Submission by the

Office of the Information Commissioner

Legal Affairs and Community Safety Committee

POLICE AND OTHER LEGISLATION (IDENTITY AND BIOMETRIC CAPABILITY) AMENDMENT BILL 2018

February 2018

The Queensland Office of the Information Commissioner (OIC) is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government.

The statutory functions of the Information Commissioner under *the Information Privacy Act 2009* (Qld) (**IP Act**) include commenting on issues relating to the administration of privacy in the Queensland public sector environment.

The OIC acknowledges the compressed time frame associated with the Committee's consideration of the Police and Other Legislation (Identity and Biometric Capability) Amendment Bill 2018 (the Queensland bill) and appreciates the opportunity to comment on the draft legislation.

The OIC supports, in-principle, the objects of the Queensland bill and the nation-wide Identity Matching Services (IMS) regime it will help facilitate. However, while the overall benefits of the system should be embraced, enthusiasm for the specific capabilities of the regime must be complemented by a measured approach to mitigating some inherent risks. Essentially, the expansion of the powers enabled by the IMS regime need to be matched by adequate oversight mechanisms and limits on potential expansion of those powers.

It is also imperative to note that the final content and timing of the Commonwealth's Identity-matching Services Bill 2018 (the Commonwealth bill) are unknown. Similarly, the content and timing of other jurisdictions' enabling legislation is unknown. This uncertainty complicates consideration of the measures needed in the Queensland legislation to mitigate risk. However, there is capacity within the Queensland bill to entrench some protections and safeguards on the use of Queensland-held data.

The OIC's comments on the Queensland bill are limited to the IMS components of the bill and no assessment is made of the liquor trading arrangements or Criminal Code explosive offences elements of the bill.

This submission will cover –

- OVERVIEW – a brief summary of the nation-wide IMS regime within which the Queensland bill is designed to operate
- RISKS – an overview of the inherent risks in the regime and factors that exacerbate those risks for Queensland, and
- RECOMMENDATIONS – options for mitigating those risks.

OVERVIEW OF IDENTITY MATCHING SERVICES REGIME

In October 2017, Australian jurisdictions entered into an Intergovernmental Agreement (IGA) to share and match identity information through specific identity matching services, including the Document Verification System, the Identity Data Sharing System and Face Matching Services.

In simple terms, the Document Verification System (DVS), which has been operational since 2009, enables agencies to confirm that the content of a document matches the records held by the issuing agency; the Identity Data Sharing Service (IDSS) enables sharing of non-biometric data; and three of the four Face Matching Services will provide relatively low risk, valuable services to verify an individual's identity (the Facial Verification System, also known as the one-to-one system, One Person One Licence Service, and the Facial Recognition Analysis Utility Service).

However, the Face Matching Services also include the Face Identification Service (FIS), sometimes referred to as the 'one-to-many' system. The FIS is the element of the IMS regime which, in the absence of adequate oversight and restrictions, is the greatest cause for concern and poses the greatest risks in terms of privacy, misuse and mistake. The FIS will allow an image of an unknown individual to be compared against images held in numerous databases to attempt to establish an individual's identity. The FIS programming is designed to identify individuals with a 65% match to the initial image. At present, these databases include driver licences, passports and immigration documents, but data sources are likely to expand.

The IGA was designed to be underpinned by Commonwealth and State enabling legislation, Participation Agreements, Access Policies, Privacy Impact Assessments and training regimes. Progress has been made on these instruments, but many are incomplete and some have not yet commenced.

The Commonwealth bill was tabled in the Australian Parliament on 7 February 2018, however the timetable for its progress is unclear. There are shortcomings in the Commonwealth bill which mean the adequacy of the Queensland bill is critical. Specific shortcomings in the Commonwealth bill are addressed later in this submission.

RISKS

The nature of risk associated with IMS is broad-ranging, from the science fiction-esque surveillance currently used in China to identify ethnic minorities, journalists and people using too much toilet paper[1], to a warrant being executed against an innocent person who met the 65% match threshold for the FIS, or a person who has attended an issue-motivated event, such as a protest, being identified in a crowd and refused entry to an event.

While acknowledging the scale and complexity of work involved in designing and implementing a national IMS regime, and the considerable efforts of officers involved to consult effectively with stakeholders, a number of systemic factors and procedural shortcomings in the IMS regime exacerbate the risks inherent in face matching at this point in time. These include –

- Uncertainty – Uncertainty about the final content and timing of the Commonwealth bill and other jurisdictions' legislation means the Queensland bill is being progressed in the absence of full knowledge of the legislative landscape in which it will operate.
- Incomplete information – The instruments intended to underpin and support the IGA, and to deliver on the IMS (the legislation, Participation Agreements, Access Policies, Privacy Impact Assessments and training regimes), are not yet finalised. This creates uncertainty about the operational parameters of the regime. Of particular concern with respect to privacy considerations is that the Privacy Impact Assessments have not yet been completed for police and law enforcement use, transport use, and private sector use. Therefore this Queensland bill is designed to facilitate the outcome without the benefit of a focussed consideration of privacy implications.
- Errors – The programming threshold for an FIS output of a 'match' is 65%. The Washington Post has reported that, in 85% of cases, FBI use of face matching technology against a group of 50 candidates would return one match and 49 false positives, but in 15% of cases, the system flags all 50 candidates as false positives[2]. While the Explanatory Notes for the Queensland bill stipulate that outputs from the identity matching services will not be used for evidentiary purposes, this is not entrenched in the legislation. The statement in the Explanatory Notes reflects only that, to date, such identity matching has not been used for evidentiary purposes. However its use in this way is likely, if not inevitable, especially as

[1] https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.c0b4130bc2eb
[2] https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.c0b4130bc2eb

technology improves. This assumption in the Explanatory Notes also fails to recognise that IMS outputs will inevitably be used for gaining/executing search warrants and making arrests. Monitoring and reporting on erroneous use of IMS outputs is not canvassed in either the Commonwealth or Queensland bills.

- Specific elements of the Commonwealth bill, as currently drafted, create gaps and pose potential risks. For example, the Commonwealth bill –
    - does not explicitly protect against or prohibit the expansion of IMS to many-to-many, blanket surveillance techniques
    - entrenches the potential for scope creep by enabling the federal Minister for Home Affairs to make rules prescribing matters 'necessary or convenient', including specific powers to include a new identity-matching service and to expand the definition of identity information without adequate Parliamentary oversight or consideration
    - uses broad, inclusive definitions that are vulnerable to broad interpretation, such as 'reasonably believed', 'significant risk', 'harm', and 'promoting' community and road safety
    - excludes non-government users of the Facial Verification Service from being identified in the annual report on use of IMS
    - fails to provide an adequate legislative review mechanism, with the only requirement being that a review must commence within five years of commencement, and with no instruction about the scope and content of that review, and
    - is silent on the nature of offences for which the Facial Identification Service (the one-to-many system) can be used. Although the IGA provides that the FIS only be used for offences carrying a maximum penalty of not less than three years imprisonment, it relies on officers using the system on a day to day basis being trained on, and complying with, these terms of the IGA.

The haste with which the Commonwealth and Queensland bills are being progressed, in order to operationalise the IMS prior to the Gold Coast Commonwealth Games, exacerbates the risks inherent in this regime.

In Queensland, media reports[3] have already indicated that the Queensland Police Service (QPS) intends to utilise a hybrid system from the Australian Criminal Intelligence Commission at the Commonwealth Games that could put issue-motivated people on watch lists. A QPS spokesperson is quoted as saying 'it's not all about counter terrorism'. Arguably, such a use of the IMS is a broad interpretation of the intended purposes of the regime. It is also important to note that the Australian Criminal Intelligence Commission is exempt from the *Privacy Act 1988 (Cth)* and therefore not subject to oversight by the Office of the Australian Information Commissioner. Little information is available about the recent use of similar systems in Wales and at the Sydney Cricket Ground. Sensible public policy practice would dictate that Queensland's adoption of a similar system should be informed by lessons from such use, especially with regard to errors.

Overall, the increase in powers facilitated by the IMS regime is not matched with a comparable increase in oversight of the regime, nor restrictions on potential expansions of the regime.

RECOMMENDATIONS

There is scope within the Queensland bill to mitigate some of these risks.

Options include –

1. Ensuring a **legislative review** of the Queensland bill is undertaken within one year of commencement, and stipulating that such a review should: assess the frequency, purpose and type of matching services used and by whom; error rates; and incidence of service expansion.
2. Including in the Queensland bill **express limitations** on the use of Queensland-held data, for example –
    i. that Queensland-held data not be used in any expansion of the IMS that involves many-to-many surveillance other than to prevent imminent harm or risk. Once a comprehensive Privacy Impact Assessment is conducted and the risks of bias, discrimination and predictive profiling are understood and mitigated, this issue can be reviewed.
    ii. that Queensland-held data not be provided to any jurisdiction that does not have a Participation Agreement, Access Policy and comprehensive training regime to ensure privacy and data security arrangements equivalent to Queensland's.

[3] The Sunday Mail, Sunday 11 February 2018, 'Policing gets in your face', p21

iii. that Queensland-held data not be accessible by the private sector through the FVS until a Privacy Impact Assessment is undertaken on private sector use and adequate reporting mechanisms on private sector access are in place.

3. Ensuring that a 'match' output from the IMS must not be used for evidentiary purposes, and that data on the use of IMS 'match' outputs for warrants, arrests and other uses be collected and reported, to an oversight body, for example the Public Interest Monitor.
4. Ensuring that the **offence provision** currently in Clause 21 of the Commonwealth bill is replicated in the Queensland bill, so that if the passage of the Commonwealth bill is delayed or the bill is modified, the offence provisions are entrenched in Queensland law.
5. Ensuring that the **threshold for using the FIS** for law enforcement purposes agreed in the IGA is embedded in the Queensland bill, i.e. that the FIS can only be used for law enforcement purposes in relation to an offence carrying a maximum penalty of not less than three years imprisonment.

Queensland safeguards are essential to ensure the integrity of Queensland-held identity information and systems, and to protect privacy rights that are vulnerable to erosion and intrusion from system expansion, misuse and mistakes.

OIC is available to provide further information or assistance to the Committee as required.