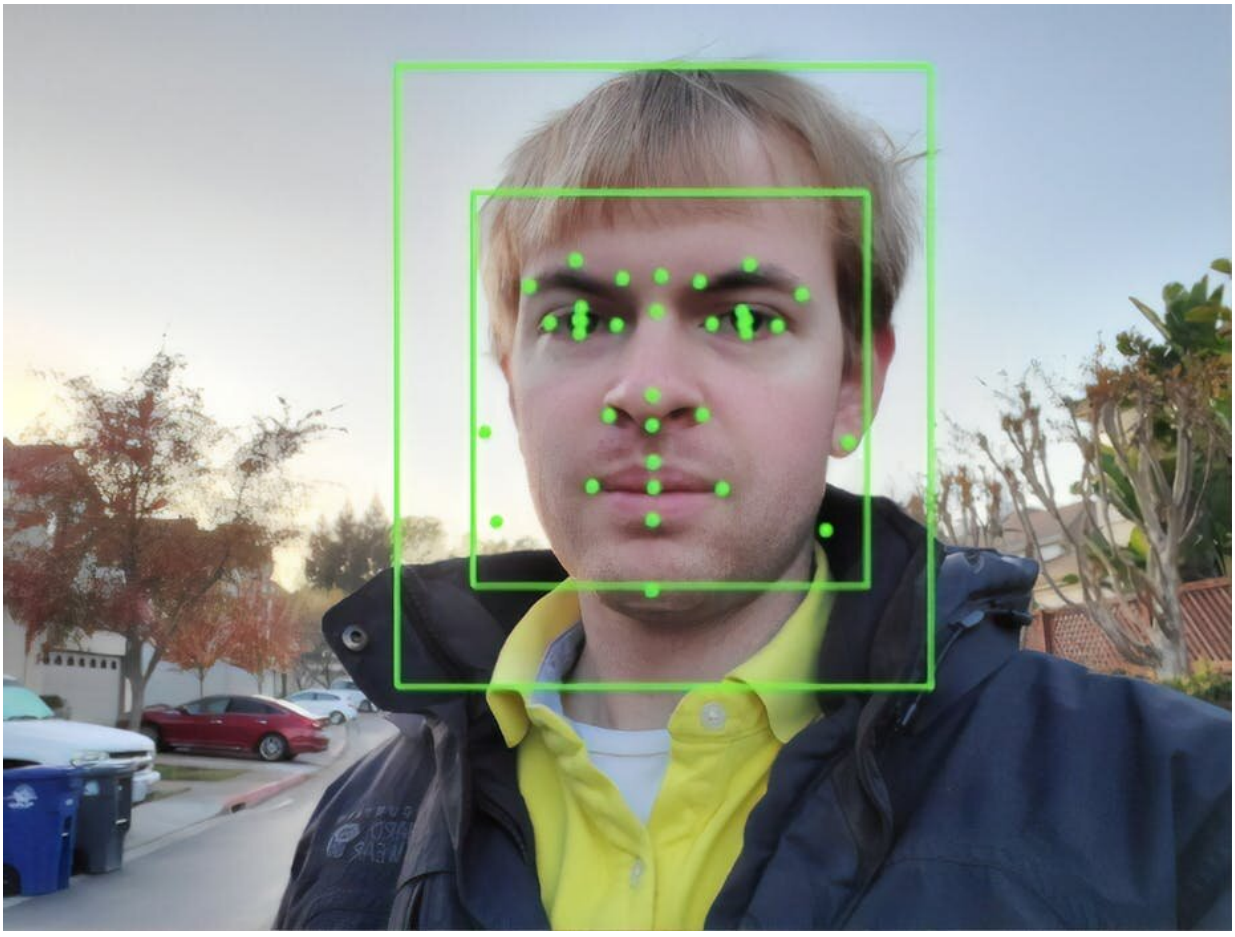
Facial recognition technology is expanding rapidly across Australia. Are our laws keeping pace?

July 10 2020, by Rick Sarre



Credit: Smith Collection/Gado/Sipa USA

Facial recognition technology is increasingly being trialed and deployed around Australia. Queensland and Western Australia are reportedly already using real-time facial recognition through CCTV cameras. 7-Eleven Australia is also deploying facial recognition technology in its 700 stores nationwide for what it says is customer feedback.

And Australian police are reportedly using a facial recognition system that allows them to identify members of the public from online photographs.

Facial recognition technology has a somewhat nefarious reputation in some police states and non-democratic countries. It has been used by the police in China to identify anti-Beijing protesters in Hong Kong and monitor members of the Uighur minority in Xinjiang.

With the spread of this technology in Australia and other democratic countries, there are important questions about the legal implications of scanning, storing and sharing facial images.

Use of technology by public entities

The use of facial recognition technology by immigration authorities (for example, in the channels at airports for people with electronic passports) and police departments is authorized by law and therefore subject to public scrutiny through parliamentary processes.

In a positive sign, the government's proposed identity matching services laws are currently being scrutinized by a parliamentary committee, which will address concerns over data sharing and the potential for people to be incorrectly identified.

Indeed, Australian Human Rights Commissioner Edward Santow recently sounded an alarm over the lack of regulation in this area.

"At the moment, there are not strong and clear enough legal protections in place to prevent the misuse of facial recognition in high stakes areas like policing or law enforcement."

Another specific concern with the legislation is that people's data could be shared between government agencies and private companies like telcos and banks.

How private operators work

Then there is the use of facial recognition technology by private companies, such as banks, telcos and even 7-Elevens.

Here, the first thing to determine is if the technology is being used on public or private land. A private landowner can do whatever it likes to protect itself, its wares and its occupants so long as it doesn't break the law (for example, by unlawful restraint or a discriminatory practice).

This would include allowing for the installation and monitoring of staff and visitors through facial recognition cameras.

By contrast, on public land, any decision to deploy such tools must go through a more transparent decision-making process (say, a council meeting) where the public has an opportunity to respond.

This isn't the case, however, for many "public" properties (such as sports fields, schools, universities, shopping centers and hospitals) that are privately owned or managed. As such, they can be privately secured through the use of guards monitoring CCTV cameras and other technologies.

Facial recognition is not the only surveillance tool available to these private operators. Others include iris and retina scanners, GIS profiling,

internet data-mining (which includes "predictive analytics," that is, building a customer database on the strength of online behaviors), and "neuromarketing" (the use of surveillance tools to capture a consumer's attributes during purchases).

There's more. Our technological wizardry also allows the private sector to store and retrieve huge amounts of customer data, including every purchase we make and the price we paid. And the major political parties have compiled extensive private databanks on the makeup of households and likely electoral preferences of their occupants.

Is it any wonder we have started to become a little alarmed by the reach of surveillance and data retention tools in our lives?

What's currently allowed under the law

The law in this area is new and struggling to keep up with the pace of change. One thing is clear: the law does not prohibit even highly intrusive levels of surveillance by the private sector on private land in the absence of illegal conduct.

The most useful way of reviewing the legal principles in this space is to pose specific questions:

Can visitors be legally photographed and scanned when entering businesses?

The answer is yes where visitors have been warned of the presence of cameras and scanners by the use of signs. Remaining on the premises denotes implied consent to the conditions of entry.

Do people have any recourse if they don't want their

image taken?

No. The law does very little to protect those who may be upset by the obvious presence of a surveillance device on a door, ceiling or wall. The best option for anybody concerned about this is to leave the premises or not enter in the first place.

What about sharing images? Can private operators do whatever they like with them?

No. The sharing of electronic data is limited by what are referred to as the "privacy principles", which govern the rights and obligations around the collection, use and sharing of personal information. These were extended to the private sector in 2001 by amendments to the Commonwealth Privacy Act 1988.

These privacy principles would certainly prohibit the sharing of images except, for example, if a store was requested by police to hand them over for investigation purposes.

Can private businesses legally store your image?

Yes, private or commercial enterprises can store images of people captured on their cameras in their own databases. A person can ask for the image to be disclosed to them (that is, to confirm it is held by the store and to see it) under the "privacy principles". Few people would bother, though, since it's unlikely they would know it even exists.

The privacy principles do, however, require the business to take reasonable steps to destroy the data or image (or ensure there is de-identification) once it is no longer needed.

What if facial recognition technology is used without warnings like signs?

If there is a demonstrable public interest in any type of covert surveillance (for example, to ensure patrons in casino gaming rooms are not cheating, or to ensure public safety in crowded walkways), and there is no evidence of, or potential for, misuse, then the law permits it.

However, it is not legal to film someone covertly unless there is a public interest in doing so.

What does the future hold?

Any change to the laws in this area is a matter for our parliamentarians. They have been slow to respond given the difficulty of determining what is required.

It will not be easy to frame legislation that strikes the right balance between respecting individuals' rights to privacy and the desires of commercial entities to keep their stock, patrons and staff secure.

In the meantime, there are steps we can all take to safeguard our privacy. If you want to protect your image completely, don't select a phone that switches on when you look at it, and don't get a passport.

And if certain businesses want to scan your face when you enter their premises, give them a wide berth, and your feedback.

Provided by The Conversation