AI facial analysis is scientifically questionable. Should we be using it for border control?

February 24 2021, by Niamh Kinchin

Credit: Pavel Danilyuk from Pexels

Developments in global border control technologies are providing innovative ways to address issues relating to migration, asylum-seeking

and the introduction of illegal goods into countries.

But while governments and national security can benefit from this, advanced surveillance technology creates risks for the misuse of personal data and the violation of human rights.

Technology at the border

One of US President Joe Biden's first actions was to introduce a bill that prioritizes "smart border controls," as part of a commitment to "restore humanity and American values to our immigration system."

These controls will supplement existing resources at the border with Mexico. They will include technology and infrastructure developed to enhance the screening of incoming asylum seekers and prevent the arrival of narcotics.

According to Biden, "cameras, sensors, large-scale X-ray machines and fixed towers" will all be used. This likely entails the use of infrared cameras, motion sensors, facial recognition, biometric data, aerial drones and radar.

Under the Trump administration, the Immigration and Customs Enforcement agency (ICE) partnered with controversial data analytics firm Palantir to link tip-offs from police and citizens with other databases, in a bid to arrest undocumented people.

Similarly, from 2016 to 2019, Hungary, Latvia and Greece piloted an automated lie-detection test funded by the European Union's research and innovation funding program, Horizon 2020.

The iBorderCtrl test analyzed the facial micro-gestures of travelers crossing international borders at three undisclosed airports, with the aim

of determining whether travelers were lying about the purpose of their trip.

Avatars questioned travelers about themselves and their trip while webcams scanned face and eye movements.

Europe's border and coastguard agency Frontex has also been investing in border control technology for several years. Since last year, Frontex has operated unmanned drones to detect asylum-seekers attempting to enter various European states.

While Australia has been slower to implement enhanced surveillance at maritime borders, in 2018 the federal government announced it would spend A$7 billion on six long-range unmanned drones to monitor Australian waters. These aren't expected to be operational until at least 2023.

Automated border control systems, however, have been used since 2007. SmartGates at many international airports use facial recognition to verify travelers' identities against data stored in biometric passports.

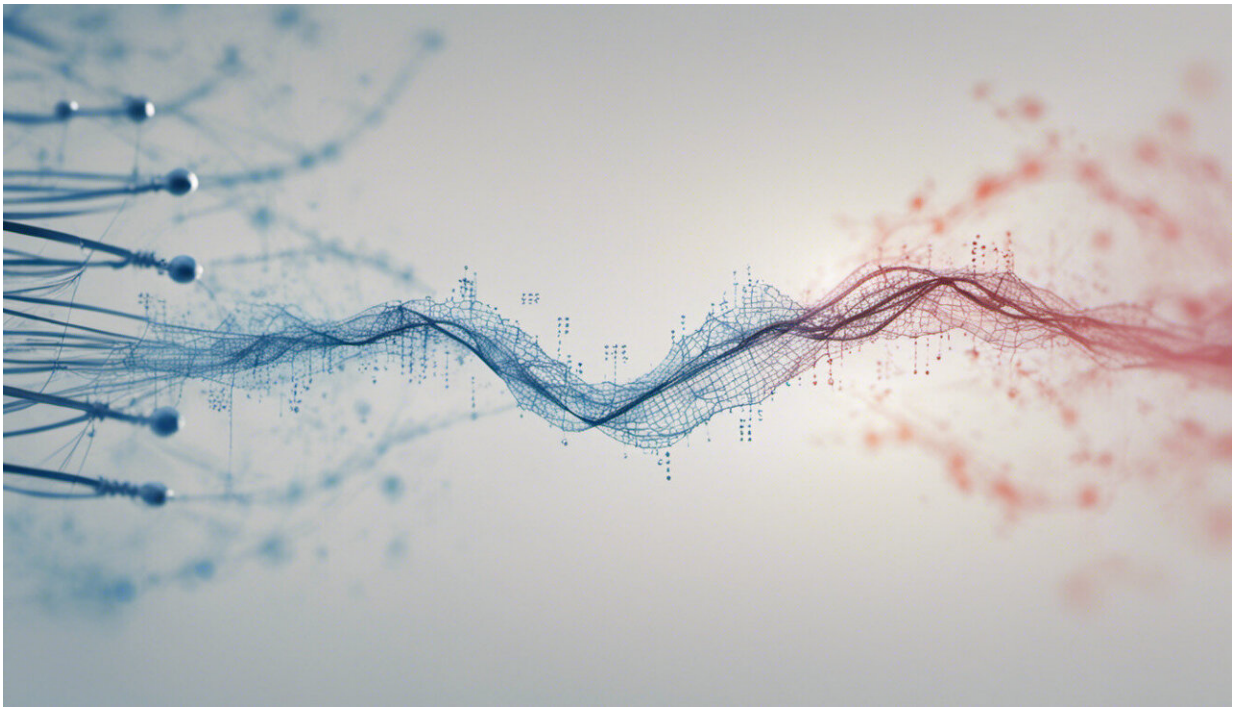
Last year, the Department of Human Services implemented the Enterprise Biometric Identification Services. The system was reportedly rolled out to meet an expected surge in demand for visa applications and citizenship.

It combines authentication technology with biometrics to match the faces and fingerprints of people who wish to travel to Australia.

Misuse of data

Governments may promise, as the Biden administration does, that technology will only serve "legitimate agency purposes." But data misuse

by governments is well documented.



Credit: AI-generated image (disclaimer)

Between 2014 and 2017 in the US, ICE used facial recognition to mine state drivers license databases to detect "illegal immigrants."

Refugees in various countries, including Kenya and Ethiopia, have had their biometric data collected for years.

In 2017, Bangladeshi Industry Minister Amir Hossain Amu said the government was collecting biometric data from Rohingya people in the country to "keep record" of them and send them "back to their own place."

Data misuse can also happen when questionable "science" is involved. For instance, emotion recognition algorithms used in unproven lie-detection tests are highly problematic.

The way people communicate varies widely across cultures and situations. Someone's ability to answer a question at a border could be affected by trauma, their personality, the way the question is framed or the perceived intentions of the interviewer.

Technologies such as iBorderCtrl undermine the rights of migrants, asylum-seekers and all international travelers. They could be used to refuse entry or detain travelers based on race or ethnicity.

Racial profiling at borders isn't uncommon. It came to light again when New South Wales MP Mehreen Faruqi experienced it at a US airport in 2016.

The Pakistani-born Greens member told The Guardian she was detained at an airport for more than an hour, after immigration staff took her fingerprint, asked her where she was "originally from" and how she got an Australian passport.

Facial recognition technology has already been found to be capable of bias against people of color. Enlisting this at airports and maritime borders—where human rights have historically been undermined on the basis of race—could be disastrous.

Fighting back

The good news is many people are now speaking out against how border control technologies can impact migrants, refugees and other travelers.

In February, the European Court of Justice heard a case brought by

digital rights activist and German politician Patrick Breyer.

Breyer is seeking the release of documents on the ethical evaluation, legal admissibility, marketing and test results of iBorderCtrl. He is concerned the EU is being secretive about a "scientifically highly controversial project" funded by taxpayer money.

In Australia, the Digital Rights Watch is the main organization that scrutinizes surveillance practices.

Of particular concern is the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. This gives the Australian Border Force extensive powers to search devices carried by people traveling internationally.

Last year the government recommended the legislation be amended so agencies can't authorize the detention of travelers whose devices are searched by the border force.

However, without an Australia bill of rights, which would prevent laws that infringed privacy rights, the potential for data misuse will persist.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation