

Why the government's proposed facial recognition database is causing such alarm

October 25, 2019 9.24am AEDT

Since before the 2019 election, the Morrison government has been keen to introduce a new scheme that would allow government agencies, telcos and banks to use facial recognition technology to collect and share images of people across the country.

While there are some benefits to such a system – making it easier to identify the victims of natural disasters, for example – it has been heavily criticised by [human rights groups](#) as an attempt to introduce mass surveillance to Australia and an egregious breach of individual privacy.

The plan hit a roadblock when the government-controlled Parliamentary Joint Committee on Intelligence and Security (PJCIS) [handed down an extensive report](#) calling for significant changes to the legislation to ensure stronger privacy protections and other safeguards against misuse.

What are the identity-matching laws?

The [identity-matching bills](#) aim to set up a national database of images captured through facial recognition technology and other pieces of information used to identify people, such as driver's licenses, passports, visa photos. This information could then be shared between government agencies, and in some cases, private organisations like telcos and banks, provided certain legal criteria are met.

The proposed database follows [an agreement](#) reached by the Commonwealth and the states and territories in 2017 to facilitate the “secure, automated and accountable” exchange of identity information to help combat identity crime and promote community safety.

Critical to this agreement was that the system include “robust privacy safeguards” to guard against misuse.

The agreement gave the federal government the green light to introduce laws to set up the identity-matching system.

Access to the service could potentially encompass a wide range of purposes. For example, a government agency could use the system to identify people

thought to be involved in identity fraud or considered threats to national security.

But the bill also includes more pedestrian uses, such as in cases of “community safety” or “road safety”.

The proposed laws contain some safeguards against misuse, including criminal sanctions when an “entrusted person” discloses information for an unauthorised purpose. In addition, access by banks or other companies and local councils can only occur with the consent of the person seeking to have their identity verified.

However, much of the detail about precisely who can access the system and what limits apply is not set out in the bills. This will be determined through government regulation or subsequent intergovernmental agreements.

Concerns about scope and safeguards

The Coalition government’s bills were first introduced in 2018, but didn’t come up for a vote. After the government reintroduced the bills in July, the PJCIS launched an inquiry and invited [public submissions](#).

[Legal bodies](#) have argued that amendments are needed to tighten the boundaries of who can access the identity-matching services and for what purposes. They note that as currently drafted, the proposed laws give too much discretionary power to government officials and actually create opportunities for identity theft.

This is particularly problematic when coupled with the potential for the rapid spread of facial recognition technology in Australian streets, parks and transport hubs.

The [Human Rights Law Centre](#) said the proposed system is “[more draconian](#)” than the one launched in the UK. Another concern is that it could be used by a wide range of agencies to confirm the identity of any Australian with government-approved documentation (such as a passport or driver’s license), regardless of whether they are suspected of a crime.

The [Australian Human Rights Commission](#) also pointed to [research](#) suggesting the software used to capture or match facial imagery could result in higher error rates for women and people from certain ethnic groups.

What’s next for the bills?

When handing down the committee's unanimous report, Andrew Hastie said the broad objectives of the identity-matching system were sound, but key changes were needed to ensure privacy protections and transparency.

While the PJCIS cannot actually stop the bills from being passed, it has a strong track record of turning its recommendations into legislative amendments.

The states and territories also have an interest in ensuring a national identity-matching scheme gets the balance right when it comes to addressing identity crime and assisting law enforcement and protecting individual privacy.

The question is whether these calls for improvements will be loud enough to put these bills back on the drawing board.

The future of the legislation will tell us something important about the strength of human rights protections in Australia, which rely heavily on parliamentary bodies like the PJCIS to help raise the alarm when it comes to rights-infringing laws.