Submission by the

Office of the Information Commissioner

Parliamentary Joint Committee on Intelligence and Security

IDENTITY-MATCHING SERVICES BILL 2018

March 2018

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

The statutory functions of the Queensland 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 Queensland OIC would like to acknowledge both the considerable efforts of officers involved in consultations to date, and the scale and complexity of work involved in designing and implementing a national Identity Matching Services (IMS) regime. The Queensland OIC supports, in-principle, the objects of the Identity-matching Services Bill 2018 (the IMS bill) and the nation-wide regime it will help facilitate.

However, the Queensland OIC calls for a cautious approach that clearly entrenches into law the principles and protections agreed to in the Intergovernmental Agreement on Identity Matching Services (the IGA), including –

(i) the intended uses of the IMS, and
(ii) strong oversight and reporting mechanisms.

These key objectives were the basis of the Queensland OIC's recent submission to the Queensland Parliament's Legal Affairs and Community Safety Committee about the Police and Other Legislation (Identity and Biometric Capability) Amendment Bill 2018 (the Queensland bill). This bill was introduced into the Queensland Parliament on 15 February 2018, was passed on 7 March 2018 and was assented to on 16 March 2018.

As the Parliamentary Joint Committee on Intelligence and Security may be aware, Queensland is the first jurisdiction to pass legislation facilitating the IGA. Given the compressed timeframe for the passage of the Queensland bill for the Commonwealth Games, there was limited opportunity for robust and informed public debate and scrutiny of the Queensland bill. The Queensland OIC therefore welcomes the opportunity to make this submission to the Commonwealth Parliamentary Joint Committee on Intelligence and Security on the IMS bill.

The Queensland OIC also notes the concerns raised by the Senate Standing Committee for the Scrutiny of Bills in Digest 2 of 2018 with respect to privacy considerations and entrenching into legislation key protections to which Governments have agreed in the IGA and other instruments.

(i) The Identity-matching Services Bill 2018 should clearly and explicitly entrench in law the intended uses of the Identity Matching Services regime.

As currently drafted, the IMS bill does not adequately embed into law the core intents of the regime to which Governments have agreed. Some of the key measures in instruments that support the regime should be entrenched in law. These instruments that underpin the IMS regime – the IGA, Participation Agreements, Access Policies, the Training Policy, the Compliance Policy, the Charging Policy and Privacy Impact Assessments – run to hundreds of pages, and it may not be realistic to assume that all individual users of IMS will be familiar with the details of these documents. Elevating core intentions, principles and protections into law will help clarify the parameters of the regime, minimise risk of scope creep, and minimise risk of disproportionate privacy incursions.

Further, while progress has been made on most of these supporting instruments, many are incomplete and their content and structure may still be subject to change. This fuels, but is not the sole source of, concern about uncertainty around the scope, operation and legal enforceability of the instruments underpinning the IMS regime. Of particular concern with respect to privacy considerations is that, at the time of writing this submission, the Privacy Impact Assessments have not yet been completed for police and law enforcement use, transport use, and private sector use.

Specifically, some key protections and core concepts warrant elevation into the IMS bill. These include –

- **Prohibition against many-to-many use –** It is clearly not Governments' intention for the IMS to be used for many-to-many or blanket surveillance. However, the broad power in s7(1)(f) could potentially facilitate such a use.
- **Offences for which Facial Identification Service (FIS) can be used** – the IGA provides that the FIS only be used for offences carrying a maximum penalty of not less than three years imprisonment.
- **Not for evidentiary purposes –** the IGA is clear that IMS results are not to be used as the sole basis for ascertaining an individual's identity for evidentiary purpose.

Further, the **broad and inclusive language** used in s6 (for example 'including' and 'promoting' community and road safety) introduces ambiguity into the scope of the IMS regime, potentially leading to currently unforeseen uses, unintended consequences and undesirable privacy incursions. Clearly and carefully defined terms that provide clarity to future users of the IMS, and that are consistent with the core principles agreed to in the IGA and other instruments, are preferable.

(ii) The Identity-matching Services Bill 2018 should include strong oversight and review mechanisms to enhance transparency and to monitor mistakes and misuse relating to the IMS regime.

Adequate Parliamentary oversight of the Ministerial rule-making powers in s5(1)(n), s7(1)(f), s8(2)(q) and s30 is imperative. Given the recent movement of some functions from the Attorney-General's Department to the Department of Home Affairs, and the multiple functions of Home Affairs in the regime (in the development and operation of the IMS, as well as being a user of the IMS), rigorous governance, accountability and transparency arrangements are essential. In this context, it may be appropriate for the Committee to consider whether a disallowable instrument will provide sufficient Parliamentary scrutiny over the Minister's broad discretion to make rules. As highlighted by the Standing Committee for the Scrutiny of Bills in Scrutiny Digest 2 of 2018, it may be appropriate to consider whether regulations are a more appropriate vehicle.

Further, an **appropriate legislative review process**, in terms of both timing and scope, is essential for public confidence and the assessment of impacts on privacy. The IMS bill is silent on the matters that should be considered as part of the review of the operation of the Act, and it may be appropriate for the IMS bill to specify critical components of that review, such as expansion of services within the IMS regime, abuse of the system, mistakes arising from false positives, unintended outcomes from the IMS, etc. It would also be preferable for the **review to commence two years after commencement** of the legislation. A two year review period was recommended by the Queensland Parliamentary Legal Affairs and Community Safety Committee following its consideration of the Queensland bill[1].

Additional requirements in annual reporting processes are also necessary to adequately monitor privacy impacts, misuse, mistakes and private sector use associated with the IMS regime. As currently drafted, the IMS bill does not require data breaches or security incidents (for example through unauthorised access or unauthorised disclosure), system failures or accuracy rates to be reported upon. For example, IMS outputs will inevitably be used for gaining/executing search

[1] 'The committee recommends that a review of the changes made by this legislation be conducted two years after its commencement to evaluate the frequency, purpose and type of identity matching services used, the users, the error rates and any incidences of service expansion' (Report No. 1, 56th Parliament, Legal Affairs and Community Safety Committee, March 2018). Accessible at https://www.parliament.qld.gov.au/work-of-committees/committees/LACSC/inquiries/current-inquiries/POLABILL2018

warrants and making arrests, however monitoring and reporting on erroneous use of IMS outputs is not canvassed in the IMS bill.

Further, the IMS bill does not require that non-government entities using the Facial Verification Service (FVS) be identified by name in the annual report [s28(b)]. The Explanatory Memorandum indicates that this is to protect commercial confidentiality. However, private sector users of the FVS will be required to secure the consent of the individual whose identity they are seeking to verify [s7(3)(b)]. As this would reveal to the individual that the non-government entity is using the FVS, it is unclear why the commercial confidentiality of that non-government entity would be compromised by its identification in the annual report.

Based on the broad themes raised in this submission – that the IMS bill should entrench the intended uses of the IMS and strong oversight mechanisms – the Queensland OIC respectfully suggests that the Committee consider amendments to the IMS bill that will:

1. Embed core principles, currently articulated in the associated instruments, into the legislation, including –
    a. that any future identity-matching service, which could be prescribed by Ministerial Rule under s7(1)(f), explicitly exclude a many-to-many service or blanket surveillance service
    b. that the FIS can only be used for offences carrying a maximum penalty of not less than three years imprisonment, and
    c. that IMS outputs are not to be used for evidentiary purposes.
2. Ensure the legislation defines key terms narrowly and explicitly to minimise potential for scope creep that could be facilitated by the broad interpretation of terms.
3. Strengthen the oversight and review mechanisms of the IMS regime by requiring –
    a. Adequate Parliamentary oversight of Ministerial rule-making powers prescribed under the legislation,
    b. That the review of the operation of the Act be initiated within two years of commencement and specifically addresses matters such as erroneous use of IMS outputs, service expansion, privacy incursions and unintended consequences, and
    c. That annual reporting requirements be expanded to include data breaches, security incidents, accuracy rates, and identification of private sector users of the FVS.

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