

Data

# Face recognition, function creep and democracy

**Marie Johnson**

 Contributor  
 9 June 2020  


IBM recently announced that [it would no longer offer](#) develop or research facial recognition technology. This is big news and I believe a good decision and here's why.

[According to Arvind Krishna](#), the chief executive officer of IBM worldwide:

"We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies."

"Artificial Intelligence is a powerful tool that can help law enforcement keep citizens safe. But vendors and users of AI systems have a shared responsibility to ensure that AI is tested for bias, particularly when used in law enforcement, and that such bias testing is audited and reported," Mr Krishna wrote.



Big call: Mounting costs and an uncertain future on identity challenges

As Chief Technology Architect of the Access Card program in 2006/2007, we did extensive work on facial recognition biometrics, authentication technologies and processes – including with National Institute of Standards and Technology (NIST). This included policies, use cases, what-if scenarios, concept of operations, security, privacy and impact on civil society including disadvantaged groups.

A hacked biometric identity was then a significant and unquantifiable risk.

The lessons from the Access Card project was that it anticipated and cast a long shadow over many of these same issues. Biometrics and facial recognition has been used for some time at the borders and increasingly in law enforcement – but now reaching into domestic service delivery should be closely examined by civil society.

I recently [wrote about lessons](#) from Access Card, for the COVIDSafe app activity. I have also written about why the MHR is a flawed model, also drawing on the lessons from Access Card.

Of note over the past 18 months or so, there has been a series of damning ANAO [cyber](#), [privacy](#) and [performance](#) audit reports on national health, biometrics and identity projects. Perhaps seen as separate ANAO reports of individual projects.

In reality, a damning indictment of connected national identity and biometrics projects.

And against this deeply troubling background, there is an ever-increasing over-reach in the application of biometrics and facial recognition in a range of government 'identity' projects, without any apparent ethics governance or consultation with civil society.

Services Australia [recently announced](#) that Australia's national facial biometrics matching database was used following this summer's bushfires, to verify the identities of people who had their documents destroyed.

Services Australia [is "now looking](#) at how the technology might be applied in the future...".

This is a stated intention of function-creep without any apparent strategy or governance.

This "natural disaster" use case is straight out of the Access Card play book – with one major exception – Access Card legislation to specifically limit function creep. Access Card was terminated largely on the grounds of function creep risk.

The DTA meanwhile have been working on myGovID, including a future facial recognition component allowing citizens to access "more confidential" services that require a "proof-of-life" test. We have proof of birth, proof of death – and now proof-of-liveness.

The problem with this "proof-of-life" concept, is the variability of results (I would say discrimination) in relation to people with disability, people who are infirmed, and people with darker skin colour. In any case, the reasons why "proof-of-life" might be needed is highly contentious – and the assumption needs to be tested by engagement with civil society especially in the context of government service delivery.

Strangely [according to the DTA](#), "extending the use of digital identity ... is expected to increase the overall costs of delivering the digital identity program", so the DTA is now looking at how it might fund the roll-out across Australia.

"Non-Commonwealth use of the Digital Identity platform will need to be funded through a charging arrangement," the DTA brief states.

While the funding model is not known, the costs are mounting. *InnovationAus* reported GovPass as [costing \\$204.3 million](#) and likely to receive significant further funding in the October Budget.

So the business case is not sorted – and of greater concern, neither is the business model, the funding model, nor the governance and nor the concept of operations – upon which a business case would rest.

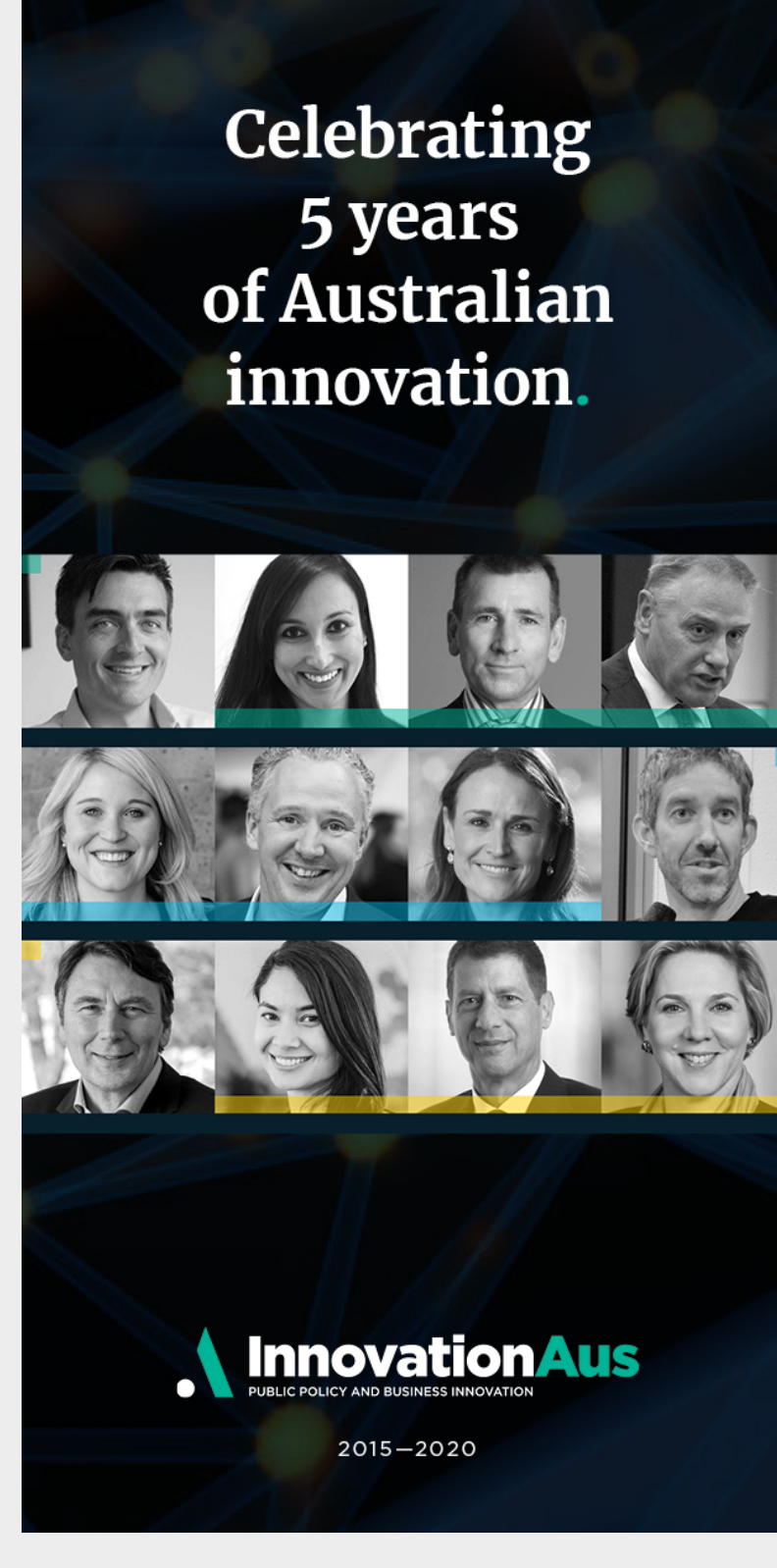
And yet, DTA is looking at the potential to incorporate \*more\* biometrics in the GovPass scheme, including voice and face data.

So, we have multiple fragmented identity activities; with no business case/s; no concept of operations; promoting Facebook-inspired platform models (which have proven to be anti-democratic); and rushing in the application of contentious and dangerous technologies to be deployed in the "service" of Australian citizens.


*Marie Johnson was the Chief Technology Architect of the Health and Human Services Access Card program, at Immigration headed up the Visa Pricing Transformation and Digital Client Services; formerly Microsoft World Wide Executive Director Public Services and eGovernment; and former Head of the NDIS Technology Authority. For many years, Marie was an Independent Member of the Australian Federal Police Spectrum Program Board. Marie is an inaugural member of the ANU Cyber Institute Advisory Board.*

Do you know more? Contact James Riley via [Email](#) or [Signal](#).

Related: [Digital Transformation Agency](#) | [DTA](#) | [Facial Recognition](#) | [GivPass](#)


[← Previous post](#)
[Next post →](#)
[Private capital wants a 'visionary plan'](#)
[Gilmour inks new rocket research deal](#)

### 3 COMMENTS


**David C**  
 2 months ago 

We have to stop perpetuating these myths around Verification vs Identification – it is holding back innovation and actually increasing the opportunities for preventing identity fraud!

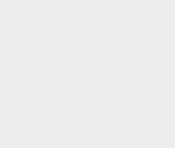
Identification is the issue that the IBM article references and is the source of great media hype around privacy. Verification, especially the approach put forward by the DTA and being used by Services Australia is about a person being able to prove their identity to a high level by using their existing credential – their passport for example. It is not creating a "digital identity" – it is creating a digital credential that can be used to assert their identity. No bias, no big risk of databases being hacked – just verifying their identity to a higher level than currently possible.

It is literally the equivalent of crossing the border by using SmartGate by presenting your passport and getting your photo taken and compared to the image in the passport. No-one seems to have any issues with that system....


Please – read what is being done by the DTA around use of the Facial Verification System – and take the tinfoil hats off. It is not surveillance, it is not invading people's privacy. It. Is. Verification.

This system will significantly reduce the opportunity for identity fraud – it is perfect? No, of course not. But it is almost infinitely better than doing nothing.

Steps off soapbox.....


**Louis Leahy**  
 2 months ago 

You don't appear to understand the issue is that NO personal information bio metrics or otherwise should be used for identification because it exposes users to identity theft and breaches of privacy. Bio metrics is particularly bad because anyone can access such inputs, they are in no way secure and it is trivial to spoof them.


**Louis Leahy**  
 2 months ago 

One of the biggest failings of biometrics is they need to be recalibrated but aside from that it is clear biometrics are not the answer for authentication because they run counter to the overriding requirement for privacy.

We have designed the algorithms required for secure private authentication they have been available for more than 10 years but rather than embrace our technological break through successive Governments in this country have instead attacked us to prevent our solution being made available for the benefit of the community.

It is a national disgrace and requires a royal commission to examine the short comings of the public sector management and their willingness to continually breach competition law with impunity.

Your email address will not be published.


Save my name, email, and website in this browser for the next time I comment.



### Related stories


**Govt urged to ditch COVIDSafe for GApple**  
 23 June 2020 | by Denham Sadler


**Renwick review won't reject encryption laws**  
 18 March 2020 | by Denham Sadler


**NSW plants \$1.6b in digital-led recovery**  
 18 June 2020 | by James Riley


**How stupid are we? Ask the government**  
 19 May 2020 | by Ed Husic