ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE
LEVEL 2, 40 MACQUARIE STREET, BARTON ACT 2600

ASPI – International Cyber Policy Centre (ICPC)
Submission to the Parliamentary Joint Committee on Intelligence and Security

Fergus Hanson, Head, International Cyber Policy Centre

July 2018

Below are brief comments on the Identity-matching Services Bill 2018. They were informed by research for a forthcoming policy brief for the International Cyber Policy Centre at ASPI on digital identity. ASPI takes no corporate positions on any policy matters, as such this submission reflects my personal views.

- In the case of intra-state uses of the Face Identification Service (FIS), the Bill is silent, even though states are likely to be the dominant users of the service because they are responsible for most law enforcement activity (i.e. states requesting matches of suspects who reside within their own jurisdiction). There are currently no minimum thresholds for intra-state uses of the FIS provided the use is permitted by state or territory law (i.e. the FIS could be used for general law enforcement purposes regardless of whether an activity carries any prison time and could be used to target petty offences). There is a question whether the Commonwealth, as the operator of the hub that will allow the FIS to function, should be permitting states and territories to use the FIS to identify individuals without any minimum threshold offence suspected of being committed (such as the offence carrying at least a three-year prison sentence for law enforcement usage)[1]. It may be argued states and territories would just build their own systems using their state drivers licence databases if strong thresholds were imposed for use of the FIS and that liberal state and territory usage was foreshadowed in Section 4.22 of the Intergovernmental Agreement on Identity Matching Services. However, setting a minimum threshold would help establish a normative national standard below which use of biometrics is unacceptable. If a state or territory did legislate to allow for the use of the FIS for petty offences it is unclear why the Commonwealth should enable this.

  In the case of the Face Verification Service (FVS), the dominant use for this service is likely to be biometric digital identity verification through the proposed GovPass program and Australia Post's already operational Digital iD. Currently, there is no dedicated legislation, beyond existing laws like the Privacy Act, to govern these far-reaching schemes and none is currently proposed. Given this gap, consideration should be given to providing basic protections against misuse of the FVS (e.g. for example, by prohibiting China-style social credit schemes that link verified identities with an individual's activities such as purchases, location etc that can then be on-sold).

- The permitted uses and any restrictions for each jurisdiction's use of the FIS should be explicitly set out (i.e. intra-Commonwealth requests, Commonwealth-state requests and vice versa, inter-state requests and intra-state requests).

- Ideally, the three-year imprisonment rule should apply to all law enforcement requests using the FIS, including intra-state requests, and substantive thresholds should be applied to other uses listed under Section 6.

[1] Beyond a state or territory law authorising its use.

- For some inter-state requests, use of the FIS appears to be permitted if a crime carries less than a three-year minimum sentence in one state, while carrying a sentence of three-years or more in the other state. The minimum threshold should be set at three years in both states. This should be set out in the legislation.

- Although the FIS is being established as a 'one-to-many image based identification service'[2], 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 factor 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.

- In the case of the FVS, development of social credit style schemes by either the private or public sector should be expressly prohibited. For private sector relying parties permitted to access digital verification services that make use of the FVS, there should be tight controls around using the identity matching service to then link data related to the customer/individual (e.g. if an individual proves their identity when buying alcohol, gathering the time, location, purchase history etc associated with that transaction and then linking it to that identity should be expressly prohibited to prevent the rise of third party 'attribute vendors' and social credit schemes).

- The bill should mandate a principle that for all identity checks the minimum amount of personal information necessary should be exchanged.

- Tighter drafting should be employed throughout to narrowly define uses, e.g. Section 6 (3) 'preventing' crime and Section 6 (7) on 'promoting road safety'.

- More broadly, to balance increasing encroachments on personal privacy and rights, there is a need to overhaul citizen and consumer rights when it comes to controlling, accessing, managing and contesting use of personal information. Reforms should provide citizens with easy and meaningful control over their data. This should include providing citizens with an online log every time their personal information is accessed by any arm of government, and providing them with an easy process for contesting any access they believe may be unauthorised. It should allow citizens to decide who can access different components of their data (like individual records) and provide strong default settings to protect those who do not bother to adjust their personal settings. The government should consider a root and branch review to ensure citizen protections, such as privacy, are fit for purpose in a digitised world. This should include ensuring minimum security baselines are maintained and rules for data use regardless of who has custody of the information (government or private sector). The shift to digitalising government services also presents an opportunity to simplify unnecessarily complex laws and processes developed for the paper-based world.

[2] https://www.homeaffairs.gov.au/crime/Documents/face-matching-services-fact-sheet.pdf