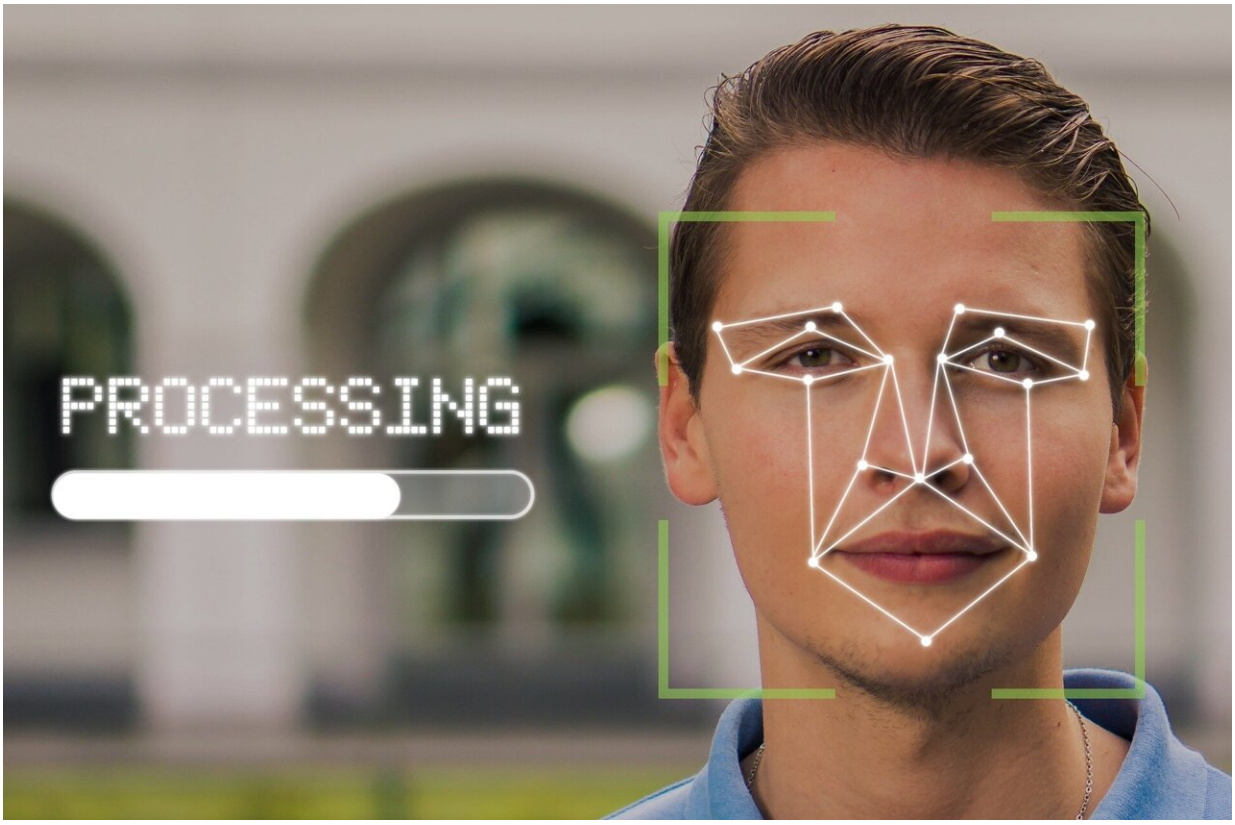
Face recognition technology follows a long analog history of surveillance and control based on physical features

January 20 2024, by Sharrona Pearl



Credit: Pixabay/CC0 Public Domain

American Amara Majeed was accused of terrorism by the Sri Lankan police in 2019. Robert Williams was arrested outside his house in

Detroit and detained in jail for 18 hours for allegedly stealing watches in 2020. Randal Reid spent six days in jail in 2022 for supposedly using stolen credit cards in a state he'd never even visited.

In all three cases, the authorities had the wrong people. In all three, it was face recognition technology that told them they were right. Law enforcement officers in many U.S. states are not required to reveal that they used face recognition technology to identify suspects.

Face recognition technology is the latest and most sophisticated version of biometric surveillance: using unique physical characteristics to identify individual people. It stands in a long line of technologies—from the fingerprint to the passport photo to iris scans—designed to monitor people and determine who has the right to move freely within and across borders and boundaries.

In my book, "Do I Know You? From Face Blindness to Super Recognition," I explore how the story of face surveillance lies not just in the history of computing but in the history of medicine, of race, of psychology and neuroscience, and in the health humanities and politics.

Viewed as a part of the long history of people-tracking, face recognition techology's incursions into privacy and limitations on free movement are carrying out exactly what biometric surveillance was always meant to do.

The system works by converting captured faces—either static from photographs or moving from video—into a series of unique data points, which it then compares against the data points drawn from images of faces already in the system. As face recognition technology improves in accuracy and speed, its effectiveness as a means of surveillance becomes ever more pronounced.

Accuracy improves, but biases persist

Surveillance is predicated on the idea that people need to be tracked and their movements limited and controlled in a trade-off between privacy and security. The assumption that less privacy leads to more security is built in.

That may be the case for some, but not for the people disproportionately targeted by face recognition technology. Surveillance has always been designed to identify the people whom those in power wish to most closely track.

On a global scale, there are caste cameras in India, face surveillance of Uyghurs in China and even attendance surveillance in U.S. schools, often with low-income and majority-Black populations. Some people are tracked more closely than others.

In addition, the cases of Amara Majeed, Robert Williams and Randal Reid aren't anomolies. As of 2019, face recognition technology misidentified Black and Asian people at up to 100 times the rate of white people, including, in 2018, a disproportionate number of the 28 members of the U.S. Congress who were falsely matched with mug shots on file using Amazon's Rekognition tool.

When the database against which captured images were compared had only a limited number of mostly white faces upon which to draw, face recognition technology would offer matches based on the closest alignment available, leading to a pattern of highly racialized—and racist—false positives.

With the expansion of images in the database and increased sophistication of the software, the number of false positives—incorrect matches between specific individuals and images of wanted people on file—has declined dramatically. Improvements in pixelation and mapping static images into moving ones, along with increased social

media tagging and ever more sophisticated scraping tools like those developed by Clearview AI, have helped decrease the error rates.

The biases, however, remain deeply embedded into the systems and their purpose, explicitly or implicitly targeting already targeted communities. The technology is not neutral, nor is the surveillance it is used to carry out.

Latest technique in a long history

Face recognition software is only the most recent manifestation of global systems of tracking and sorting. Precursors are rooted in the now-debunked belief that bodily features offer a unique index to character and identity. This pseudoscience was formalized in the late 18th century under the rubric of the ancient practice of physiognomy.

Early systemic applications included anthropometry (body measurement), fingerprinting and iris or retinal scans. They all offered unique identifiers. None of these could be done without the participation—willing or otherwise—of the person being tracked.

The framework of bodily identification was adopted in the 19th century for use in criminal justice detection, prosecution and record-keeping to allow governmental control of its populace. The intimate relationship between face recognition and border patrol was galvanized by the introduction of photos into passports in some countries including Great Britain and the United States in 1914, a practice that became widespread by 1920.

Face recognition technology provided a way to go stealth on human biometric surveillance. Much early research into face recognition software was funded by the CIA for the purposes of border surveillance.

It tried to develop a standardized framework for face segmentation: mapping the distance between a person's facial features, including eyes, nose, mouth and hairline. Inputting that data into computers let a user search stored photographs for a match. These early scans and maps were limited, and the attempts to match them were not successful.

More recently, private companies have adopted data harvesting techniques, including face recognition, as part of a long practice of leveraging personal data for profit.

Face recognition technology works not only to unlock your phone or help you board your plane more quickly, but also in promotional store kiosks and, essentially, in any photo taken and shared by anyone, with anyone, anywhere around the world. These photos are stored in a database, creating ever more comprehensive systems of surveillance and tracking.

And while that means that today it is unlikely that Amara Majeed, Robert Williams, Randal Reid and Black members of Congress would be ensnared by a false positive, face recognition technology has invaded everyone's privacy. It—and the governmental and private systems that design, run, use and capitalize upon it—is watching, and paying particular attention to those whom society and its structural biases deem to be the greatest risk.

Provided by The Conversation

https://techxplore.com/news/2024-01-recognition-technology-analog-history-surveillance.html