Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

21 March 2018

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Committee Secretary,

Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission to the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) in relation to the Review of the *Identity-matching Services Bill 2018* (**the Bill**) and the *Australian Passports Amendment (Identity-matching Services) Bill 2018*.

Established in September 2017, OVIC is the primary regulator for information privacy, data protection and freedom of information for the state of Victoria. As Information Commissioner I have a strong interest in matters that affect individuals' privacy, and one of my functions under the *Privacy and Data Protection Act 2014* (**PDP Act**) is to make public statements in relation to such matters.

This submission outlines my office's views on the Bill, highlighting the serious concerns we have about the privacy impacts on individuals and the Bill's implications for the civil liberties of all Australians more broadly.

1. In principle, OVIC supports the use of the identity-matching services (**IMS**) in the context of national security, however this must be subject to the strictest controls. As the Bill stands, OVIC has concerns about the rigour of the governance processes currently proposed, given that risk will largely be managed via agreements between the parties – such as through the Participation Agreement – rather than through the legislation itself. We question the enforceability of these arrangements. The ability for fundamental controls to be amended without parliamentary oversight may also be problematic.

2. Based on discussions with the Department of Home Affairs (**DHA**), OVIC understands that the governance of the IMS is modelled on the regime already in place for the Document Verification Service (**DVS**). OVIC appreciates that this process has been largely successful, however the scope and potential privacy impact of the IMS is considerably greater than that of the DVS. The DVS allows the validity of documents to be assessed; the IMS allows similar functionality, with the addition of the ability to verify that the photo on a document matches one or more individuals. However, it potentially also offers law enforcement and national security agencies the ability to determine where an individual has been, and when. This is a substantial difference in the kind of service offered by the DVS. For that reason alone, my office suggests that a more robust set of

checks and balances is necessary on the use of the IMS, to protect against misuse or scope creep in the application of the service.

3. OVIC has a number of concerns about the expansion of the IMS to the private sector and local government authorities (clause 7(2)). The variation in the quality of governance and security that can be expected, particularly from local government, raises issues in relation to the adequacy of information management practices and personal information protection. The potential for scope creep – in that personal information may be used for additional purposes other than those for which it was initially collected – is also a significant concern.

4. OVIC notes that the use of the Face Identification Service (**FIS**) – commonly described as 'one-to-many' matching – is limited to the bodies listed in clause 8(2) of the Bill, and that new users of the FIS may only be added if they fulfil the functions of the law enforcement, border protection and integrity bodies listed in that clause. This restriction is welcome as the extension of the FIS to any other bodies would represent a considerable risk, including to the security of legally assumed identities. OVIC notes that the risk of compromise of legally assumed identities is proportional to the number of bodies able to perform such matching, so it is in the interests of the national security community to restrict this access to as few agencies (and individuals in those agencies) as possible.

5. However, OVIC would be very concerned if any of the functions of the bodies identified in clause 8(2)(a) to (p) were to be undertaken by the private sector. This would substantially change the nature of the risk and compliance framework, especially given the caps the Participation Agreement places upon liability, which are very low relative to common commercial practice. Expansion of the FIS to the private sector may not be currently contemplated or even permitted by clause 8(2), however, given the broad power of the Minister under clause 30(1), my office recommends that this possibility be expressly ruled out.

6. The Bill contains a single measure for reporting on the use of the IMS. Clause 28(3) of the Bill requires the Secretary of the Department to provide a report to the Minister within six months of the end of the financial year. The report must then be tabled in Parliament by the Minister (clause 28(4)). The Bill requires that the report contain details of the frequency of access and the agency accessing the service (clause 28(1)), but it does not specify any reporting on data breaches or misuse of the services. The reporting is thus similar to reporting on the operation of the Commonwealth *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015,* in that it tells the public about the quantum of requests but little about the security of the data or the compliance of participants in the IMS ecosystem.

   In the context of such a powerful tool, that has the capability to be used for surveillance, OVIC believes the scope of this reporting in relation to the IMS is inadequate. We recommend that another mechanism be incorporated into the Bill to include specific reporting relating to instances of unauthorised or inappropriate access and remedial action taken, and that this be included in the Minister's annual report. Transparency is integral to good governance, and the Bill falls significantly short of expectations in this regard. In order for the public to have confidence that the compromise between civil liberties and security is appropriately managed, it will be necessary for the public to have an informed view of that management.

7. In assessing reporting under the IMS, we note that the Notifiable Data Breaches scheme, introduced under the new Part IIIC of the Commonwealth *Privacy Act 1988*, applies to DHA's operation of the service, such that if DHA exposed data, the breach may be reportable. However, if a state or territory were to expose data provided by another jurisdiction, there does not appear to be an arrangement under which this would be publicly reported. While Part 4 of the Bill provides for penalties for misuse, there needs to be more transparency in reporting any misuse or accidental disclosure, as a mechanism for public scrutiny.

8. In general, while we appreciate that management of activities across multiple jurisdictions cannot be achieved through Commonwealth law alone, OVIC has a concern that managing compliance through the Participation Agreement and Compliance Policy may not be sufficiently robust. Given that law enforcement and national security bodies will come to rely on the IMS for information, and that completeness of the information is an important part of the effectiveness of the IMS, there is an element of moral hazard in that suspension of a Requesting Agency for non-compliance may have an impact on the willingness of a state or territory Data Holding Agency from the same jurisdiction to continue to provide data. The mechanisms to manage this, out of public gaze in a governance committee, should be strengthened by public disclosure of the issues raised in paragraphs 6 and 7 above, to ensure members of the governance committee are held accountable for secure and proper operation of the IMS.

9. The Bill relies upon the provisions of the *Intergovernmental Agreement on Identity Matching Services* (**IGA**), agreed by COAG on 5 October 2017, to provide consent mechanisms for sharing of facial biometrics and other data. However, the Bill itself does not provide any detail on the offences for which the one-to-many power of the FIS can be utilised. Clause 4.21(b) of the IGA limits the use of the FIS to Commonwealth or state offences carrying a penalty greater than three years imprisonment. The interaction between the Bill and the ecosystem of agreements (including the related policy documents) places a high burden on training users of the FIS in order to understand the circumstances under which the use of the one-to-many service can be accessed. We recommend that the threshold for accessing the FIS be stipulated in the Bill to avoid confusion and signal to the community through the legislation that access to the FIS is not unfettered.

   The inter-related nature of the Bill, the IGA and the other agreements also makes assurance of compliance activities more complex, and is another reason for more transparent reporting – so that the Commonwealth, the states and territories, the various Data Hosting and Requesting agencies, and the public, have a clearer view of the uses of the FIS.

10. OVIC suggests the review provisions outlined in clause 29 are insufficiently detailed to provide reassurance about the scope of the review, or the criteria that will be applied. We recommend that this clause contain further detail to ensure that reviews are sufficiently robust and achieve their purpose.

11. Because so few of the governance rules to be observed in the operation of the IMS are encompassed by the Bill, the breadth of discretion provided to the Minister in clause 30(1), which enables the Minister to do anything necessary or convenient, has considerable potential for scope creep. While the inclusion of this clause may be necessary to make the Bill workable, we suggest that parliamentary review for the purposes of disallowing the instrument under clause 30(3) requires accurate and comprehensive information on governance and misuse (if any) of the IMS, and that the reporting suggested in the paragraphs above will also be necessary to provide sufficient protection in relation to this potential for scope creep.

Thank you for the opportunity to comment on the Bill. My office will be watching this review with interest, and we look forward to reading the Committee's final report.

Yours sincerely,

Sven Bluemmel
Information Commissioner