

Cover Story: Australia's Dangerous Foray Into Facial Recognition

[Joseph Brookes](#) / [August 5, 2019](#)

The revived proposal for the Identity-Matching Services Bill will allow the Department of Home Affairs to begin developing a national scheme of identity and data matching, including the expanded use of facial recognition technology.

The contentious scheme would see the department operate a hub and spoke model of identity data sharing with government agencies, state and federal police, anti corruption agencies, security agencies, and in some cases private organisations.

Dubbed “The Capability” the program has attracted criticism from privacy and human rights advocates, with its expansion of facial recognition capabilities of particular concern.

In addition to privacy concerns, there is growing evidence facial recognition technologies, which often rely on opaque algorithms, are inaccurate, discriminatory, and infringe on human rights.

Widespread adoption would fundamentally harm Australian civil society, according to some experts.

Proponents, meanwhile, say facial recognition is now a prerequisite for fighting terrorism and serious crime, reducing fraud, and in the effective delivery of government services.

As the debate continues, more and more facial recognition services are being quietly rolled out in Australia.

‘Boiling A Frog’

“The widespread use of facial recognition is going to change the nature of our society,” says Professor Toby Walsh, a Fellow of the Australian Academy of Science and an Artificial Intelligence expert.

“It changes the world we’re in. It’s this idea that you can be watched anytime. Even if no one is watching you, even if you never come to any harm, that [still] changes what you do because you don’t have the privacy to question.”

Walsh says, the steady rise and enhancement of surveillance technology in Australia is akin to boiling a frog: throw it into a boiling pot and it jumps out, but gently increase the heat over time and the frog fails to realise its eventual end.

“We’re used to the idea that there are loads of CCTV cameras around. But that was before we had face recognition. Before we knew no one was looking, there were too many cameras for people to be looking at ... [CCTV] actually wasn’t invading our privacy. And now we can just upgrade those cameras with software that will be invading our privacy. It will be able to identify people in real-time. It will be able to track you in real-time.”



Toby Walsh, Scientia Professor

of Artificial Intelligence at UNSW, says the risks of facial recognition technology outweigh any benefits.

Walsh, who is a strong proponent of other emerging technologies, now believes the risks of facial recognition technology outweigh its benefits and its roll-out should be suspended.

The Department of Home Affairs has defended its federated system of identity data sharing, insisting it is “[not intended for mass surveillance](#)” and government ministers argue facial recognition services would be restricted to security agencies and not include live video feeds. In a reading of the bill on Thursday, Immigration Minister David Coleman told Parliament the legislation would also provide “robust privacy protections” over the use of personal information.

The problem is that the evidence of past government behaviour suggests the Minister is wrong, and the mooted privacy protections hold no water as the use of metadata by government agencies (see below) demonstrates.

In the bill’s supporting documents the department concedes that provisions for facial identification tools are likely to infringe on human rights, particularly the right to privacy. That infringement is reasonable, according to the department, because it is

restricted to security agencies and “necessary and proportionate” to the objective of the safety and security for all Australians.

While the new powers have been positioned primarily as a way of fighting terrorism and serious crime, certain provisions suggest a broad application of identity matching services could occur.

For example, according to the explanatory memorandum, the bill allows for the identification of individuals who are “not yet directly linked to a specific national security or law enforcement threat”. The use of the “Facial Identification Service” is warranted in such a case based on an individual’s behaviour or specific circumstances, such as “a person behaving suspiciously at a significant public gathering or major event”.

The bill will likely face further scrutiny. The Government introduced a 2018 version in the last Parliament which was referred to a Parliamentary Joint Committee on Intelligence and Security, eventually lapsing with the dissolution of the House of Representatives, but not before being heavily criticised by human rights, privacy, and civil liberty groups, concerned, among other things of potential scope creep.

Walsh says the likelihood of scope creep means the protections and restrictions afforded by legislation – only a prescribed list of law enforcement, national security and anti-corruption agencies would have access to facial identification services in the case of the Identity Matching Services Bill – ultimately mean little.

His example is the explosion of access to metadata by a wide array of government agencies. *The Saturday Paper* [revealed in November last year](#) that at least 80 government authorities, from federal and state law enforcers to departments and local councils, are using legal loopholes to lodge 350,000 requests a year for access to Australians’ telecommunications metadata, despite legislation supposedly restricting access to just 22 security agencies.

The metadata access powers have similarly been justified by the government as necessary to fight serious crime and proportionate to that objective.

“There’s absolutely no reason why [certain government agencies and local councils] should be accessing people’s metadata,” Walsh says, “That’s just government powers creeping too far.”

A similar creep is likely with facial recognition technology given the appeal of the powers to governments, according to Walsh.

Technical Difficulties

As the government presses ahead with the national scheme which would at least provide some oversight of the use of facial recognition technology, many public and private organisations in Australia are already using it.

During last year's Commonwealth Games, Queensland police used facial recognition as part of a mass surveillance program. An [ABC investigation](#) revealed police, which fought to suppress a review of the program, were not able to identify any high priority targets and faced several technical setbacks. The review noted the program was limited because the absence of state and federal legislation "reduced the database from an anticipated 46 million images to approximately eight million".

The technology is also being trialled at Australian [stadiums](#), [airports](#), [shopping centres](#), without clear notice to the public, often relying on the implied consent or terms buried in the fine print.

Around the globe, adoption has varied, as has public pushback.

At the extreme end is China. The country has deployed a mass surveillance program which among other things, [uses facial recognition to monitor ethnic minorities](#). In Hong Kong the technology has allowed [identity to be weaponised](#) during recent democracy protests, sparking fears China is expanding its surveillance outside the mainland.

In the UK, police use facial recognition technology to search for suspected criminals in public. The first major review of the London police's program, an independent analysis by the University of Sussex, found matches were only correct in a fifth of cases and the system was likely to break human rights laws. In Wales, similarly poor rates led to a judicial review of the technology.

Two US cities have banned facial recognition technologies outright, although it is still used widely by law enforcement, researchers, and the private sector. In 2017 Georgetown Law school [revealed that already 117 million US citizens](#) – more than half the population – are now included in law enforcement facial-recognition software.



“While news about facial recognition often makes headlines and the topic usually draws concern when people are asked, I don’t think the majority of the Australian public is aware of the number of contexts in which this technology is being used,” says Digital Rights Watch board member Lilly Ryan.

“This is partly because cameras aren’t always obvious, but also because it is being used for so many purposes in both the public and private sector.”

Digital Rights Watch is pushing for an [urgent review](#) of the expansion of facial recognition technologies in Australia, following reports that Victorian citizens are being required to use facial recognition software in order to access government solar rebates.

40 per cent of Solar Victoria’s attempted facial recognition identity checks failed in the first two weeks of July and citizens were not given an upfront option to use other forms of identity verification, according to [Nine newspapers](#).

Those failure rates are not uncommon, Ryan tells Which-50.

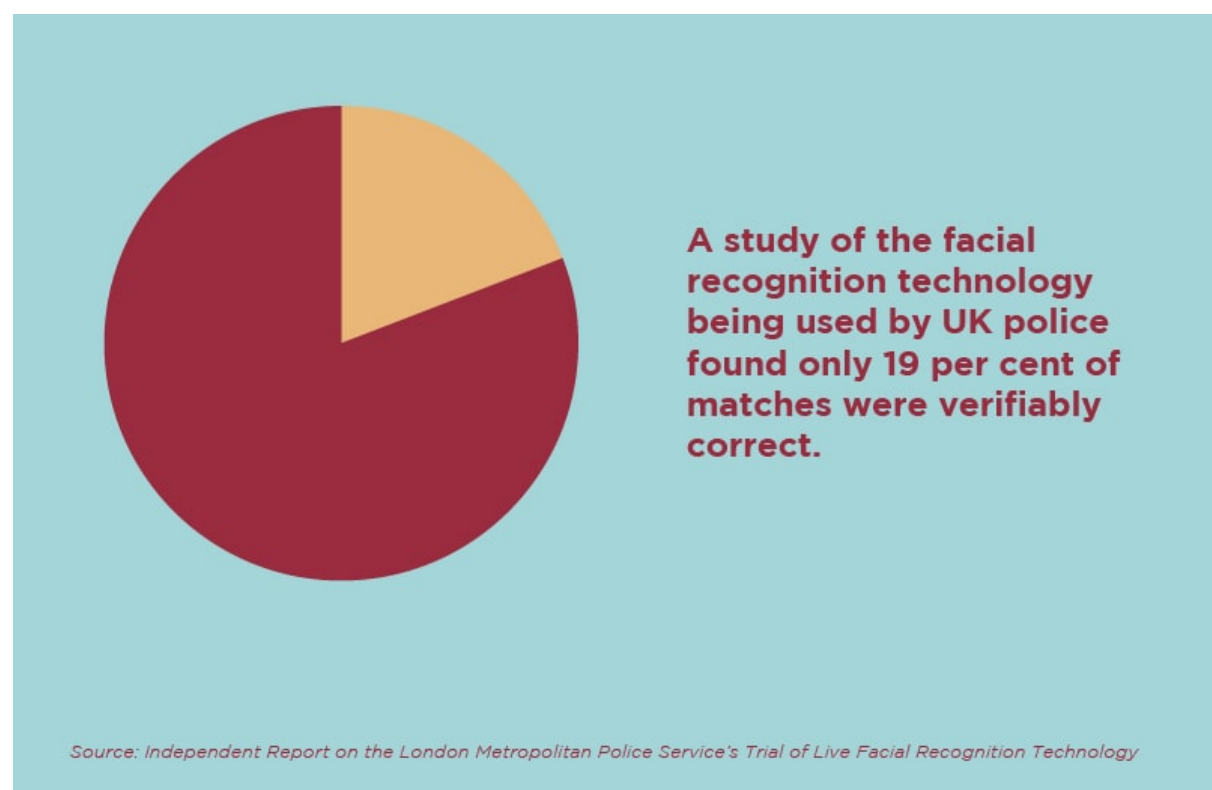
“Facial recognition technology isn’t a single product, which means that its accuracy and effectiveness varies enormously depending on who wrote the software and the conditions in which it gets used.”

Ryan says people tend to have an implicit trust of technology, often pumped up by [vendor hype](#), but facial recognition technologies remain largely inaccurate and in some cases discriminatory.

“Most facial recognition technology is proprietary, and the organisations who purchase this type of software do not usually get the opportunity to audit it for accuracy in the contexts they wish to deploy it.

“This means that the biases inherent in the datasets that were used to train the software only come out after it is being actively used, which might be too late for anyone the software developers didn’t think about at the time.”

Last year, [research from the MIT Media lab](#) revealed leading facial recognition software has potential inherent bias towards certain groups, stemming from the data facial recognition algorithms are “trained” on. According to the study, the error rates when matching faces of dark skinned females was as high as 34.7 per cent while the maximum error rate for white males in the same analysis was 0.8 per cent.



Ryan says facial recognition technologies have proved effective in some cases. Its use in airport smart gates and to unlock mobile phones, for example, works well, not only because of controlled conditions, but because users remain in control and are usually able to provide informed consent. These cases, however, are generally rare.

A Regulatory And Legal Void

Accuracy should improve over time. But an appropriate legal and regulatory framework is less certain. Australia’s current privacy laws and regulations are inadequate for the expansion of facial recognition technology, according to Dr Monique Mann, Co-chair of the Australian Privacy Foundation’s Surveillance Committee.

Mann, a QUT Vice-Chancellor's Research Fellow for Technology and Regulation, conducted a thorough analysis of developments of automated facial recognition technology and approaches to oversight, along with colleague Marcus Smith.

The 2017 research concluded, "[T]he development, implementation and application of [automated facial recognition technologies] have not been matched with increased protections or oversight ... Presently in Australia, there is a regulatory gap: an absence of an effective regulatory regime or framework to govern the use of biometric and police technologies."

In terms of technology that research was almost outdated by the time it was published, Mann tells Which-50. But while the technology has moved quickly the regulatory response has not.

"What we do in that paper is that we overview the kind of regulatory structures in other jurisdictions. In this case, we looked at the US, the UK, Germany, compared kind of what the systems of regulation work with respect to the Australian context."

Foreign jurisdictions had moved quickly on regulating facial recognition technology, compared to Australia, establishing biometrics commissioners in some cases, Mann said.



Dr Monique Mann, QUT Vice-Chancellor's Research Fellow for Technology and Regulation.

"Within the Australian context, we don't even have these kind of protections at all. And there's no really specific biometric oversight at all."

Mann argues the risk is especially high in Australia because it lacks an enforceable charter of human rights or bill of rights. In terms of a right to privacy some protections exist at a state level, but federal laws rely largely on the Privacy Act, which, while recognising biometric data as sensitive information, has several exemptions for government and security agencies.

Mann says the silver lining of the government's proposed Identity-Matching Services Bill, is it would at least bring more oversight and a legal framework to how some of the technology is already being.

"While I'm not advocating for facial recognition, in some respects [the Identity-Matching Services Bill] is actually a positive development in some ways because it actually brings what they're already doing within the legislative purview."

But even if a robust legal and regulatory framework could be put in place, the nature of the technology means privacy could never be completely guaranteed, Mann says.

"From an individual privacy perspective, of course, facial recognition is highly privacy-invasive. It connects individuals' presence and physical space, to all of this information that's possibly out there about them. Whether that's online, in government data sets, in private corporation data sets.

"So I don't think it's really possible to, [when] using facial recognition technology, reduce those risks to privacy because it's inherent [in the technology]. So maybe it shouldn't happen at all."

If use of the technology is to happen, Mann says, individuals must be informed, able to provide consent and have avenues to remove their biometric data from data sets.

Services Potential

Paul Shetler, the former head of the government's Digital Transformation Office, argues the concerns about government creep with facial recognition technology are legitimate but often overshadow a much more sophisticated private sector.

Shetler, who sees facial recognition as a viable way to remove friction in the delivery of some government services, says when it comes to the use of data, including biometric, more scrutiny should be placed on private organisations, who will likely be providing governments with the technology and data sets needed for facial recognition.

"Government simply doesn't have most of the data that people think it does. And government certainly doesn't share it internally," Shetler says.



Paul Shetler, former CEO of

the Digital Transformation Office.

“So there’s a general basic problem there: the information about people that people should be most concerned about, actually is held by private companies. And they’re the ones with the least scruples about using it.”

In that regard at least, government is better placed to be overseeing facial recognition technology and biometric data use, according to Shetler.

“Government is, at least nominally, subject to political control, [and] at least nominally, to democratic control. There is a constitution, which limits what government can do ... There are limits to what the government can legally do with data.

“Whereas in the private sector, there’s very few [limits] and people are more than happy to give away their own data.”

Government services could be considerably improved with the use of facial recognition technology, Shetler says, reducing friction and fraud. Critically though, the public must have confidence in the technology, a requirement currently being undermined by other

digital projects, Shetler says, most notably the contentious “robodebt” scheme which has error rates [as high as 17 per cent](#).

“That was outrageous, you don’t do that. When you have a government service, you don’t have those kinds of crazy error rates,” Shetler tells Which-50.

“Something like that should never be allowed to be rolled out to the public with an error rate like that. For many reasons; it undermines faith in governments, but it’s [also] an incredible inconvenience and imposition on the users.”

According to Shetler, if governments take a similarly poor standard with already “fraught” facial recognition technology in services “it won’t be forgotten” by Australian citizens.

“My argument is that, in theory, it’s a good thing, to have these kinds of [facial recognition] services. But just because a good thing in theory, doesn’t mean it’s a good thing in practice.

“If [governments] don’t actually know how to do this properly, or if they’re not actually capable of rolling things out so they don’t break and misidentified people, well, then don’t do it.”