Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Our reference: 13/000174-05

Mr Andrew Hastie MP
Chair, Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Mr Hastie

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

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) on the Identity-matching Services Bill 2018 (IMS Bill) and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (Passports Bill). The provisions in these Bills apply to the collection, use or disclosure of identification information[1] or information relating to the identity of a person[2] via identity-matching services.

The OAIC appreciates the engagement of the Department of Home Affairs (Home Affairs)[3] with the OAIC and its commitment to undertaking Privacy Impact Assessments as the proposal has developed.[4]

Under the *Privacy Act 1988* (Cth) (Privacy Act) a function of the Australian Information Commissioner and Privacy Commissioner (the Commissioner) is to examine a proposed enactment that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals.[5] The Commissioner also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised.[6]

The OAIC supports measures that aim to address identity-related crime, and enable law

---

[1] As defined in s 5 of the IMS Bill.

[2] As referred to in s 1 of the Passports Bill.

[3] The Attorney-General's Department commenced this engagement, though Home Affairs was subsequently established and carries out some of the functions of the Attorney-General's Department, including the engagement with the OAIC on this matter.

[4] See https://www.homeaffairs.gov.au/about/crime/identity-security/face-matching-services, which lists PIAs of the NFBMC's Interoperability Hub and the Face Verification Service.

[5] Section 28A(2)(a) of the *Privacy Act 1988.*

[6] Section 28A(2)(c).

enforcement bodies to cooperate to achieve this objective. The right to privacy is not absolute, and in some circumstances privacy rights must necessarily give way where there are compelling public benefits to do so. However, initiatives which require or authorise the collection, use or disclosure of personal information should be reasonable, necessary and proportionate, having regard to the objectives they seek to achieve.

The OAIC suggests that the Bill requires further consideration to better ensure that any adverse effects of the proposed enactment on the privacy of individuals are minimised. In particular, we ask that the Committee give consideration to the following matters:

- the IMS Bill should be the primary source of privacy protection measures, supported by relevant governance documents and arrangements
- the IMS Bill explicitly limits local government authority or non-government entity access to only the Face Verification Service (FVS)
- the reporting requirement in the IMS Bill is expanded to include a wider range of matters that are relevant to the performance of the identity-matching services
- the appropriateness of the five year review period for the IMS Bill
- any Rules made by the Minister should be subject to mandatory consultation with the Commissioner, not only those rules which prescribe additional types of identification information or new identity matching services.

Privacy impacts of sharing identification information

The Privacy Act regulates the way individuals' personal information is handled. Australian Government agencies (and the Norfolk Island administration) and all businesses and not-for-profit organisations with an annual turnover more than $3 million have responsibilities under the Privacy Act, subject to some exceptions.

Identification information, as defined in the IMS Bill,[7] would appear to be personal information, as defined in the Privacy Act.[8] Additionally, some identification information, such as biometric information, would be sensitive information for the purposes of the Privacy Act.[9] Sensitive information is generally afforded a higher level of privacy protection under the Australian Privacy Principles (APPs) in the Privacy Act than other personal information.

The APPs regulate the way in which entities are authorised to collect, use and disclose personal information. Entities regulated by the Privacy Act are generally not permitted to collect, use or disclose personal information for a purpose other than the purpose for which the personal information was collected, unless the individual has consented or an exception applies. One such exception is where a collection, use or disclosure of personal information for a secondary purpose is required or authorised by an Australian law.

The IMS Bill and Passport Bill, if passed, would invoke this exception by authorising the

[7] Section 5 of the IMS Bill.

[8] *Privacy Act 1988* (Cth), s 6(1).

[9] *Privacy Act 1988* (Cth), s 6(1).

collection, use and disclosure of personal and sensitive information. However, other APPs, such as principles relating to information security,[10] information quality[11] and information governance[12] will continue to apply. The OAIC also notes that in the event of a data breach, entities regulated by the Privacy Act and using the identity-matching services will be required to comply with the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act.

The IMS Bill and Passports Bill will enable the sharing of identification information of the vast majority of individuals living in Australia. In addition, the identity-matching services will enable the transmission of identification information at a much faster rate than is currently possible.[13] For these reasons, the Bills should be drafted as narrowly as possible to achieve their objectives while minimising the adverse impacts on privacy rights and obligations.

IMS Bill

Privacy protections in the IMS Bill

The OAIC suggests that the IMS Bill should be the primary source of privacy protection measures, supported by governance documents and arrangements. We consider this a necessary measure due to the scale and sensitivity of information that will be collected, used and disclosed by the identity-matching services.

The OAIC understands that there will be a number of privacy, transparency and accountability measures that will form part of Home Affairs' overall implementation of the identity-matching services. The Explanatory Memorandum (EM) to the IMS Bill refers to participation agreements and data-sharing arrangements under which specific conditions can be placed on the use of a particular agency's data by another entity.[14] At the time of writing this submission, these governance documents are undergoing consultation, and could be subject to change.

The *Intergovernmental Agreement on Identity Matching Services* (IGA), signed by the members of the Council of Australian Governments on 5 October 2017, also refers to privacy measures such as the requirement to conduct privacy impact assessments, conduct annual compliance audits, and provide appropriate training, which are further outlined in the EM to the IMS Bill.[15] The IGA also states that law enforcement use of the identity-matching services is intended to be restricted to offences that carry a minimum penalty of three years imprisonment. Comparative legislation incorporates this three year imprisonment requirement.[16]

Importantly, these measures are not currently contained within the IMS Bill. Given the robust scrutiny process surrounding the creation and amendment of Acts of Parliament, the OAIC

---

[10] APP 12.

[11] APP 10.

[12] APP 1.

[13] Refer to p 3, 48, 52-3 of the EM to the IMS Bill

[14] Refer to p 8 of the EM to the IMS Bill.

[15] Refer to p 43 of the EM to the IMS Bill.

[16] Section 180(4) of the *Telecommunications (Interception and Access) Act 1979*.

suggests that these privacy protection measures are included in primary legislation, rather than governance documents.

The OAIC notes that the IMS Bill does include some privacy enhancing provisions. For example, the OAIC welcomes the requirement for the Minister for Home Affairs to consult the Australian Information Commissioner before prescribing an additional type of identification information, or an additional type of identity-matching service.[17] The OAIC also supports the IMS Bill imposing limits on the recording and disclosure of protected information,[18] which helps to narrow the authorised collection, use or disclosure of personal information.

The OAIC notes that the Senate Standing Committee for the Scrutiny of Bills, in its Scrutiny Digest of 14 February 2018,[19] raised a similar consideration as to whether the administrative safeguards identified in the EM to the IMS Bill could be strengthened by inclusion in the Bill.

Use of identity-matching services

The IMS Bill allows local government authorities or non-government entities (including the private sector) to collect, use, and disclose identification information, and to have access to the interoperability hub or NDLFRS,[20] subject to a number of conditions.[21]

The OAIC understands from the EM to the IMS Bill that the use of identity-matching services by local government and non-government entities will be limited to the FVS function. This limitation is not made explicit in the IMS Bill. In the interests of maintaining stringent controls over access to the identity-matching services, the OAIC suggests that the Bill include a provisions limiting local government and non-government entities' use of the identity-matching services to the FVS.

Annual reporting

Under s 28 of the IMS Bill, the Secretary of Home Affairs must give the Minister a report that includes a range of information each financial year. However, as the Senate Standing Committee for the Scrutiny of Bills notes,[22] there is no requirement to record and report on instances in which information was disclosed to lessen or prevent threat to life or health,[23] or relating to a corruption issue.[24] The EM to the IMS Bill does not explore why these instances should not be reportable. The OAIC suggests that, subject to national security or commercial

---

[17] See ss 5(1)(n) and 5(4)(b); ss 7(1)(f) and 7(5).

[18] Section 21 of the IMS Bill.

[19] Standing Committee for the Scrutiny of Bills, Scrutiny Digest 2 of 2018, 14 February 2018, pp 20–28, <https://www.aph.gov.au/~/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2018/PDF/d02.pdf?la=en>.

[20] Section 7 of the IMS Bill.

[21] See s 7(3) of the IMS Bill.

[22] Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 2 of 2018*, 14 February 2018, pp 27–28, <https://www.aph.gov.au/~/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2018/PDF/d02.pdf?la=en>.

[23] Section 23 of the IMS Bill.

[24] Section 24 of the IMS Bill.

confidentiality requirements,[25] the IMS Bill be amended to incorporate a reporting requirement for these instances.

While the IMS Bill outlines a number of statistical requirements for the report,[26] the Secretary is not required to report on a number of other matters that would be relevant and useful in considering the performance of the identity-matching services. For example, the Secretary could report on any data breaches (such as through unauthorised access) that may have occurred as part of the use of identity-matching services, any system outages affecting the identity-matching services, or the number of 'false positive' matches generated by the identity-matching services that incorrectly identify an individual.

The OAIC suggests that s 28 of the IMS Bill be expanded to include a requirement for the reporting of data breaches, security incidents, accuracy issues, and any other matters that the Committee considers relevant and useful to assist the Minister to determine areas in which the identity-matching services can be improved. These additional reporting obligations would provide greater certainty and transparency about the privacy impacts of the use of identity-matching services.

Review of the operation of the identity-matching services

Section 29 of the IMS Bill requires the Minister to cause a review of the operation of its provisions within five years of enactment. The EM to the IMS Bill suggests that a five year timeframe is required to allow sufficient operating time for all of the states and territories using the identity-matching services.

Recognising the sensitivity of identification information, and particularly biometric identifiers, information handling practices that will be authorised by this legislation, a time span of up to five years before this review is conducted appears to be a disproportionately long period. Comparative recent legislation that enabled the 'data retention scheme', which also introduced a new set of practices for the handling of large volumes of personal information, required a review of the relevant provisions within three and a half years.[27]

With this in mind, the OAIC suggests the Committee considers the appropriateness of the five year timeframe for a review of this Bill. The OAIC supports the tabling of this review in Parliament and, in the interests of transparency and accountability, encourages the public release of this review to the fullest extent possible.

Rules

Under s 30(1)(b) of the IMS Bill, the Minister can make rules prescribing matters required or permitted to be prescribed, or necessary or convenient for carrying out or giving effect to the

---

[25] Refer to p 37 of the EM to the IMS Bill, which indicates that commercial confidentiality may be a consideration for some aspects of the application of the IMS Bill to non-government entities.

[26] Section 28(1) of the IMS Bill.

[27] Section 187N(1A) of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*.

Bill. This provides the Minister with a wide discretion to make rules affecting the operation of the identity-matching services. These rules would be in the form of a disallowable instrument.

The OAIC again notes the sensitivity and volume of information that will be handled by the identity-matching services, and the potentially wide-ranging ramifications of any rules made under the IMS Bill.

The OAIC suggest that any rules made by the Minister should be subject to mandatory consultation with the Commissioner, not only those rules which prescribe additional types of identification information or new identity matching services.

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

Yours sincerely

Angelene Falk
Acting Australian Information Commissioner
Acting Privacy Commissioner

10 April 2018