Law Council
OF AUSTRALIA

Office of the President

21 March 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 and the Australian Passports Amendment (Identity-matching Services) Bill 2018

1. The Law Council welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Security and Intelligence (**the Committee**) regarding the review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-Match Services) Bill 2018 (**the Bills**).

2. The Law Council acknowledges the assistance of its Privacy Law Committee of the Business Law Section, the Law Society of New South Wales, the Law Institute of Victoria and the Bar Association of Queensland in the preparation of this submission.

3. The Identity-matching Service Bill 2018, if enacted, will facilitate the exchange of identity-information between the Commonwealth and State and Territory Governments as agreed by the Council of Australia Governments under the Intergovernmental Agreement on Identity Matching Services of 5 October 2017. The Bill will authorise the Department of Home Affairs to collect, use and disclose identification information to operate the systems that will support a set of new biometric face-matching services.

4. The Australian Passports Amendment (Identity-matching Services) Bill 2018, if enacted, will amend the *Australian Passports Act 2005* (Cth) to allow automated disclosure of Australian travel document data available between Commonwealth, state and territory agencies for the purposes of identity-matching services.

5. Some States such as Queensland have already enacted legislation to reflect the Council of Australian Governments agreement to allow law enforcement agencies across the Australia to share access to passport, visa, citizenship and driver's licence images. The Law Council notes that the Police and Other Legislation (Identity and Biometric Capability) Bill 2018 (QLD) was enacted without the concerns of the Bar Association of Queensland being addressed (see Attachment A for the Bar Association of Queensland's submission).

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

Consultation timeframe

6. The Law Council is disappointed at the extremely short timeframe that has been set for submissions to the Committee's inquiry into these Bills. The opportunity for public submissions was announced on 8 March 2018[1] and submissions have been requested by 21 March 2018. This has resulted in a very limited time for thorough review and consideration of the proposed legislation, which the Law Council considers is particularly problematic in light of the potentially serious privacy implications of the Bills. The Law Council notes that it is unclear why such a short timeframe has been imposed on this inquiry.

7. As a result of the timeframe for response, the Law Council has only had a very brief opportunity to review the proposed legislation and has been unable to develop a comprehensive submission. The Law Council requests that the Committee extend the period by which to provide feedback and that the Australian Government extend the reporting date of the Committee so that the Committee has a reasonable opportunity to consider the Bills.

8. Extra time is needed to allow for example a proper analysis of the following issues in the Identity-matching Service Bill 2018:

    (a) overlap and inconsistencies in the definitions (e.g. 'personal information' and 'identification information');
    (b) scope of the definition of 'identification information' to include information about deceased individuals; and
    (c) conditions on local government authority or non-government entity requesting identity-matching service appear to include consent. It is not clear how this is to work given the broader mandated purposes provided for in the Bill and the fact that the *Privacy Act 1988* (Cth) does not *prima facie* apply to local governments. The working combination of requirements in proposed subsection 7(3) needs more testing including what the protections would be should the Bill be enacted as proposed.

9. Due to the short timeframe, the Law Council makes the following comments and recommendations primarily in relation to the Identity-matching Service Bill 2018.

The nature of the Interoperability Hub[2]

10. The Identity-matching Services Bill 2018 will enable the Secretary of the Department of Home Affairs to develop and operate an interoperability hub, to be used for the purposes of requesting and providing the identity-matching services provided for in the Bill. These include:

    - the Face Verification Service, which will allow government agencies and private sector organisations to verify a known or claimed identity;
    - the Face Identification Service, which will allow law enforcement, intelligence and anti-corruption agencies to identify an unknown person;

[1] House of Representatives Media Release, 'Committee to review Identity-matching Services Bill', 8 March 2018.
[2] The Law Council adopts this input from the Law Society of New South Wales.

- the One Person One Licence Service (**OPOLS**) which will allow state and territory agencies to detect cases where a person may hold multiple driver or other licences or fraudulent identities across jurisdictions;
- the Facial Recognition Analysis Utility Service, which will allow state and territory agencies to assess the accuracy and quality of their data holdings;
- the Identity Data Sharing Service, which will allow for the sharing of biometric information between Commonwealth, state and territory agencies; and
- any other service prescribed by the rules that involves the collection, use and disclosure of identification information and involves the Interoperability Hub or the National Driver Licence Facial Recognition Solution.

11. The Bill also provides for the creation of a National Driver Licence Facial Recognition Solution.

12. The Law Council notes that the identity matching services operating through the Interoperability Hub will use information taken for a particular purpose for other purposes for which the consent of individuals has not been obtained. For example, individuals have consented to providing a photograph to obtain a passport or driver licence but have not consented to their biometric information being extracted from that image and being used for other purposes. The Law Council considers that enabling the use of biometric information in this way may have the effect of undermining the notion of informed consent by individuals in relation to their personal information.

13. Further, the Law Council notes that the Senate Standing Committee for the Scrutiny of Bills has expressed concern that the Identity-matching Services Bill 2018 may unduly trespass on personal rights and liberties in seeking to enable the sharing 'of an extensive amount of personal information for a broad range of purposes to a broad range of agencies'.[3] Part of the reason for this concern arises because, as currently drafted, the Bill will allow state and territory agencies to share and seek to match facial images and other biographical information for persons suspected of involvement in very minor offences. The Law Council considers that this may not be a necessary or proportionate response and that aspect of the Bill may constitute an arbitrary interference with the right to privacy in conflict with Article 17 of the *International Covenant on Civil and Political Rights*.[4] The Law Council also notes that the Bill implements an intergovernmental agreement, and therefore aspects of the Bill may constitute an arbitrary interference with the right to privacy in conflict with the *Charter of Human Rights and Responsibilities Act 2006* (Vic) and the *Human Rights Act 2004* (ACT).

14. In addition, information about a person, such as their race, ethnic origin or religious affiliation, may be inferred from the 'identification information' that is collected. This may indirectly result in the collection, use and disclosure of inferred information for a purpose, such as a community protection activity, that targets people based on their membership of a particular race, ethnic group or religion. The Law Council is of the view that the Bill does not currently have sufficient safeguards to protect against this kind of targeting.

15. A previous Privacy Impact Assessment of the Interoperability Hub concluded that the Interoperability Hub could collect more information than necessary and retain that data for

[3] Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 2 of 2018, 22-23.
[4] *International Covenant on Civil and Political Rights* opened for signature 16 December 1966, 993 UNTS (entered into force 3 January 1976), Art 17.

longer than necessary.[5] While the Attorney-General's Department indicated in response that only the minimum amount of transaction data required for audit and control purposes would be retained, it is unclear how this will work in practice.[6] It is difficult for the Law Council to comment further on the nature and operation of the Interoperability Hub or various identity matching services as there has been very little information released by the Government on their technical development.

16. To add to this concern, the Law Council also notes that there remain flaws with existing facial recognition technologies. Reportedly, the Australian Capital Territory Government has asked for assurances that data will only be used outside of counter-terrorism when the Interoperability Hub returns a perfect match.[7] The Law Council is of the view that additional technical information about the nature of the identity matching services and the process for ensuring that there are not false matches should be released publicly to allow informed debate about the proposed legislation.

Security of access to the Interoperability Hub and the National Driver Licence Facial Recognition Solution

17. The personal nature of information that passes through the Interoperability Hub raises serious concerns about the consequences of any potential security breach or unauthorised disclosures. Any inadvertent release, or breach in the security of biometric information is irrevocable.

18. Given the potentially life long consequences of a compromise, the Law Council considers that it would be appropriate for the Government to be asked to provide further information on:

- the consideration being given to developing an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security both in the short term and in the longer term, noting that in the long term many of the security measures currently in place may no longer be effective; and
- the methods for assessing the implications of any security breach and communicating the breach to both the general public (data subjects) and the technical, privacy and security communities.

Scope of the Interoperability Hub

19. Proposed section 5 of the Identity-matching Services Bill 2018 provides a definition of 'identification information'. Proposed paragraph 5(1)(n) provides that 'identification information' can include 'any information that is prescribed by the rules and related to the

[5] Information Integrity Solutions 'National Facial Biometric Matching Capability: Privacy Impact Assessment – Interoperability Hub' dated August 2015, available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF, Appendix 2.
[6] Attorney-General's Department, 'Preliminary Privacy Impact Assessment of the National Facial Biometric Matching Capability Interoperability Hub: Attorney-General's Department Response', December 2015, 3-4, available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/AGD-response-privacy-impact-assessment.pdf.
[7] 'Facial recognition: Feature creep may impose government's software in our lives, expert warns' *ABC News*, 5 October 2017, available at http://www.abc.net.au/news/2017-10-05/facial-recognition-coag-privacy-concerns-about-the-capability/9017494; 'Facial recognition tech perpetuates injustice', *Eureka Street,* 5 October 2017 available at https://www.eurekastreet.com.au/article.aspx?aeid=54138.

individual'. Such a broad Rule-making power would provide an opportunity for a Minister to use delegated legislation to significantly enhance the scope of this scheme.

20. The Law Council is concerned that the scope of this scheme, which may unduly trespass on personal rights and liberties, will be determined by delegated legislation rather than the primary legislation. The scope of this scheme will therefore not be subject to parliamentary scrutiny and oversight. The Law Council submits that 'identification information' should only be defined in the primary legislation and the Minister should not be granted this rule-making power.

21. Proposed subsection 5(4) provides that before making rules prescribing information for the purpose of proposed paragraph 5(1)(n) the Minister must consult with the Human Rights Commissioner and the Information Commissioner. The Law Council notes that as currently funded it may be the case that neither of these organisations will be sufficiently resourced to undertake this role.

22. The Law Council considers that the Bill should go beyond the current requirement to simply 'consult' and include a requirement for the Minister to report to the public on results of these consultations before any rule is made under proposed paragraph 5(1)(n). The Law Council also considers that it would be appropriate for the Minister to provide reasons if rules are made that are inconsistent with any advice provided by the Human Rights Commissioner or Information Commissioner, to ensure public confidence that the consultation and advice has been given proper weight by the Minister.

23. The Law Council also notes that the Senate Standing Committee for the Scrutiny of Bills has considered whether proposed paragraph 5(1)(n) should more appropriately provide a power to make 'rules' or to make 'regulations'.[8] Given that regulations are subject to a higher level of executive scrutiny than other delegated legislation, the Law Council suggests that it would be more appropriate for the Bill to provide for the making of regulations.

Access by private organisations – the Face Verification Service

24. The Intergovernmental Agreement allows for the possibility of private sector access to the Face Verification Service. Proposed section 7 of the Identity-matching Services Bill 2018 provides that:

> *…the Minister may make rules 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.*

25. 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 will be verified. The Law Council considers 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.

[8] Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 2 of 2018, \ 25.

26. The Law Council notes that the Bill does not provide any further safeguards or penalties for private organisations if they should make use of the Interoperability Hub or identity data in an unauthorised way. The provisions set out in proposed Part 4 relate only to 'entrusted persons', as defined. The current drafting of proposed section 7 of the Bill places the onus on an individual to make a complaint or seek recourse if his or her personal information is dealt with by a local government authority or non-government entity contrary to the law or agreement as a result of using the Face Verification Service. The Law Council considers that the proposed controls in place for the use of personal information by a local government authority or non-government entity are not sufficient.

27. The provisions of the Identity-matching Services Bill 2018 regarding local government or non-government entities accessing the Face Verification Service do not take into account the caveats on such access set out in the Intergovernmental Agreement.[9] The Intergovernmental Agreement provides private sector access to the Face Verification Service to match information held by states and territories will be subject to:

    (a) the express approval of the relevant minister(s) in each state or territory to use their jurisdiction's information for this purpose, to be communicated in writing to the Commonwealth at any stage following signature of this Agreement;
    (b) the outcomes of a privacy impact assessment covering the types of Organisations to be given access to the service
    (c) compliance with a [Face Verification Service] Commercial Service Access Policy developed by the Coordination Group, including a fee for service arrangement, and
    (d) an [Face Verification Service] Commercial Service audit and compliance programme overseen by the Coordination Group.[10]

28. The requirement for these factors to be satisfied has not been incorporated in the Bill. The Law Council considers that these are important safeguards that should be incorporated into the Bill.

29. Additionally, while the explanatory memorandum states that any private sector usage of the Face Verification System will only return a 'match or no match' response, without any additional information about the person,[11] this limitation is not contained within the Bill. Since the 'access policies and data sharing arrangements supporting the implementation of the Bill' have not been provided by the Government for review, it is unclear what the terms of those policies and agreements will contain.

Face Identification Service

30. The Intergovernmental Agreement states that the Face Identification Service can only be used for one or more of the permitted purposes set out at paragraph 4.21 of the Agreement. Those include general law enforcement, which is defined as the 'prevention, detection, investigation or prosecution of an offence under Commonwealth, state and/or territory laws carrying a maximum penalty of not less than three years imprisonment'.[12]

[9] Intergovernmental Agreement on Identity Matching Services, 5 October 2017, 5.4.
[10] Ibid.
[11] Identity-matching Services Bill 2018 (Cth), Explanatory Memorandum, [145].
[12] Intergovernmental Agreement on Identity Matching Services, 5 October 2017, 4.2(b).

31. The Identity-matching Services Bill 2018 provides that the Face Identification Service is a service used by specific agencies in the course of an identity or community protection activity[13]. The Explanatory Memorandum states that the term has been defined in the Bill to reflect the terms of the Intergovernmental Agreement.[14] However, in relation to law enforcement the Bill does not incorporate the limit that the offence must carry a maximum penalty of not less than three years imprisonment. While the Explanatory Memorandum states that the maximum period will be by agreement with the states and does not need to be included in the Bill,[15] the Law Council considers that in this respect the Bill appears inconsistent with the provisions and the spirit of the Intergovernmental Agreement.

32. Similarly, the Bill does not incorporate any of the additional requirements for the Face Identification Service, including the need to comply with the requirements of the Participation Agreement, set out in the Intergovernmental Agreement.

Oversight of the Interoperability Hub

33. The Law Council considers that it is necessary for the Government to provide further information about the proposed oversight of the Interoperability Hub and the operation of the Identity-matching Services Bill 2018.

34. The Law Council considers that the current requirement for an annual report, set out in proposed section 28 of the Identity-matching Services Bill 2018, provides insufficient oversight of the Interoperability Hub. As currently drafted, the Minister does not have to report on the details of non-government entities that access the Face Verification Service. While the Explanatory Memorandum states that this is due to consideration of commercial confidentiality,[16] the Law Council considers that the public have a right to know which non-government entities have access to the Face Verification Service.

35. Similarly, the Law Council notes that proposed paragraph 28(1)(c) excludes material relating to the Australian Security Intelligence Organisation (**ASIO**) from being included in the annual report to be made to Parliament. While there may be circumstances where it would affect matters of national security to release information about the type of information that ASIO collected or disclosed, the Law Council considers that this should be determined on a case by case basis and not included in proposed paragraph 28(1)(c) as a blanket exception, particularly in circumstances where ASIO has shared biometric data with international partners.

36. The Identity-matching Services Bill 2018 provides that the Minister must cause a review of the operation of the Act and the provision of identity matching services within 5 years of the commencement of that section. The Law Council considers that it would be desirable for an independent privacy review to be conducted of the Interoperability Hub.

37. Information previously published by the Attorney-General's Department states that the Office of the Australian Information Commissioner (**OAIC**) will be responsible for conducting audits of the Interoperability Hub.[17] No specific funding to support such an audit appears to have been included in the current Budget and it is unclear what such an

[13] Identity-matching Services Bill 2018 (Cth), s 8(1)(b).
[14] Identity-matching Services Bill 2018 (Cth), Explanatory Memorandum [70].
[15] Ibid [76].
[16] Ibid [242].
[17] Attorney-General's Department, "Fact Sheet: Face Matching Services", available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Face-matching-services-fact-sheet.pdf.

audit will involve and whether the report will be made publicly available. The requirement for regular audits by the OAIC is not included in the Identity-matching Services Bill 2018.

38. The Law Council notes that oversight of the retention, collection and use of biometric information is a substantial role, particularly given the significant expansion contemplated by this Bill. Accordingly, the Law Council suggests that Government should fully consider the utility of establishing a new regulatory authority with responsibility for this role. This would allow oversight to be conducted thoroughly and by an agency with a sole focus on, and expertise in, biometric data. The Law Council notes that the United Kingdom has created a Commissioner for the Retention and Use of Biometric Material, to ensure that there is an office responsible for governing the retention and use of biometric information in the United Kingdom.[18]

Thank you for the opportunity to provide these comments.

The Law Council would be pleased to elaborate on the above issues, if required.

Please contact Dr Natasha Molt, Deputy Director of Policy, Policy Division [redacted] in the first instance should you require further information or clarification.

Yours sincerely

Morry Bailes
President

[18] For further information see: https://www.gov.uk/government/organisations/biometrics-commissioner. See also useful discussion in Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approached to Oversight" [2017] UNSWLawJI 6; (2017) 40(1) University of New South Wales Law Journal 121.