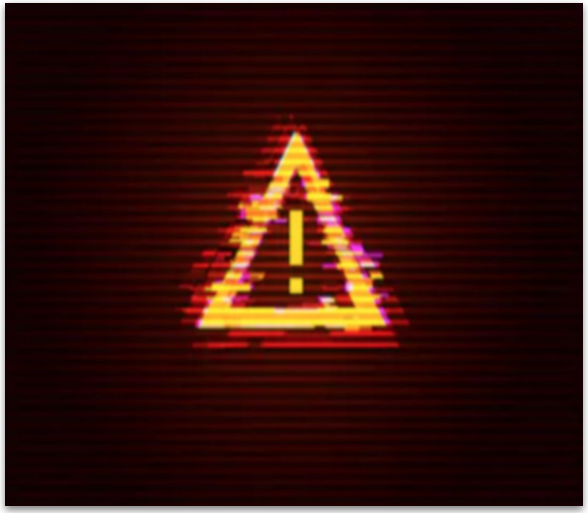
- Durham University has reduced racial bias by 1% in their facial recognition software by producing multiple images from faces with different racial features but consistent identifying features. This shifts the softwares reliance from race to unique facial features.
- Feeding the algorithm more images of women and people with darker skin tones is vital to tackle the issue of bias.
- Where an unbiased dataset is not possible, MIT has found that training algorithms to focus more heavily on underrepresented examples in the dataset reduces the accuracy gap between lighter and darker skinned males.

How do we regulate this technology

- Microsoft will not sell its software to the police until regulation is put in place.
- In the UK, a legislative framework will have to pass through Parliament.
- If such laws were to pass, what could be governed?
  - Facial recognition technology could be tested to meet a minimum standard.
  - Private companies selling their customer face identification data to public services could be banned or monitored.
  - Legal frameworks could be implemented to protect those who feel they have been wrongly misidentified by this technology.

Should it be regulated?

- In my opinion it should be regulated.
- The current facial recognition technology available to public services is still too biased.
- There are potential breaches of fundamental human rights and privacy that need to be expertly evaluated.
- In the wrong hands, it could be dangerous.
- Opt-out system.



Questions