Review of the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019

Submission prepared by Fergus Hanson

Below are brief comments on the Identity-Matching Services Bill 2019. They are in addition to my submission of July 2018 to the earlier review.

As outlined in my July 2018 submission, restrictions around use of the Face Identification Service (FIS) and protections against its misuse need to be significantly strengthened. In an era of heightened strategic competition, where authoritarian states are making increased use of surveillance technologies to suppress their own people and commit mass human rights abuses, Australia should take a pointedly different approach to its use of surveillance technologies, of which the FIS will be a foundational component. As the Prime Minister said on 7 June 2019 in Vietnam:

> I said in Jakarta in my first overseas trip as Prime Minister that, set against rapid social and economic changes, our region is experiencing sharpening strategic competition.
>
> In an era of rapid change and uncertainty, we must know who we are, what we offer and what we're about.
>
> ….I've said before that our foreign policy must not be simply transactional. It's about our character and values. Who we are in the world, and what we believe in.
>
> We believe in the rule of law;..."[1]

Low crime rates, the fact many major crime types (like domestic violence) occur away from public spaces, and high levels of societal stability mean reasonable use cases for the FIS are very limited in Australia. However, creating a national surveillance network will impinge on all Australians' liberties. Most directly it will mean innocent Australians are incorrectly identified as suspected criminals, but more subtly it will likely drive a gradual transformation of core societal norms and values: away from doing the right thing because it is right, towards a mentality of doing the right thing because you are under surveillance. There is also the very high likelihood that use of the FIS capability will gradually be extended to increasingly trivial offences (and the current draft Bill permits the FIS's use for trivial offences in most circumstances).

Once created, the use cases and evolution of the technology will inevitably lead to the expansion of the surveillance network. Beyond broad statements on the potential value of FIS-enable capabilities, an intellectually rigorous case is yet to be made to the public, preventing the required level of informed public policy discourse. In the current very low domestic threat environment and absent a credible use case, it is worth considering whether the FIS is necessary given the deleterious effect it will have on all Australians' liberties and the very marginal benefits.

[1] https://www.pm.gov.au/media/speech-singapore

If the FIS is to be used, to ensure our domestic and international values align, Australia needs to sharply distinguish its use of surveillance technologies from those of authoritarian states. Most notably this means very clearly setting out limits for the use of these technologies and creating protections for citizens that err on the side of constraining use of the tools, providing ample protections for citizens and boosting transparency around the use of the tools. The current draft Bill does not achieve this balance. Simple utility of a FIS is not enough to justify its establishment in the absence of a framework that actively balances civil liberties with the security attributes of this technology.

As outlined in my earlier submission, authorised uses should be much more tightly focussed than the current draft legislation would permit. Protections for citizens should also be sharply improved. For example, although the FIS is being established as a 'one-to-many image based identification service', the Bill does not seem to prevent it being subsequently adapted to allow many-to-many, or many-to-one checking, or its use as a de facto many-to-many service (for example, by checking multiple images one by one). The Bill should set limits on potential future changes to the FIS, particularly, many-to-many checking and many-to-one checking that would further impinge on privacy rights, and note what restrictions apply in each jurisdiction (Commonwealth-Commonwealth, Commonwealth-state, inter-state and intra-state). Lifting thresholds for all use cases listed in Section 6 and in all jurisdictions (Commonwealth-Commonwealth, Commonwealth-state, inter-state and intra-state) would also help prevent overreach.

The Face Verification Service (FVS) is less problematic than the FIS, but still has the potential to be seriously misused under the current draft legislation. As outlined in my July submission, in the case of the FVS, the dominant use for this service is likely to be biometric digital identity verification through the GovPass program and Australia Post's Digital iD. Currently, there is no dedicated legislation, beyond existing laws like the very inadequate Privacy Act, governing these schemes and none is currently proposed. Given this gap, consideration should be given to providing basic protections against misuse of the FVS in the draft Bill.

In particular, two key protections are needed. First, trade in personal attributes enabled by digital identity should be explicitly curtailed. At present Australia's digital identity could be used to facilitate attribute exchanges. This would see digital identity used to confirm a person's identity with a high degree of confidence with the subsequent activities of that consumer collected and sold via attribute exchanges that trade attributes that are, thanks to digital identity, now linked to the same individual. Companies are already exploring the Australian market as a test case for this type of scheme, because of its lax regulatory environment. This type of democratic social credit scheme would likely entrench social and economic disadvantage. Second, the law should expressly require the minimum necessary exchange of personal information during digital identity checks. This would help improve privacy.