Law Council
OF AUSTRALIA

Office of the President

6 April 2018

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

By email: pjcis@aph.gov.au

Dear Mr Hastie

Review of the Identity-matching Services Bill 2018

1. Thank you for the opportunity to provide a supplementary submission to the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) regarding the Identity-matching Services Bill 2018 (Cth) (**the Bill**).

2. The Law Council acknowledges the assistance of its Privacy Law Committee of the Business Law Section and the Law Society of New South Wales in the preparation of this supplementary submission.

3. The Law Council has limited its comments to those matters raised in paragraph 8 of the Law Council's original submission to the Committee on 21 March 2018. These are:

   (a) inconsistencies between the definitions in the Bill and the *Privacy Act 1988* (Cth) (**Privacy Act**), including 'identification information'; and
   (b) conditions on local government authorities or non-government entities requesting access to identity-matching services.

4. The issues set out below outline the Law Council's concern that the Bill operates to create a new category of data and will erode current protections provided by the Privacy Act. It is the Law Council's view that such a shift should, at a minimum, be expressly identified and acknowledged to allow for informed consideration and public debate.

Overlap and inconsistencies in definitions

5. Proposed section 5 of the Bill defines 'identification information'. The Law Council notes that this definition does not directly align with the definition of 'personal information' in the Privacy Act.[1] The definition of 'identification information' also extends to information about

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

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

a deceased person, which is not generally covered by the Privacy Act.[2] These differences are not addressed in the Explanatory Memorandum or any other material accompanying the Bill and it is unclear whether this difference in the definitions is intended or the implications have been fully considered.

6. The Law Council is concerned that this difference in definitions will result in a complex legal and regulatory landscape and create uncertainty for both organisations and individuals.

7. These inconsistencies will also result in a departure from existing standards for the protection of personal and sensitive information in the Privacy Act. The Bill authorises the Department of Home Affairs to collect, use and disclose identification information in order to operate the Interoperability Hub and the identity-matching services set out in the Bill,[3] as agreed in the Intergovernmental Agreement on Identity Matching Services (**IGA**).[4] The Bill will facilitate the collection, use and dissemination of a large volume of existing personal information that would otherwise be protected under the Privacy Act. It will also facilitate the creation of a large volume of personal information, much of which will be sensitive information,[5] which generally receives a higher level of protection under the Privacy Act.

8. The Law Council considers that at present there is insufficient recognition of the adverse impact of this Bill on existing privacy protections, the scope of this impact or justification for the reduced privacy protections. Given the potential impact of the Bill, the Law Council is of the view that the departures from existing privacy standards within the Bill need to be expressly articulated to allow for a full and informed debate.

Local Government Authorities and Non-Government entities

9. The IGA provided for the possibility of private sector access to the Face Verification Service. Proposed subsection 7(2) of the Bill provides that:

> *… the Minister may only make rules for the purposes of paragraph (1)(f) prescribing a service that involves a request from a local government authority or non-government entity, relating to an individual if:*
>
> *a) the purpose of the service is to verify the individual's identity; and*
>
> *b) the conditions in subsection (3) are met in relation to the local government authority or non-government entity.*

[2] Office of the Australian Information Commissioner 'What is personal information' (May 2017), available at https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information.
[3] Explanatory Memorandum, Identity-matching Services Bill 2018 (Cth), 2 [5].
[4] Council of Australian Governments, 'Intergovernmental Agreement on Identity Matching Services' (5 October 2017) available at https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf.
[5] *Privacy Act 1988* (Cth) s 6, noting specifically items (d) and (e) of the definition of "sensitive information" expressly includes "biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates".

10. Proposed subsection 7(3) of the Bill sets out the conditions which must be met for a local government authority or non-government entity to request an identity-matching service. These are:

    a) *verification of the individual's identity is reasonably necessary for one or more of the functions or activities of the local government authority or non-government entity; and*

    b) *the individual has given consent for the local government authority or non-government entity to use and disclose, for the purpose of verifying the individual's identity, the identification information about the individual that is included in the request; and*

    c) *the local government authority or non-government entity either:*

        (i) carries on activities in Australia from premises in Australia; or
        (ii) resides in Australia; and

    d) *either:*

        (i) the Privacy Act 1988 applies (with or without modifications prescribed by regulations under that Act) to the local government authority or non-government entity as an organisation (within the meaning of that Act); or

        (ii) the local government authority is bound by a law of a State or Territory, or has entered into a written agreement with the Department, that meets the requirements of subsection (4).

Consent

11. One of the requirements set out in proposed subsection 7(3) of the Bill is that the local government authority or non-government entity must obtain the consent of the individual whose identity is to be verified. In the Law Council's previous submission on this Bill, it was noted that further information is needed as to how such informed consent is to be recorded and verified to a standard that will enable access to the Face Verification Service. For the reasons set out below, the Law Council considers that the reference to 'consent' in this context may be misleading.

12. Guidance issued by the Office of the Australian Information Commissioner states that there are four elements of consent in the context of the Privacy Act:

    a) *the individual is adequately informed before giving consent;*

    b) *the individual gives consent voluntarily;*

    c) *the consent is current and specific; and*

d) the individual has the capacity to understand and communicate their consent.[6]

13. That guidance also provides that consent is voluntary in circumstances where 'a person has a genuine opportunity to provide or withhold consent'. In the context of the operation of this Bill it is unlikely that individuals will have a genuine choice to withhold consent if they wish to obtain the relevant services. There is no obligation on entities to provide a practical alternative means of accessing the relevant services to avoid use of the facial matching services. The Law Council considers that 'consent' given in such a situation will not satisfy the requirements for consent. The Law Council also notes that it would not be aligned with the prescribed notion of consent in certain key international instruments that operate to regulate privacy, most notably the European Union's (**EU**) General Data Protection Regulation (**GDPR**) which comes into effect on 25 May 2018.[7] While the GDPR regulates the privacy rights of individuals in the EU, it also serves as an important precedent for privacy regulations and their application internationally.

14. While the Law Council has noted a number of concerns with local government authorities or non-government entities having access to identity matching services, if such proposed access is to proceed it would be appropriate for the Bill to be amended to more accurately refer to a requirement for the relevant local government authority or non-government entity to provide clear notice to individuals of the collection and use of their identifying information. This would assist to ensure that users or consumers fully appreciate the basis on which they are providing their identification information. This is particularly important given that local governments deliver a range of services which by their very nature collect and generate a large volume of personal information, often sensitive information (for example, day care services or other community service initiatives for people within the council area).

15. The Law Council also proposes that the information provided by local government authorities or non-government entities to individuals whose identities are to be verified using identity-matching services should be required to include information about a number of aspects of the use of the data including:

    (a) practices undertaken in relation to the face matching services;
    (b) the risks to the individual in the event that their biometric data is compromised;
    (c) the absence of any enforceable legal remedy if the information is lost or breached;
    (d) the jurisdiction and control over the data hosting and usage mechanisms; and
    (e) the full list of identity-matching systems which may be able to use this data once collected.

[6] Office of the Australian Information Commissioner, 'Australian Privacy Principle Guidelines' Chapter B, (March 2015), available at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#consent.

[7] Article 4 defines consent to mean to be 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' and Article 7 prescribes the conditions that must be met before the consent is said to be valid.

16. Information of this kind will provide individuals with an opportunity to understand what is being done with their biometric data and the potential implications.

Protections for use of identifying information by local government authority or non-government entity

17. Proposed subsection 7(4) of the Bill allows the Minister to make rules allowing organisations who are not covered by the Privacy Act to use a service to verify an individual's identity. The requirements in proposed subsection 7(4) are that the law or agreement must provide for:

    a) *protection of personal information comparable to that provided by the Australian Privacy Principles (**APPs**);*

    b) *monitoring of compliance with the law or agreement;*

    c) *a means for an individual to seek recourse if his or her personal information is dealt with in a way contrary to the law or agreement.*

18. It is unclear how these provisions will operate. For example, there is no indication who will be responsible for 'monitoring of compliance with the law or agreement' as required in proposed paragraph 7(4)(b). Participating agencies who are not APP bodies under the Privacy Act may not be subject to existing audits or independent oversight by external bodies.

19. Further, the requirement for 'a means for an individual to seek recourse' does not provide for that means to be the same as, or equivalent to, the options available to individuals under the Privacy Act. This may result in a scheme where individuals dealing with a non-APP entity will have a different range of dispute resolution options available to those interacting with an APP entity. The Law Council is concerned that this approach will result in complexity, possible confusion and inadvertent erosion of existing rights.

Should you have any queries, please contact Dr Natasha Molt, Deputy Director of Policy, Policy Division [redacted]

Yours sincerely

Morry Bailes
President