Law Council
OF AUSTRALIA

Office of the President

30 October 2018

Mr Roger Wilkins AO
National Arrangements for the Protection and Management of Identity Information
Department of Home Affairs
4 – 6 Chan Street
BELCONNEN ACT 2613

By email: submissions@homeaffairs.gov.au

Dear Mr Wilkins,

National Arrangements for the Protection and Management of Identity Information

1. The Law Council welcomes the opportunity to provide a submission the Department of Home Affairs' (**Department**) Review of national arrangements for the protection and management of identity information (**Review**).

2. The Review intends to focus on arrangements for issuing, using and managing an individual's documents, credentials and their related identity information that are most commonly relied upon as evidence of a person's identity by government and sectors of the economy. The Review has been commissioned to determine ways to enhance or strengthen arrangements that support and govern the protection and management of identity information in order to:

   - better protect Australians from the theft or misuse of their identity information, and assist people to minimise and recover from the impacts of identity crime should they become victims;
   - provide better targeted (that is, more convenient, tailored, efficient and effective) government services to individuals and business; and
   - achieve these objectives in ways that respect and promote peoples' privacy.

3. The Review intends to consider the national arrangements for the protection and management of identity information, including under legislative frameworks, practices and systems for the collective, use and sharing of identity information, and coordination amongst government agencies, and between government and other entities.

4. The Law Council confines its feedback to remarks relevant to this stage of the process, noting that legislation relating to a consistent identity framework across a wide range of sectors is not yet underway for comment. The Law Council commends you and the Department for engaging early and including a broad cross section of industry. The Law Council would welcome an opportunity to provide further comments on any early drafts of the pending exposure draft of any pending Bills.

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

5. The Law Council provides the below comments regarding the issues as they present themselves in the course of the process to date, building on the discussions in the course of the sessions in Sydney on Tuesday 16 October 2018 and in Melbourne Monday, 22 October 2018 which were attended by representatives of the Law Council.

Consent for the use of Government-collected data

6. The Law Council considers it would be important for the Review to articulate the problem that is sought to be addressed by reference to the current data driven environment, in both the public and private sectors. It appears that the challenges in banking are vastly different to those in less regulated industries (such as consumer goods) and at least in part lends itself to some form of consent driven models. By contrast, most of the Government information gathering and data use requirements are driven by compulsory means. To the extent that data collected by Government agencies is to be used in the private sector context (such as the facial recognition data already collected) careful attention will need to be paid to the extended use of that data and putting in place appropriate privacy and security arrangements. The Law Council draws your and the Department's attention to the following Law Council submissions, which may be assistance in the context of the Review:

   - Submission to the Senate Legal and Constitutional Affairs Committee regarding Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 (10 April 2018);[1]

   - Submission to the Parliamentary Joint Committee on Security and Intelligence regarding the review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (21 March 2018);[2]

   - Submission to the Parliamentary Joint Committee on Law Enforcement on the Inquiry on the impact of new and emerging information and communications technology on Australian law enforcement agencies (6 February 2018);[3]

Definition of 'identity' information

7. The Law Council considers it would be important to define what is meant as 'identity' information. There is currently a live debate as to what data is required for what purpose and what can be multiple purposes. For example, the information required to transact and access an *entitlement* (commercial or otherwise) merely requires that the person or party seeking to interact is entitled to do so. This is different to collecting information that is more extensive and captures more detail, some of which highly sensitive. Reference was made in the consultation sessions as to the concept of a

[1] Law Council of Australia, Submission No 10 to Senate Legal and Constitutional Affairs Committee, *Migration Amendment (Strengthening Biometrics Integrity) Bill 2015,* 10 April 2015.
[2] Law Council of Australia, Submission No 8 to the Parliamentary Joint Committee on Intelligence and Security, *Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018,* 21 March 2018.
[3] Law Council of Australia, Submission No 21 to the Parliamentary Joint Committee on Law Enforcement, *Impact of new and emerging information and communications technology on Australian law enforcement agencies,* 6 February 2018.

'skinny identity' based on forms of biometrics currently available to Government. This requires more detail and further consultation. Related to that is the concept of collecting data for multiple purposes, some purely commercial and some compliance related. The Law Council queries what identity information is in a hybrid context. For example, the name and identity documents for a Know Your Customer (**KYC**) check attaching to provision of services that, in the absence of regulation and law enforcement objectives, can be delivered based on a pseudonym or some form of proof of entitlement not related to identity. The detailed additional information is required for compliance obligations imposed by law, not by the nature of the particular commercial transaction itself.

Biometric data and privacy considerations

8. It is important to address the inherent complexity of using biometric data as proof of identity. As noted in the roundtable sessions, any data base relying on biometric data will need stringent privacy and security controls. Specifically, in relation to privacy, it will need protection for future uses currently unspecified but will become apparent as data is collected and used. New data will find new uses. The Law Council queries what protections are to be offered against such function creep, and whether these be different in the private and public sectors.

9. Use of biometric data will need to specifically address that such data cannot be changed post compromise given its direct link to the biological features of any given individual. Further, collection and use of such data involves a degree of physical intervention (e.g. collection of various samples). It is not clear as to how this is proposed to be addressed in addition to information privacy. The Law Council has on a number of occasions recommended the introduction of a new role as part of the data protection regime – a Biometric Information Commissioner, similar to the Commissioner for the Retention and Use of Biometric Material in the United Kingdom.[4] Further consideration should be given to these considerations.

Changes in technology

10. Technology, particularly information technology, is moving very quickly and many sectors, such as Fintech have been early adopters of these technologies. The Law Council questions how this will be addressed in the framework under consideration, to ensure that any given solution can be scaled and not be outdated or superseded shortly after implementation.

Recent changes to the data regime

11. Industries such as financial services and telecommunications will need to be considered in the context of pending changes in the data regime to be brought about by the introduction of open banking in 2019 in the banking community and its subsequent expansion to other industries as planned. This is relevant as businesses within the scope of the new consumer data right are likely to exchange large volumes of information and do so based on notions of consent assuming that the person authorising the transfer is duly authorised or entitled to make such a request or issue the instruction.

[4] Law Council of Australia, Submission No 8 to the Parliamentary Joint Committee on Intelligence and Security, *Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018,* 21 March 2018, 8.

Law Institute of Victoria recommendations

12. The Law Institute of Victoria makes the following additional recommendations in relation to the Review:

- the National Identity Security Strategy (**NISS**) should be significantly updated regarding the relevance of technology, use case, and human behaviour;
- updates to the NISS should be informed by studies of other countries that have existing or recently implemented digital identity services;
- when updating the NISS relevant standards should be considered as guides, including the most up to date versions of: Australian Government Information Security Manual (managed by the Australian Signals Directorate), the National Institute of Standards and Technology, and ISO27001;
- rigorous Privacy Impact Assessments be conducted when increasing the modalities of biometrics, as occurred in relation to the Document Verification Service;
- rigorous oversight provisions be enacted to control how the Facial Verification Service is accessed and used across government agencies;
- the Department conduct extensive public consultations as part of any consideration to allow access of biometric data by private entities;
- the Department improve transparency around the potential for data capture to be extended beyond passport, visa, citizenship, and driver licence images;

  the Department consider the need to regulate the private sector in relation to the provision of identity related services to ensure minimum standards;
- as a basic principle, private sector providers of identity related services should only retain the metadata associated with the verification of documents and not retain the actual source documents;
- the Department should consider how the private sector is to manage and have access to information held by the National Identity Security Coordination group, for example, the banking sector and real estate agencies that require verification of identity (**VOIs**) for simple things like lease agreements;
- requirement of verification of identity due to PEXA (an electronic conveyancing service) should be done by licensed conveyancers and law firms should be tied in to this framework and have a coherent framework across the board;
- Private/public cooperation be required in relation to the VOI framework and procedures (used, for example, in electronic conveyancing), in order to protect personal information stored and prevent cybercrime;
- the Department consider the applicability of Guidelines and Standards to VOI;
- the Department consider the use of other standards for the VOI framework, such as ISO/IEC 27001:2013, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security

management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature;

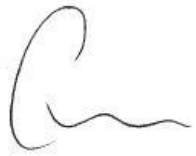
- in relation to the prevention of identity theft, security by design guidelines for private sector manufacturers and service providers should be promoted; and
- there be a review of current practices such as modern passwords with chips and biometric data, and Department of Human Services' functions that are all linked via my.gov.au including Medicare, the Australian Taxation Office, and Centrelink;

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 (02 6246 3754 or at natasha.molt@lawcouncil.asn.au), in the first instance should you require further information or clarification

Yours sincerely



Morry Bailes
President