

Plan for massive facial recognition database sparks privacy concerns

Identity fraud is justification for collecting photos from drivers' licences and passports but critics say plan too invasive

If you've had a driver's licence photo or passport photo taken in Australia in the past few years, it's likely your face will end up in a massive new national network the federal government is trying to create.

Victoria and Tasmania have already begun to [upload driver's licence details](#) to state databases that will eventually be linked to a future national one.

Legislation before federal parliament will allow government agencies and private businesses to access facial IDs held by state and territory traffic authorities, and passport photos held by the foreign affairs department.

The justification for what would be the most significant compulsory [collection of personal data since My Health Record](#) is cracking down on identity fraud.

The home affairs department estimates that the annual cost of ID fraud is \$2.2bn, and says introducing a facial component to the government's document verification service would help prevent it.

The verification service is already used by 100 government agencies and 700 businesses, carrying out more than 30m ID checks in 2017 alone.

But alongside the document verification service, a facial identification service for law enforcement would be introduced.

Almost all state and territory governments have updated their driver's licence laws in anticipation of the database after an agreement at the Council of Australian Governments in October 2017, while people getting passports sign a form that states that their photographs will be used for biometric matching purposes.

What are the concerns?

[Privacy](#) advocates say the new legislation lacks proportionality – that the benefits do not outweigh the intrusion into people's privacy.

The Australian Privacy Foundation says the proposal is highly invasive, because the system could be integrated into a number of other systems that collect facial data, including closed-circuit television.

“We are on our way to automated and real-time surveillance of public spaces,” the foundation says.



[Facebook](#)[Twitter](#)[Pinterest](#)

A notice displayed by London's Metropolitan Police in 2017. Photograph: Mark Kerrison/Alamy

The Australian Human Rights Commission says facial recognition technology “remains unreliable”.

“If inaccurate information received from the use of this technology is used by law enforcement, it could also have drastic consequences for the person concerned, including being arbitrarily detained and having fundamental features of their right to a fair trial compromised,” the human rights commissioner, Edward Santow, told the parliamentary inquiry.

The Human Rights Law Centre noted that NEC Neoface, a separate facial recognition technology used by federal agencies and some state and territory police, has not been tested for accuracy on different ethnic groups, meaning a potentially disproportionate rates of misidentification of ethnic minorities.

The home affairs department says it conducts testing and tuning of facial recognition software, and matching results will be reviewed by “trained facial recognition experts” to prevent false matches.

“In other words, decisions that serve to identify a person will never be made by technology alone,” the department says.

Trials such as the one at the Commonwealth Games, and a similar schemes in Perth and Brisbane, work on live facial recognition. The scheme proposed by the federal government would be a more manual input process.

The Department of Home Affairs argues that concerns about mass surveillance are not warranted, because it's just not feasible. They say the systems are not designed for it and there are nowhere near the resources, including personnel sufficiently trained in facial recognition, that would be needed to conduct a mass surveillance program.

The standalone system for law enforcement requires a person to manually submit a person's image and resolve against possible matches, and it creates an audit trail, the department says.



[Facebook](#)[Twitter](#)[Pinterest](#)

A woman boarding a Scandinavian Airlines flight goes through facial recognition verification system. Photograph: Jim Watson/AFP/Getty Images

While CCTV still images can be put into the system to identify someone, the department says it is “not technically possible” to livestream CCTV footage into the system.

But should it become “technically possible” under the legislation, the minister could set the rules to allow it. Kristine Klugman, the president of Civil Liberties Australia, told the committee it could happen soon.

“Indeed, it is only a matter of time before the combination of cloud services, mobile, high-definition video capture (including smartphones) and ‘big data’ analytics will make such real-time surveillance possible, cheap and enticing,” she said.

“When that happens, we can again expect to hear similar claims that our police and spy agencies ‘are only effective if they have the tools necessary to effectively enforce the law and detect and prevent threats to the Australian community’.”