Avoiding a surveillance society: How better rules can rein in facial recognition tech

September 27 2022, by Nicholas Davis, Edward Santow and Lauren Perry

Credit: JR Korpa / Unsplash

The human face is special. It is simultaneously public and personal. Our faces reveal sensitive information about us: who we are, of course, but also our gender, emotions, health status and more.

Lawmakers in Australia, like those around the world, never anticipated our face data would be harvested on an industrial scale, then used in

everything from our smartphones to police CCTV cameras. So we shouldn't be surprised that our laws have not kept pace with the extraordinary rise of facial recognition technology.

But what kind of laws do we need? The technology can be used for both good and ill, so neither banning it nor the current free-for-all seem ideal.

However, regulatory failure has left our community vulnerable to harmful uses of facial recognition. To fill the legal gap, we propose a "model law": an outline of legislation that governments around Australia could adopt or adapt to regulate risky uses of facial recognition while allowing safe ones.

The challenge of facial recognition technologies

The use cases for facial recognition technologies seem limited only by our imagination. Many of us think nothing of using facial recognition to unlock our electronic devices. Yet the technology has also been trialed or implemented throughout Australia in a wide range of situations, including schools, airports, retail stores, clubs and gambling venues, and law enforcement.

As the use of facial recognition grows at an estimated 20% annually, so too does the risk to humans—especially in high-risk contexts like policing.

In the U.S., reliance on error-prone facial recognition tech has resulted in numerous instances of injustice, especially involving Black people. These include the wrongful arrest and detention of Robert Williams, and the wrongful exclusion of a young Black girl from a roller rink in Detroit.

Many of the world's biggest tech companies—including Meta, Amazon

and [Microsoft](#)—have reduced or discontinued their facial recognition-related services. They have cited concerns about consumer safety and a lack of effective regulation.

This is laudable, but it has also prompted a kind of "regulatory-market failure." While those companies have pulled back, other companies with fewer scruples have taken a bigger share of the facial recognition market.

Take the American company Clearview AI. It scraped billions of face images from [social media](#) and other websites without the consent of the affected individuals, then created a face-matching service that it sold to the Australian Federal Police and other law enforcement bodies around the world.

In 2021, the Australian Information & Privacy Commissioner found that both [Clearview AI](#) and [the AFP](#) had breached Australia's privacy law, but enforcement actions like this are rare.

However, Australians want better regulation of facial recognition. This has been shown in the [Australian Human Rights Commission's 2021 report](#), the [2022 CHOICE investigation](#) into the use of facial recognition technology by major retailers, and in research we at the Human Technology Institute have commissioned as part of our [model law](#).

Options for facial recognition reform

What options does Australia have? The first is to do nothing. But this would mean accepting we will be unprotected from harmful use of facial recognition technologies, and keep us on our current trajectory towards mass surveillance.

Another option would be to ban facial recognition tech altogether. Some

jurisdictions have indeed instituted moratoriums on the technology, but they contain many exceptions (for positive uses), and are at best a temporary solution.

In our view, the better reform option is a law to regulate facial recognition technologies according to how risky they are. Such a law would encourage facial recognition with clear public benefit, while protecting against harmful uses of the technology.

A risk-based law for facial recognition technology regulation

Our model law would require anyone developing or deploying facial recognition systems in Australia to conduct a rigorous impact assessment to evaluate the human rights risk.

As the risk level increases, so too would the legal requirements or restrictions. Developers would also be required to comply with a technical standard for facial recognition, aligned with international standards for AI performance and good data management.

The model law contains a general prohibition on high-risk uses of facial recognition applications. For example, a "facial analysis" application that purported to assess individuals' sexual orientation and then make decisions about them would be prohibited. (Sadly, this is not a far-fetched hypothetical.)

The model law also provides three exceptions to the prohibition on high-risk facial recognition technology:

> 1. the regulator could permit a high-risk application if it considers the application to be justified under international human rights

law

2. there would be a specific legal regime for [law enforcement](#) agencies, including a "face warrant" scheme that would provide independent oversight as with other such warrants

3. high-risk applications may be used in academic research, with appropriate oversight.

Review by the regulator and affected individuals

Any law would need to be enforced by a regulator with appropriate powers and resources. Who should this be?

The majority of the stakeholders we consulted—including business users, technology firms and civil society representatives—proposed the Office of the Australian Information Commissioner (OAIC) would be well suited to be the regulator of facial regulation. For certain, sensitive users—such as the military and certain security agencies—there may also need to be a specialized oversight regime.

The moment for reform is now

Never have we seen so many groups and individuals from across civil society, industry and government so engaged and aligned on the need for facial recognition technology reform. This is reflected in support for the model law from both the Technology Council of Australia and CHOICE.

Given the extraordinary rise of uses of facial recognition, and an emerging consensus among stakeholders, the federal attorney-general should seize this moment and lead national reform. The first priority is to introduce a federal bill—which could easily be based on the our model law. The attorney-general should also collaborates with the states and territories to harmonize Australian law on facial recognition.

This proposed reform is important on its own terms: we cannot allow facial recognition technologies to remain effectively unregulated. It would also demonstrate how Australia can use law to protect against harmful uses of new technology, while simultaneously incentivizing innovation for public benefit.

More information about the model law can be found in our report "Facial recognition technology: Towards a model law."

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

Provided by The Conversation