Facial recognition: UK plans to monitor migrant offenders are unethical—and they won't work

August 18 2022, by Namrata Primlani

Credit: Clément Proust from Pexels

One afternoon in our lab, my colleague and I were testing our new prototype for a facial recognition software on a laptop. The software used a video camera to scan our faces and guess our age and gender. It correctly guessed my age but when my colleague, who was from Africa, tried it out, the camera didn't detect a face at all. We tried turning on lights in the room, adjusted her seating and background, but the system still struggled to detect her face.

After many failed attempts, the software finally detected her face—but got her age wrong and gave the wrong gender.

Our software was only a prototype, but the difficulty working with darker skin tones reflects the experiences of people of color who try to use facial recognition technology. In recent years, researchers have demonstrated the unfairness in facial recognition systems, finding that the software and algorithms developed by big technology companies are more accurate at recognizing lighter skin tones than darker ones.

Yet recently, the Guardian reported that the UK Home Office plans to make migrants convicted of criminal offenses scan their faces five times a day using a smart watch equipped with facial recognition technology. A spokesperson for the Home Office said facial recognition technology would not be used on asylum seekers arriving in the UK illegally, and that the report on its use on migrant offenders was "purely speculative."

Get the balance right

There will always be a tension between national security and individual rights. Security for the many can take priority over privacy for a few. For example, in November 2015 when the terrorist group ISIS attacked Paris, killing 130 people, the Paris police found a phone that one of the terrorists had abandoned at the scene, and read messages stored on it.

There is a lot of nuance to this issue. We must ask ourselves, whose rights are curbed by a breach of privacy, to what degree, and who judges if a breach of privacy is in balance with the severity of a criminal offense?

In the case of offenders taking photographs of their faces several times a day, we could argue the breach of privacy is in the national security interest for most people, if the crime is serious. The government is entitled to make such a decision as it is responsible for the safety of its citizens. For minor offenses, however, face recognition may be too strong a measure.

In its plan, the Home Office has not differentiated between minor and serious offenders; nor has it provided convincing evidence that facial recognition improves people's compliance with immigration law.

Credit: Clément Proust from Pexels

Worldwide, we know facial recognition is more likely to be used to police people of color by monitoring their movements more often than those of white people. This is despite the fact that facial recognition systems are more accurate with lighter than darker skin tones.

Taking a picture of your face and uploading it five times a day could feel demeaning. Glitches with darker skin tones could make checking into the system more than just a frustrating experience. There could be serious consequences for offenders if the technology fails.

The flaws in facial recognition might also create national security issues for the government. For example, it might misidentify the face of one person as another. Facial recognition technology is not ready for something as important as national security.

The alternative

Another option the government is considering for migrant offenders is location tracking. Electronic monitoring already keeps track of people with criminal records in the UK using ankle tags, and it would make sense to apply the same technology to migrant and non-migrant offenders equally.

Location tracking comes with its own ethical issues for personal privacy and racial surveillance. Due to the intrusive nature of electronic monitoring, some people who wear these devices can suffer from depression, anxiety or suicidal thoughts.

But location tracking technology gives options, at least. For example, data can be handled sensitively by following data privacy guidelines such as the UK's Data Protection Act 2018. We can minimize the amount of location data we collect by only tracking someone's location once or twice a day. We can anonymize the data, only making people's names visible when and where necessary.

The UK Home Office could use location data to flag up suspicious activity, such as if an offender enters an area from which they have been barred. For minor offenders, we need not track the person's exact location but only the general area, such as a postcode or town.

As a society, we should strive to maintain the dignity and privacy of people, except in the most serious cases. More importantly, we should ensure technology does not have the potential to discriminate against a

group of people based on their ethnicity. The law and regulation should apply equally to all people.

The Home Office spokesperson added: "The public expects us to monitor convicted foreign national offenders … Foreign criminals should be in no doubt of our determination to deport them, and the government is doing everything possible to increase the number of foreign national offenders being deported."

Provided by The Conversation

Citation: Facial recognition: UK plans to monitor migrant offenders are unethical—and they won't work (2022, August 18) retrieved 26 April 2024 from https://techxplore.com/news/2022-08-facial-recognition-uk-migrant-unethicaland.html