Against
AI and Facial Recognition in Policing

Team A

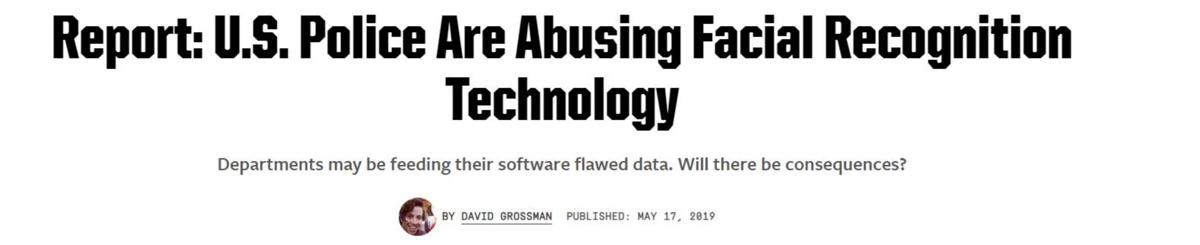
Privacy and inaccuracy concerns

Several cities in China uses facial recognition technology to fine and “humiliate” jaywalkers, but the system was soon cancelled due to inaccuracies in the recognition results, which often displays other citizen’s information on the screen.

Automated-policing approaches are often inaccurate. A 2018 trial conducted by the London Metropolitan Police used facial recognition to identify 104 previously unknown people who were suspected of committing crimes. Only 2 of the 104 were accurate.

Potential abuse of power

- False inputs from officers (using other images to find criminals)
- Lack of training of officers using the technology leads to abuse
- Use of composite sketches leads to false arrests
- Focus on matching face rather than solving crime
- Could be used against protesters and others exercising civil liberties



Report: U.S. Police Are Abusing Facial Recognition Technology

Departments may be feeding their software flawed data. Will there be consequences?

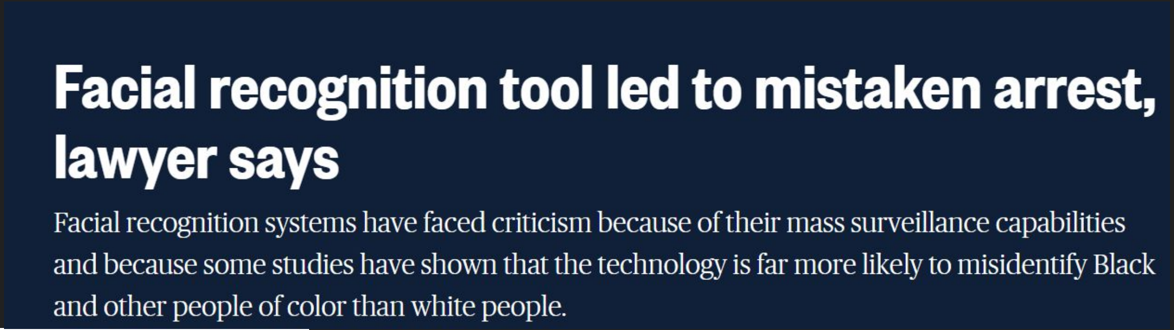
BY DAVID GROSSMAN PUBLISHED: MAY 17, 2019

Wrongfully arrested man sues Detroit police over false facial recognition match

Robert Williams, a 43-year-old father in the Detroit suburb of Farmington Hills, was arrested last year on charges he'd taken watches from a Shinola store after police investigators used a facial recognition search of the store's surveillance-camera footage that identified him as the thief.

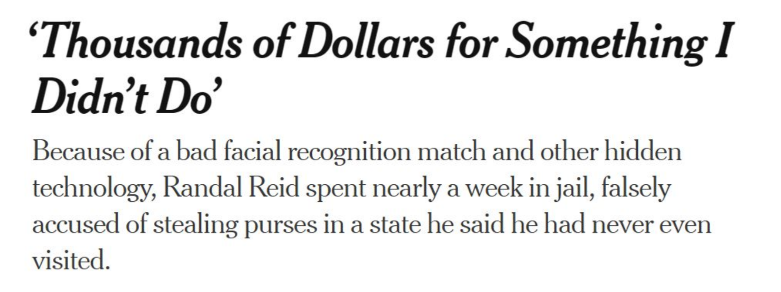
Prosecutors dropped the case less than two weeks later, arguing that officers had relied on insufficient evidence. Police Chief James Craig later apologized for what he called "shoddy" investigative work. Williams, who said he had been driving home from work when the 2018 theft had occurred, was interrogated by detectives and held in custody for 30 hours before his release.

Racially biased systems



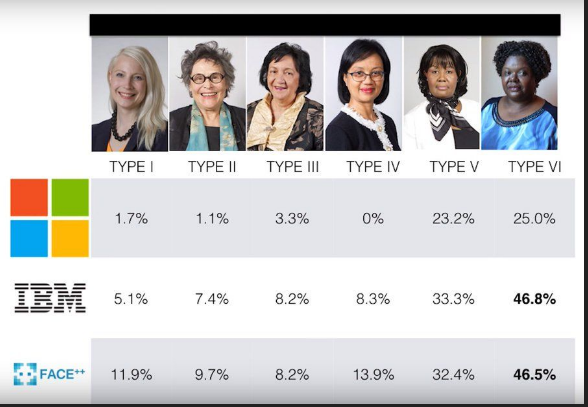
Facial recognition tool led to mistaken arrest, lawyer says

Facial recognition systems have faced criticism because of their mass surveillance capabilities and because some studies have shown that the technology is far more likely to misidentify Black and other people of color than white people.

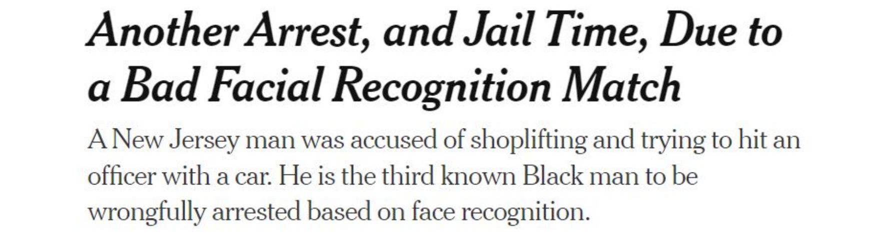


‘Thousands of Dollars for Something I Didn’t Do’

Because of a bad facial recognition match and other hidden technology, Randal Reid spent nearly a week in jail, falsely accused of stealing purses in a state he said he had never even visited.



	TYPE I	TYPE II	TYPE III	TYPE IV	TYPE V	TYPE VI
🟥🟩🟦🟨	1.7%	1.1%	3.3%	0%	23.2%	25.0%
IBM	5.1%	7.4%	8.2%	8.3%	33.3%	**46.8%**
FACE++	11.9%	9.7%	8.2%	13.9%	32.4%	**46.5%**

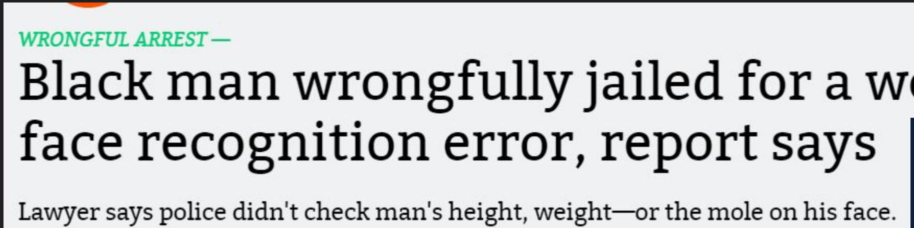


Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match

A New Jersey man was accused of shoplifting and trying to hit an officer with a car. He is the third known Black man to be wrongfully arrested based on face recognition.

Racially biased systems, cont.

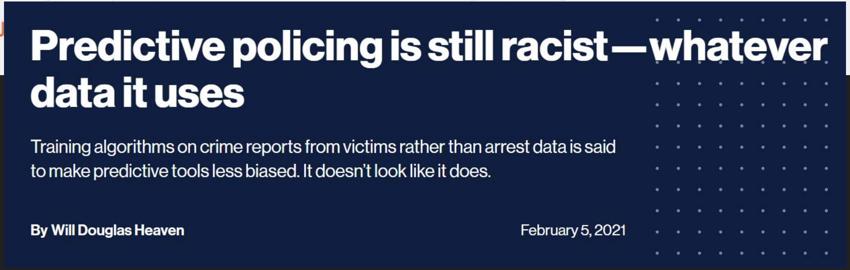
- Predictive policing
- AI trained on already biased police datasets will end up biased
- High rate of error when it comes to people of color



WRONGFUL ARREST —

Black man wrongfully jailed for a week after face recognition error, report says

Lawyer says police didn't check man's height, weight—or the mole on his face.

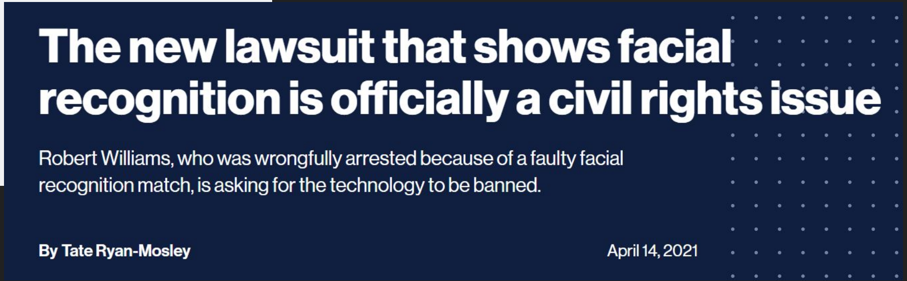


Predictive policing is still racist—whatever data it uses

Training algorithms on crime reports from victims rather than arrest data is said to make predictive tools less biased. It doesn't look like it does.

By Will Douglas Heaven

February 5, 2021



The new lawsuit that shows facial recognition is officially a civil rights issue

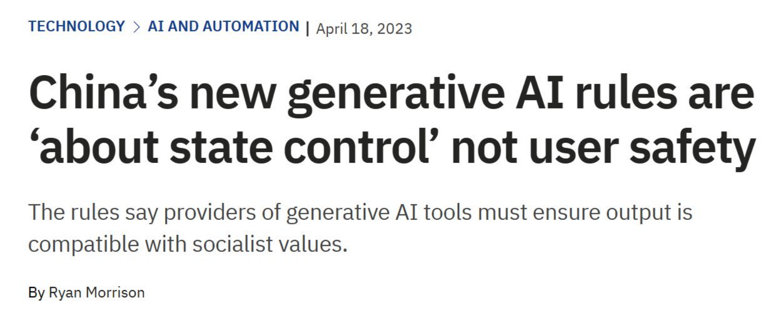
Robert Williams, who was wrongfully arrested because of a faulty facial recognition match, is asking for the technology to be banned.

By Tate Ryan-Mosley

April 14, 2021

Negative effects on civil liberties

Moderation rules in the guidelines place a requirement on providers to ensure content is consistent with “social order and societal morals”, and doesn’t endanger national security.



TECHNOLOGY > AI AND AUTOMATION | April 18, 2023

China’s new generative AI rules are ‘about state control’ not user safety

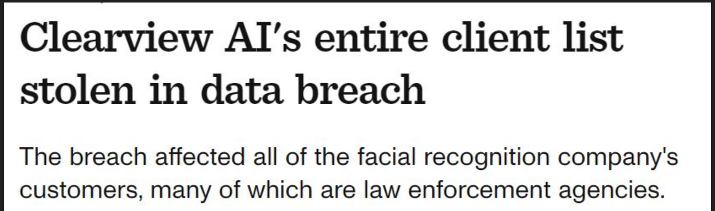
The rules say providers of generative AI tools must ensure output is compatible with socialist values.

By Ryan Morrison

Data leaks will lead to further privacy breaches

Unauthorized or unintended exposure of sensitive or confidential data during the **training**, testing, or deployment phases of an **AI system**

- **Training Data Leakage:** If the training data is sensitive AI model reproduce this sensitive information, potentially compromising privacy or intellectual property.
- **Feature Leakage:** For example, in a medical dataset, even if the patient names are removed, certain features like age, gender, or ZIP code might indirectly identify individuals.
- **Model / data Leakage :** an adversary gains access to the trained AI model itself or the sensitive data. This can happen if the model is shared or distributed without proper safeguards
- **Output Leakage:** For instance, if a recommender system inadvertently exposes user preferences or private data through its recommendations



Clearview AI's entire client list stolen in data breach

The breach affected all of the facial recognition company's customers, many of which are law enforcement agencies.

Rebuttal

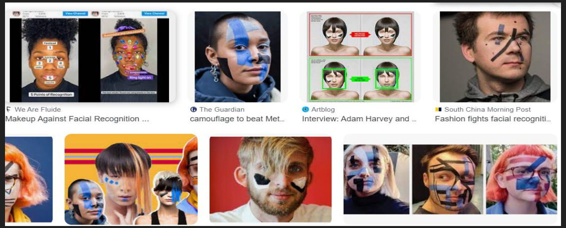
It is risky to have complete transparency regarding policies/algorithms because it creates security concerns, making the system weaker and more subject to security breaches (malware, cyber attacks, hacking, etc.)

- AI systems, especially those used by state surveillance organizations or governments handle massive amounts of data
- Any data breach would have massive negative consequences

Mass surveillance on online platforms will further damage the freedom of speech

How could you make sure that face recognition is used temporarily and data is not being stored?

Rebuttal, cont.



We Are Fluide
Makeup Against Facial Recognition ...

The Guardian
camouflage to beat Met...

Artblog
Interview: Adam Harvey and ...

South China Morning Post
Fashion fights facial recogniti...

- Facial recognition used via social media used as data for state policing, privacy concerns on an international level: TikTok
- Data needed to offset biases would create massive privacy concerns
- Data storage issues
- Anti-facial recognition camouflage emerging, effective countermeasures are emerging and making facial recognition for policing obsolete
  - AI algorithm (eg. facial recognition) helps crime prevention and investigation
  - Criminals are aware of these technologies, which may make existed digital forensics methods (eg. CCTV) ineffective