Large-scale facial recognition is incompatible with a free society

10 July 2020, by Seth Lazar, Claire Benn, Mario Günther

Credit: Shutterstock

In the US, tireless opposition to state use of facial recognition algorithms has recently won some victories.

Some progressive cities have banned some uses of the technology. Three tech companies have pulled facial recognition products from the market. Democrats have advanced a bill for a moratorium on facial recognition. The Association for Computing Machinery (ACM), a leading computer science organization, has also come out against the technology.

Outside the US, however, the tide is heading in the other direction. China is deploying facial recognition on a vast scale in its social credit experiments, policing, and suppressing the Uighur population. It is also exporting facial recognition technology (and norms) to partner countries in the Belt and Road initiative. The UK High Court ruled its use by South Wales Police lawful last September (though the decision is being appealed).

Here in Australia, despite pushback from the Human Rights Commission, the trend is also towards greater use. The government proposed an ambitious plan for a national face database (including wacky trial balloons about age-verification on porn sites). Some local councils are adding facial recognition into their existing surveillance systems. Police officers have tried out the dystopian services of Clearview AI.

Should Australia be using this technology? To decide, we need to answer fundamental questions about the kind of people, and the kind of society, we want to be.

From facial recognition to face surveillance

Facial recognition has many uses.

It can verify individual identity by comparing a target image with data held on file to confirm a match—this is "one-to-one" facial recognition. It can also compare a target image with a database of subjects of interest. That's "one-to-many." The most ambitious form is "all-to-all" matching. This would mean matching every image to a comprehensive database of every person in a given polity.

Each approach can be carried out asynchronously (on demand, after images are captured) or in real time. And they can be applied to separate (disaggregated) data streams, or used to bring together massive surveillance datasets.

Facial recognition occurring at one end of each of these scales—one-to-one, asynchronous, disaggregated—has well-documented benefits. One-to-one real-time facial recognition can be convenient and relatively safe, like unlocking your phone, or proving your identity at an automated passport barrier. Asynchronous disaggregated one-to-many facial recognition can be useful for law enforcement—analyzing CCTV footage to identify a suspect, for example, or finding victims and perpetrators in child abuse videos.

However, facial recognition at the other end of these scales—one-to-many or all-to-all, real-time,

integrated—amounts to face surveillance, which has less obvious benefits. Several police forces in the UK have trialed real-time one-to-many facial recognition to seek persons of interest, with mixed results. The benefits of integrated real-time all-to-all face surveillance in China are yet to be seen.

And while the benefits of face surveillance are dubious, it risks fundamentally changing the kind of society we live in.

Face surveillance often goes wrong, but it's bad even when it works

Most facial recognition algorithms are accurate with head-on, well-lit portraits, but underperform with "faces in the wild." They are also worse at identifying black faces, and especially the faces of black women.

The errors tend to be false positives—making incorrect matches, rather than missing correct ones. If face surveillance were used to dole out cash prizes, this would be fine. But a match is almost always used to target interventions (such as arrests) that harm those identified.

More false positives for minority populations means they bear the costs of face surveillance, while any benefits are likely to accrue to majority populations. So using these systems will amplify the structural injustices of the societies that produce them.

Even when it works, face surveillance is still harmful. Knowing where people are and what they are doing enables you to predict and control their behavior.

You might believe the Australian government wouldn't use this power against us, but the very fact they have it makes us less free. Freedom isn't only about making it *unlikely* others will interfere with you. It's about making it impossible for them to do so.

Face surveillance is intrinsically wrong

Face surveillance relies on the idea that others are entitled to extract biometric data from you without your consent when you are in public.

This is false. We have a right to control our own biometric data. This is what is called an underived right, like the right to control your own body.

Of course, rights have limits. You can lose the protection of a right—someone who robs a servo may lose their right to anonymity—or the right may be overridden, if necessary, for a good enough cause.

But the great majority of us have committed no crime that would make us lose the right to control our biometric data. And the possible benefits of using face surveillance on any particular occasion must be discounted by their probability of occurring. Certain rights violations are unlikely to be overridden by hypothetical benefits.

Many prominent algorithms used for face surveillance were also developed in morally compromised ways. They used datasets containing images used without permission of the rightful owners, as well as harmful images and deeply objectionable labels.

Arguments for face surveillance don't hold up

There will of course be counterarguments, but none of them hold up.

- "You've already given up your privacy to Apple or Google—why begrudge police the same kind of information?" Just because we have sleepwalked into a surveillance society doesn't mean we should refuse to wake up.
- "Human surveillance is more biased and error-prone than algorithmic surveillance." Human surveillance is indeed morally problematic. Vast networks of CCTV cameras already compromise our civil liberties. Weaponizing them with software that enables people to be tracked across multiple sites only makes them worse.
- "We can always keep a human in the loop." False positive rates can be reduced by human oversight, but human oversight of automated systems is itself flawed and biased, and this doesn't address the other objections against face surveillance.

- "Technology is neither good nor bad in itself; it's just a tool that can be used for good or bad ends." Every tool makes some things easier and some things harder. Facial recognition makes it easier to oppress vulnerable populations and violate everyone's basic rights.

It's time for a moratorium

Face surveillance is based on morally compromised research, violates our rights, is harmful, and exacerbates structural injustice, both when it works and when it fails. Its adoption harms individuals, and makes our society as a whole more unjust, and less free.

A moratorium on its use in Australia is the least we should demand.

Provided by The Conversation