Law Council
OF AUSTRALIA

Migration Amendment (Strengthening Biometrics Integrity) Bill 2015

Senate Legal and Constitutional Affairs Committee

10 April 2015

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

Acknowledgement

The Law Council acknowledges the assistance of its Business Law Section's Privacy Law Committee, Migration Law Committee, National Criminal Law Committee, National Human Rights Committee, the Law Institute of Victoria and the Law Society of South Australia in the preparation of this submission.

Executive Summary

1. Thank you for the opportunity to provide comments to the Senate Legal and Constitutional Affairs Committee's Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 (the Bill) Inquiry.

2. The Bill will expand existing powers of collection of personal information, including sensitive biometric data, for both Australian citizens and non-citizens.

3. The Law Council has limited its comments in this submission to three key issues:

    - the broad new collection power;
    - privacy impacts of greater collection; and
    - special issues with collection of biometric data from asylum seekers, children and incapable persons.

4. The Law Council's key recommendations include that:

    (a) The Bill not be passed until Parliament and the Australian community have the opportunity to consider the results of a privacy impact statement on the Bill conducted by the Privacy Commissioner;

    (b) The Bill should exhaustively define the purposes for which personal identifiers are collected, the types of personal identifiers that may be collected and how identifiers must be provided;

    (c) The Bill should be amended so that one or more personal identifiers can only be required from an individual where the Minister or DIBP/ACBPS officer reasonably believes that the person has or will breach or potentially breach an Australian law or the individual may pose a threat to national security.

    (d) The Privacy Commissioner should conduct a review as to whether current obligations to store biometric data securely are sufficient or whether increased security for the data set is required;

    (e) The Bill be amended to require the Department of Immigration and Border Protection (DIBP) to encrypt retained biometric information;

    (f) Current provisions allowing for the indefinite retention of certain identifying information should be removed;

    (g) The Privacy Commissioner and the public should be consulted on appropriate periods of time for the retention of biometric data;

    (h) The Bill be amended to provide for additional security measures reflecting the sensitivity of the information collected and expressly address the requirement to notify the individual and Privacy Commissioner for data breach notification in the event of a breach;

    (i) The *Migration Act 1958* (Cth) (Migration Act) should include a requirement to notify individuals affected as to how the biometric information may be handled and for what purposes it may be used;

    (j) The DIBP should liaise with the United Nations High Commissioner for Refugees about the appropriate safeguards that could be employed to ensure

the protection of biometric information for asylum seekers and refugees under Australia's jurisdiction;

(k) Specific guidelines should be implemented and published in relation to obtaining biometric information from children, to ensure that information is obtained in a respectful way, including ensuring that younger children are not separated from their parent, guardian or independent person unnecessarily;

(l) The Explanatory Memorandum should be amended to clarify the number of children and the threat younger children may pose which justifies the amendments to no longer require the consent and presence of a parent, guardian or independent person and to change the age for consent from 15 to 5 years of age;

(m) An independent guardian should be appointed to an unaccompanied minor if biometric information is required to be taken from the minor under the Migration Act;

(n) Guidance be provided in the Bill on what criteria need to be satisfied before a person is assessed as 'incapable' and that the Government consult with stakeholders in the disability and trauma sector on what criteria should be used; and

(o) Safeguards should be provided in the Bill to ensure adequate protection of all people affected by the legislation, including vulnerable groups. Policy guidance should then be issued to departmental officers as to how to ensure compliance with the legislative protections.

Introduction

5. The Government has stated that biometric checks at Australia's air and seaports will enable rapid identity verification with domestic and international security, law enforcement and immigration agencies through portable, hand-held devices.[1] This is said to help tackle identity fraud and disclose security and criminal histories to protect against the spread of terrorism and human trafficking including children.[2]

6. The Bill has been partly introduced in the context of national security concerns.[3] The Explanatory Memorandum to the Bill notes that Australia's 10 year-old biometric legislative framework needs to be updated and simplified to provide officers with the tools to more effectively meet current border and terrorism-related threats and to keep pace with advances in biometric technology.[4]

7. In particular the Bill reforms the collection of 'personal identifiers' from individuals.[5] A 'personal identifier' is based on individual physical characteristics, such as facial

[1] Minister for Immigration and Border Protection, *Greater Protection at Australia's Borders*, Media Release, 5 March 2015 at http://www.minister.immi.gov.au/peterdutton/2015/Pages/greater-protection-aus-borders.aspx
[2] Ibid.
[3] Explanatory Memorandum to the Bill, p. 42.
[4] Ibid, p. 1. In August 2014, the Prime Minister also stated that biometric screening will be introduced at airports within 12 months – see http://www.smh.com.au/federal-politics/political-news/tony-abbott-announces-new-counterterrorism-units-for-major-australian-airports-20140827-1091m6.html.
[5] Defined in current subsection 5A(1) of the *Migration Act 1958* (Cth).

image, fingerprints and iris, which can be digitised into a biometric template for automated storage and checking.[6]

New broad collection power

8. The Bill will insert section 257A into the Migration Act which will replace the current provisions that authorise the collection of personal identifiers.[7] The policy intention, as explained in the Explanatory Memorandum, is that there should not be limitations on the:

    - type of personal identifiers required from persons entering Australia; or
    - particular circumstances in which personal identifiers can be collected from persons, as is currently the case.

9. The Explanatory Memorandum notes that this is to enable DIBP to 'effectively and quickly collect personal identifiers in response to emergent risks based on individual circumstances, recent events and detected or realised threats'.[8]

10. Under new subsection 257A(1) a person can be required to provide one or more personal identifiers for any purposes of the Migration Act or Migration Regulations, including, but not limited to, persons who are:

    - citizens and non-citizens at the border seeking to enter or depart Australia;
    - unauthorised maritime arrivals who have not lodged an application for a visa;
    - non-citizens who are applicants for temporary or permanent protection visas, or any other visa of a class that is designated as a class of humanitarian visas;
    - non-citizens who are applicants for any other class of visa created under the Migration Act or the Migration Regulations; and
    - visa-holders, who are the subject of identity fraud allegations.

11. Policy guidance will be issued to officers exercising power under subsection 257A(1).[9]

12. Under new subsection 257A(1), a person can be required to give any type of personal identifier listed in subsection 5A(1), or prescribed in the Migration Regulations under paragraph 5A(1)(g) (other than an identifier which would require an intimate forensic procedure[10]).

13. The Law Council and the Law Institute of Victoria (LIV) consider that the power to prescribe both a purpose for which personal identifiers may be collected and the collection of biometric data via regulation raises the potential for the scheme to go beyond the initial intention of the Bill and the Migration Act, without adequate parliamentary scrutiny. Permitting the purposes and collection of biometric data to be increased by regulation is not sufficiently defined to allow people to know the extent of the restrictions on their rights and freedoms and for them to know their legal

[6] Explanatory Memorandum to the Bill, p. 1.
[7] Ibid.
[8] Ibid, p. 18.
[9] Ibid, p. 19.
[10] Within the meaning of section 23WA of the *Crimes Act 1914* (Cth).

obligations. The Law Council's *Rule of Law Principles* provide that the law must be readily known, available, certain and clear.[11]

14. The Law Council's *Rule of Law Principles* also require that where legislation allows for the Executive to issue regulations, the scope of that delegated authority should be carefully confined and subject to Parliamentary supervision.[12] Such a requirement ensures that Executive powers are defined by law, such that it is not left to the Executive to determine for itself what powers it has and when and how they may be used.[13]

15. As a matter of good legislative practice, significant matters should be specified in primary legislation which generally undergoes extensive consultation, not potentially subject to change by Ministerial decision and regulation.[14] The categories of biometric data, and the purposes for which it should be collected, will raise significant questions of policy and have substantial privacy implications. Given that citizens and non-citizens will be required to provide one or more personal identifiers that are sensitive information under the *Privacy Act 1988* (Cth) (the Privacy Act),[15] it is inappropriate for the types of biometric data to be prescribed by regulations.

16. An indeterminate biometric data set and range of purposes for which it may be collected fails to allow for a full Parliamentary consideration of the necessity and proportionality of the scheme. The type of biometric data, which can be stored and disclosed in certain circumstances, is a central and fundamental concern for Parliament in deciding whether the Bill should be enacted. This concern is heightened as the data is 'sensitive information' and collected outside the traditional environment where consent is freely given.

17. Ministerial expansion of the purposes for collection and the types of biometric data collected is also concerning as there are no security protections specified in the Bill for data collected or protection from expanded and unintended secondary uses or 'function creep'.

18. A Parliamentary process should consider any subsequent diminution of civil rights caused by increased scope of the collection scheme. While there is a prohibition against an 'intimate forensic procedure' under section 23WA of the Crimes Act,[16] there is no such limitation regarding 'non-intimate forensic procedures' under that Act. This means that there is the ability for the Minister to prescribe by way of regulation that the following types of biometric data can be required from an individual:

    (a) an examination of a part of the body other than the genital or anal area, the buttocks or, in the case of a female or a transgender person who identifies as a female, the breasts, that requires touching of the body or removal of clothing;

---

[11] Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011, Principle 1. See also Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Guidance Note 1: Drafting statements of compatibility* (2014) 1.
[12] Ibid, Principle 6(a).
[13] Ibid, Principle 6.
[14] Senate Standing Committee for the Scrutiny of Bills, *Alert Digest,* No 16 of 2014, 26 November 2014, 3; Peter Leonard, *Internet Data Retention in Australia – A Quick (but Deep) Dive into the new Bill*, (Gilbert and Tobin Lawyers, November 2014) 3.
[15] This means that agencies are only able to collect sensitive biometric information about an individual in defined circumstances, including where: the individual has consented to the collection; the collection is authorised or required by or under law, or the collection is necessary to prevent a serious threat to the life, health or safety of any individual – see Australian Privacy Principle 3 in Schedule 1 of the *Privacy Act 1988* (Cth).
[16] See section 5A(1) of the *Migration Act 1958* (Cth).

(b) the taking of a sample of blood by a finger prick;

(c) the taking of a sample of saliva, or a sample by buccal swab;

(d) the taking of a sample of hair other than pubic hair;

(e) the taking of a sample from a nail or under a nail;

(f) the taking of a sample by swab or washing from any external part of the body other than the genital or anal area, the buttocks or, in the case of a female or a transgender person who identifies as a female, the breasts;

(g) the taking of a sample by vacuum suction, by scraping or by lifting by tape from any external part of the body other than the genital or anal area, the buttocks or, in the case of a female or a transgender person who identifies as a female, the breasts;

(h) the taking of a foot print or toe print;

(i) the taking of a photograph or video recording of, or an impression or cast of a wound from, a part of the body other than the genital or anal area, the buttocks or, in the case of a female or a transgender person who identifies as a female, the breasts.

19. Arguably, scrutiny by the Senate Rules and Ordinances Committee and the regulation disallowance process provides a mechanism for addressing these concerns. However, a regulation can have effect from the date of registration and it may be weeks or months before a disallowance motion may be tabled or considered by the Parliament.

20. A similar issue arises in terms of there being inadequate legislative restrictions on how a Minister or an officer may require a personal identifier to be provided. Paragraph 257A(5)(b) would provide a new power for the Minister or an officer to require that personal identifiers be provided in 'another way'. As explained in the Explanatory Memorandum, this will provide flexibility about how a person is to provide personal identifiers when required to do so.[17] However, the current system of safeguards applying to the collection of personal identifiers by means of an identification test, such as not involving the removal of more clothing than is necessary for carrying out the test and affording reasonable privacy to the person,[18] will be able to be bypassed where an officer or the Minister authorises a different method of collection.

21. While the Explanatory Memorandum contemplates that mobile fingerprint scans will be an authorised different method of collection of personal identifiers, [19] paragraph 257A(5)(b) is broadly drafted so that the Minister or officer has a wide discretion as to how a personal identifier must be provided. Given the potential intrusiveness of particular methods of requiring a personal identifier from a person, particularly where current safeguards do not apply, the Bill should clearly set out the manner in which a personal identifier should be provided and how that information is to be safeguarded from misuse and unauthorised access once so collected.

22. Further, the power for the Minister or an officer to require a citizen to provide one or more personal identifiers at the time they are entering Australia, are travelling on an

[17] Explanatory Memorandum to the Bill, p. 37.
[18] See section 258E of the *Migration Act 1958* (Cth).
[19] Explanatory Memorandum to the Bill, p. 37.

overseas vessel from port to port, or when they are departing Australia[20] has the potential to impact on the travel and privacy of citizens who may not even be suspected of contravening an Australian law or posing a risk to national security. For that reason, while a wide range of personal identifiers may be required, the highly personal nature of such data should not be underestimated and its use and retention ought to be tightly controlled. Consequently, there should be a threshold test for requiring one or more personal identifiers from an individual only where the DIBP and ACBPS officer reasonably believes that the person has or will breach or potentially breach an Australian law or the individual may pose a threat to national security.

Recommendations:

- **The Bill should exhaustively define the purposes for which personal identifiers are collected and the types of personal identifiers that may be collected. The power to prescribe these matters by way of regulation should be removed from the Bill.**
- **The Bill should exhaustively define how personal identifiers must be provided rather than permitting the Minister or an officer to make such a determination.**
- **The Bill should be amended so that one or more personal identifiers can only be required from an individual where the Minister or DIBP/ACBPS officer reasonably believes that the person has or will breach or potentially breach an Australian law or the individual may pose a threat to national security.**

Privacy Impact

Privacy Impact Assessment

23. The Statement of Compatibility to the Bill acknowledges that the Bill 'will allow more widespread collection of personal identifiers' and that there is a 'negative impact on privacy'.[21] Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy. To the extent that there is a restriction on an individual's right to privacy, any interference must be reasonable, necessary and proportionate. The Law Council agrees with the Privacy Commissioner that:

> *… biometric information is about a person's physical characteristics. When we collect biometric information from a person, we are not just collecting information **about** that person, but information **of** that person.*
>
> *Biometric information cuts across both information privacy and physical privacy. It can reveal information about us, including information about our health, genetic background and most importantly, it is **intrinsic** to each of us.…*
>
> *Enjoying the benefits of biometric technologies does not also mean we have to give up other freedoms or rights. Biometric technology has a lot to offer. Let's*

[20] See sections 257A(3), 166, 170 and 175 of the *Migration Act 1958* (Cth).
[21] Explanatory Memorandum to the Bill, p. 41.

take responsibility to develop biometric systems carefully so that they achieve their aims while protecting privacy.

… the development and use of biometric technologies has the potential to impinge on individual privacy and thereby risk undermining community confidence in such technologies. Once that community confidence evaporates, so too does much of the potential that might have made the technologies attractive in the first place. This is why it is important to address and build in privacy now.[22]

24. The Privacy Commissioner noted that one way to build privacy in is for agencies to conduct a Privacy Impact Assessment (PIA) when commencing biometric projects that are likely to impact on privacy.[23]

25. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) considered proposed amendments to expand biometric data collection when it reviewed the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* and made the following recommendation:

The Committee recommends the Government consult with the Privacy Commissioner and conduct a privacy impact statement prior to proposing any future legislative amendments which would authorise the collection of additional bio-metric data such as fingerprints and iris scans.[24]

26. Relevantly, the PJCIS noted that, while it was 'generally supportive' of the amendment, the quantity of sensitive personal information proposed to be collected, stored, shared and used by government agencies meant a review of the measure taken to protect the privacy of the information was required.[25]

27. There is no indication of a PIA having been conducted or public release of results from consultation with the Privacy Commissioner on the privacy impacts flowing from this Bill. Further, it appears that the Parliament is being asked to consider this Bill, before it can assess the Privacy Commissioner's privacy impact statement of the data collected and stored by DIBP and the Australian Customs and Border Protection Service as a result of a recommendation of the PJCIS on the Foreign Fighters Bill, with the result to be reported to the Attorney-General by 30 June 2015.[26]

Recommendations:

- **The Bill not be passed until Parliament and the Australian community have the opportunity to consider the results of:**
  - **the privacy impact statement of the data collected and stored by the DIBP or Customs (as a result of a recommendation of the PJCIS on the Foreign Fighters Bill); and**
  - **a privacy impact statement on the Bill conducted by the Privacy Commissioner.**

[22] Speech by Timothy Pilgrim, Privacy Commissioner, Privacy in Australia: Challenges and Opportunities, to Biometrics Institute, 27 May 2010 available at http://www.oaic.gov.au/privacy/privacy-archive/privacy-speeches-archive/privacy-in-australia-challenges-and-opportunities
[23] Ibid.
[24] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, October 2014, p. 185, Recommendation 36.
[25] Ibid, p. 183.
[26] Ibid, Recommendation 34.

Obligations relating to biometrics information

28. Given that individuals may be obliged to provide identifying information to the DIBP including ACBPS,[27] strong protections should be implemented around the use, handling and disclosure of biometric information. This is an essential component of ensuring community confidence in biometric information handling practices.

29. Two overlapping legislative frameworks currently apply to biometric information obtained under the Migration Act:

    - the Australian Privacy Principles (APPs) provide general limits around how Australian government agencies handle personal information; and

    - Part 4A of the Migration Act, which specifies how a person may handle 'identifying information', which includes biometric information.

30. Part 4A of the Migration Act governs access, disclosure, modification and destruction of identifying information that has been collected and is held by DIBP. These safeguards should be strengthened in a number of respects and in light of the Bill's proposed amendments.

31. The Law Council also notes that DIBP in conjunction with the Attorney-General's Department and the Privacy Commissioner conducted a *Review of Personal Identifier Provisions Introduced In 2004 to the Migration Act 1958* (11 September 2009) (the PIP Review). While some suggestions in this review have been adopted, such as considering biometric information as 'sensitive information' for the purposes of the Privacy Act, the then Government and the current Government have not produced a formal response to the review.

32. The result is implementation of some of the PIP Review's findings without explanation as to why other recommendations or suggestions have been rejected. A prompt response is now required.

Recommendation:

- **The Government should respond promptly to the Review of Personal Identifier Provisions Introduced In 2004 to the Migration Act 1958 (11 September 2009).**

Security

33. Whether or not biometric information is effectively secured is critical to assessing whether the Bill's scheme is proportionate. Currently, obligations of personal information security for biometric data include:[28]

    (a) APP 11 requires that Government agencies, such as DIBP that holds personal information, to take reasonable steps to protect the information from **misuse**, **interference** and **loss**, as well as **unauthorised access**, **modification** or **disclosure.**

[27] See the Australian Border Force Bill 2015 and the Customs and Other Legislation Amendment (Australian Border Force) Bill 2015 which will combine the current DIBP with the ACBPS.
[28] As indicated from the Office of the Australian Information Commissioner's *Guide to Securing Personal Information: Reasonable Steps to Protect Personal Information*, January 2015, p. 4.

(b) Under the *Public Governance, Performance and Accountability Act 2013* (Cth), Australian Government agencies must also act in a way that is not inconsistent with the policies of the Australian Government.[29]

(c) Offence provisions in Part 4A of the Migration Act[30] may also encourage identifying information to be stored securely.

34. The collection of larger quantities and a broader range of biometric information create a risk that the data may be misused through unauthorised access and the risk of identity theft and fraud as a result of data breaches.

35. In 2014, DIBP was the subject of a data breach in which the personal details of nearly 10,000 asylum seekers were mistakenly made available on the Department's website.[31] On 30 March 2015 it was also reported that DIBP had inadvertently disclosed the passport and visa details of world leaders attending the G20 summit in Brisbane.[32] As the Sydney Morning Herald reported last year:

> *Privacy advocates are particularly worried about the consequences of biometric data being hacked because, unlike a passport or a tax file number, it cannot be changed*.[33]

36. This illustrates the importance of securing strong safeguards for the collection, use and disclosure, security and destruction of biometric data.

37. On this basis, there is a need for the Privacy Commissioner to conduct a review as to whether current obligations to store biometric data securely are sufficient or whether increased security of the data set is required. For example, the review could examine the appropriateness of requiring the biometric data collected to be quarantined and kept separate from other data sets.

38. Mandatory encryption of any biometric data retained is also a necessary and appropriate measure to secure retained data. This requirement should be included in the Bill as it would assist in ensuring individuals that their privacy and security is maintained.

Recommendations:

- **The Privacy Commissioner should conduct a review as to whether current obligations to store biometric data securely are sufficient or**

[29] Under section 21 of the *Public Governance, Performance and Accountability Act 2013* (Cth) the accountable authority of a non-corporate Commonwealth entity must govern the entity in accordance with paragraph 15(1)(a) in a way that is not inconsistent with the policies of the Australian Government. From the security perspective these policies include the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual.* These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government.

[30] Such as accessing identifying information (section 336C of the Migration Act) and disclosing identifying information (section 336E of the Migration Act).

[31] Immigration slammed for privacy breach which saw asylum seeker records released, New Matil-da, 12 November 2014 https://newmatilda.com/2014/11/12/immigration-slammed-privacy-breach-which-saw-asylum-seeker-records-released.

[32] See: http://www.theguardian.com/world/2015/apr/01/g20-leaders-details-leak-new-privacy-taskforce-announced.

[33] Opposition grows to storage of photo and biometric data, SMH, 15 October 2014 http://www.smh.com.au/federal-politics/political-news/opposition-grows-to-storage-of-photo-and-biometric-data-20141015-116lur.html.

whether increased security for the data set is required.

- **The Bill be amended to require the DIBP to encrypt retained biometric information.**

Retention period

39. Under section 336K of the Migration Act, a responsible person for identifying information commits an offence, punishable by up to two years imprisonment, or 120 penalty units, or both, for failing to destroy the information as soon as practicable after the person is no longer required to keep it under the *Archives Act 1983* (Cth).

40. However, section 336L of the Migration Act provides for the indefinite retention of identifying information, including for individuals who have been in immigration detention. The Law Council considers, as did the Privacy Commissioner, that in the absence of a clear and specific need for retaining identifying information, it should not be held indefinitely.[34] The Privacy Commissioner and the public should be consulted on appropriate periods of time for the retention of biometric data.

Recommendations:

- **The DIBP should be transparent about what biometric information it retains or requires to be retained and for how long.**
- **Current provisions allowing for the indefinite retention of certain identifying information should be removed.**
- **The Privacy Commissioner and the public should be consulted on appropriate periods of time for the retention of biometric data.**

Destroying identifying information

41. The offence under section 336K of failing to destroy biometric information does not apply if the identifying information is a personal identifier relating to a person's height and weight, a photograph or other image of a person's face and shoulders, a person's signature or identifying information derived from or relating to such a personal identifier. It is not immediately apparent as to why such information is treated differently as it can still be used to re-identify an individual at a later time. Much of this information cannot be changed or updated in the event of a breach.

Recommendation:

- **The Committee should be satisfied that the exceptions under section 336K that currently permit certain types of biometric information not to be destroyed are justified as necessary, reasonable and proportionate and that the distinctions made between different data elements are equally justified as reasonable in the circumstances.**

[34] As noted in the Department of Immigrations and Citizenship's *Final Report: Review of Personal Identifier Provisions Introduced in 2004 to Migration Act 1958*, 11 September 2009, p. 52.

Disclosure for the enforcement of criminal law

42. Subsection 336E(2) of the Migration Act sets out a wide range of circumstances where a disclosure may be permitted including where it is reasonably necessary for the **enforcement** of the criminal law of the Commonwealth or of a State or Territory.[35] However, subsection 336E(3) sets out limitations on what constitutes a permitted disclosure. A disclosure is not a permitted disclosure if it is for the purpose of using a prescribed type of personal identifier in **investigating, or prosecuting** a person for, an offence against a law of the Commonwealth or a State or Territory. It is not clear, as noted in the PIP review, why this provision and corresponding provisions in subsection 336D(3) were inserted into the Act.[36]

43. The Law Council considers that the Explanatory Memorandum to the Bill should provide greater clarity around the difference between permitted uses and disclosures under paragraph 336E(2)(ea) and disclosures prohibited under subsection 336E(3).

Recommendation:

- **The Explanatory Memorandum should more clearly explain the difference of allowing uses and disclosures for the enforcement of the criminal law but not for investigating, or prosecuting a person for, an offence.**

Disclosure to foreign countries

44. Section 336F of the Migration Act authorises the disclosure of identifying information to foreign countries or specified bodies in other countries or international organisations for a broad range of purposes set out in subsection 5A(3). The Law Council suggests, as has the Privacy Commissioner, that it would be appropriate to include a mechanism in the Migration Act to ensure that the foreign country will handle this information appropriately.[37]

45. The PIP Review noted that this may involve, for example, establishing administrative arrangements, undertakings, memorandums of understanding or other protocols with the foreign country regarding the personal information handling practices for personal information transferred to that country under section 336F. [38] The review also noted that such arrangements should be publicly available and include easily accessible complaint handling and accountability mechanisms.[39]

46. However, given the sensitivity of biometric information, there should also be an express legislative provision in the Migration Act that only permits disclosure to a foreign country or agency where it protects the information in a way that is consistent with the APPs.

Recommendation:

- **There should be an express legislative provision in the Migration Act that only permits disclosure to a foreign country or agency**

[35] Paragraph 336E(2)(ea) of the *Migration Act 1958* (Cth).
[36] Department of Immigrations and Citizenship's *Final Report: Review of Personal Identifier Provisions Introduced in 2004 to Migration Act 1958*, 11 September 2009, p. 57.
[37] Ibid, p. 52.
[38] Ibid, p. 62.
[39] Ibid.

where it protects the information in a way that is consistent with the APPs.

Mandatory data breach notification

47. A large repository of biometric information increases the risk and possible consequences of a data breach. The large volume of biometric information held by the Government will be an attractive resource for people with malicious intent. Notification to individuals affected by a data breach involving biometric information would be essential for them to seek legal remedies and mitigate any possible unintended consequences.

48. For this reason, the Law Council recommends that the Bill be amended to include an obligation for the DIBP to notify the Privacy Commissioner and affected individuals in the event that there is a data breach affecting biometric data collected and retained.

Recommendation:

- **The Bill be amended to provide for additional security measures reflecting the sensitivity of the information collected and expressly address the requirement to notify the individual and Privacy Commissioner for data breach notification in the event of a breach.**

Notification of the purposes for which the information may be used

49. The Law Council agrees with the PIP Review that:

> *The fundamental protection should be that the person supplying information should be notified of the purposes for which the information may be used with as much particularity as is possible having regard to the need to keep notices simple.*
>
> *This will ensure that the authorisation does not inadvertently facilitate the use or disclosure of personal information in a broader range of circumstances than was intended*.[40]

50. A legislative requirement to notify individuals of how their biometric information may be handled, and for what purposes it may be used, would assist the DIBP to meet its obligations under APP 5. Clear information should be provided to those affected by the collection and use of biometric material, which may include:

(a) the use of examples;

(b) providing details of the particular domestic or international agencies that may have access to this data;

(c) providing information about the application of the Privacy Act and the role of the Privacy Commissioner; and

(d) how to make a complaint about misuse of information.

[40] As noted in the Department of Immigrations and Citizenship's *Final Report: Review of Personal Identifier Provisions Introduced in 2004 to Migration Act 1958*, 11 September 2009, p. 72.

51. In the specific context of the proposed mobile fingerprint scan the Explanatory Memorandum indicates:

> *The scans will be conducted in public, with information about the purpose of the scan, what the scan involves, and that data will not be retained after the scan is complete communicated verbally by an officer*.[41]

52. Where an individual has difficulty understanding the information due to cultural or other reasons, the information should be provided in written form and in the person's language of origin. The Government should also consult with the Privacy Commissioner in the preparation of such explanatory material.

Recommendations:

- **The Migration Act should include a requirement to notify individuals affected as to how the biometric information may be handled and for what purposes it may be used.**
- **Notification should be issued verbally and where necessary in written form and in the person's language of origin.**
- **The Government should also consult with the Privacy Commissioner in the preparation of explanatory memorandum to be used by staff when notifying individuals.**

Information privacy and bodily privacy

53. Privacy implications of biometric technologies were considered by the Australian Law Reform Commission (ALRC) as part of its review of the Privacy Act in its report *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108).[42]

54. As noted, the collection, use and security of biometric data is about information and bodily privacy. Under the current privacy regime, substantive protections and the enforcement powers of the Privacy Commissioner are exclusively focused on information privacy. Given the far reaching privacy implications of collection use and disclosure of biometric data, consideration should be given to appropriate expansions in the protections afforded to the biometric data beyond information rights in that data.

55. To that end, the functions conferred on the Office of the Biometric Commissioner in the United Kingdom (UK)[43], includes a Commissioner for Retention and Use of Biometric Data. The structure is established pursuant to the *Protection of Freedom Act 2012* (UK).[44] The Commissioner has oversight of a number of agencies that regularly use and share biometric data and includes agencies dealing with local crime and law enforcement, national security and immigration related matters.

Recommendation:

- **Consideration should be given to a review of the Privacy Commissioner's**

[41] Explanatory Memorandum to the Bill, p. 37.
[42] http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20%28ALRC%20Report%20108%29%20/9-overview.
[43] The Office of the Biometric Commissioner in the United Kingdom was created in 2013.
[44] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387601/45428_Biometrics_Annual_Report_ACCESSIBLE.PDF.

powers, to ensure that the Privacy Commissioner has adequate powers to deal with matters involving bodily privacy (in addition to information privacy). The review should consider the merits of establishing an office holder dedicated to oversight of biometric related matters simular to the UK model.

Collection of biometric data from asylum seekers

56. The Law Council recognises the necessity of the use of biometric data, and also notes that there are benefits of the use of biometric data in the context of asylum seekers. For example, the United Nations High Commissioner for Refugees (UNHCR) uses biometrics for the purpose of safeguarding the identity of refugees on the basis that they often lose their identity documents during displacement.[45] UNHCR's use of biometric data 'is encouraged, *except* where no protection or operational benefit is expected to be gained from doing so.'[46] UNHCR notes that safeguards must be put in place, including in relation to the sharing of biometric information.[47] Further, UNHCR restricts the sharing of data for the purpose for which it was collected.[48]

57. Owing to UNHCR's mandate to protect refugees, it would be beneficial for the DIBP to liaise with UNHCR on the appropriate safeguards to ensure the protection of asylum seekers and refugees under Australia's jurisdiction. UNHCR can provide guidance on the use of biometric data for asylum seekers and refugees by reference to its *Policy on Biometrics* in refugee registration and verification and *Confidentiality Guidelines.*

58. Currently under the Migration Act, a request may be made for a range of personal identifiers.[49] As noted, the new broad power in section 257A will permit a wider range of personal identifiers to be requested in more circumstances. Unless the Minister makes a determination under new section 258, a person may be required to provide several personal identifiers to:

- be eligible to apply for certain visas[50];
- enter Australia[51];
- travel on an overseas vessel from a port to another port[52];
- depart from a place in Australia on a vessel[53];
- prove to an immigration officer that they are a lawful non-citizen[54]; or

[45] See: UN High Commissioner for Refugees, *Biometric Identity Management System: Enhancing Registration and Data Management*, available at: http://www.unhcr.org/cgi-bin/texis/vtx/home/opendocPDFViewer.html?docid=550c304c9&query=biometric.
[46] UN High Commissioner for Refugees, *UNHCR Resettlement Handbook, 2011*, 157 [4.7.4], available at: http://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=search&docid=4ecb973c2&skip=0&advsearch=y&process=y&allwords=&exactphrase=Policy%20on%20Biometrics%20in%20Refugee%20Registration%20and%20Verification%20&atleastone=&without=&title=&monthfrom=&yearfrom=&monthto=&yearto=&coa=&language=&citation=.
[47] Ibid.
[48] Ibid.
[49] See sections 40, 46, 166, 170, 175, 188 and 192 of the *Migration Act 1958* (Cth).
[50] Protection visas under sections 40 and 46 of the *Migration Act 1958* (Cth).
[51] Ibid, section 166.
[52] Ibid, section 170.
[53] Ibid, section 175.

- comply with an immigration officer who knows or reasonably suspects that a non-citizen holds a visa that may be cancelled[55].

59. One form of personal identifier requested may be non-fraudulent or official documentation. This requirement may be particularly problematic for asylum seekers who may rely on fraudulent documentation to leave a country where they are subject to persecution by the State[56].

60. The Law Society of South Australia (LSSA) expressed concern that under the Bill, the Minister may refuse a person a visa through section 40 or 46 of the Migration Act if the person refused to provide personal identifiers. The LSSA noted that in addition to needing to resort to the use of false documentation to ensure safe passage to seek asylum, asylum seekers could fear what may be a reasonable request to provide identifiers due to their own experiences in their countries of origin.

61. There is no indication of how such an issue would be resolved, and this could potentially lead to *refoulement* of asylum seekers, which is inconsistent with Australia's commitments under the *Convention relating to the Status of Refugees* and international human rights law.

62. The Law Council acknowledges the necessity of the collection of biometric data and supports its use provided that there are relevant safeguards in place. It considers that any use of biometric data on the basis of bogus documents provided by asylum seekers should contain safeguards that are consistent with those employed by UNHCR.

63. It is therefore important that Parliament consider the unique circumstances of refugees and asylum seekers in relation to the storage and use of biometric data. This would include a recognition that it may be inappropriate to contact countries of origin, from which asylum seekers may be fleeing persecution, to obtain such data.

64. The LSSA notes that for offshore applicants, the requirements to give personal identifiers which already exist for mainstream visas such as orphan relatives, child or partner visas, do not yet extend to humanitarian visas. They submit that already those requirements have proven extremely difficult for applicants in developing countries or in refugee camps and note their concern that if the requirements to provide identifiers were to extend to all humanitarian applicants, they may become inhibitive, and prevent genuine applicants from being given resettlement or reunification with family members in Australia.

65. The LSSA notes that there are no appeal avenues specific to the issue of personal identifiers apparent in the Bill.

[54] Ibid, section 188.
[55] Ibid, section 192.
[56] Law Council submission to Senate Committee on Legal and Constitutional Affairs re Migration Amendment (Protection Obligations and Other Measures) Bill 2014, 4 August 2014.

Recommendations:

- **The DIBP should liaise with the UNHCR about the appropriate safeguards that could be employed to ensure the protection of biometric information for asylum seekers and refugees under Australia's jurisdiction. In particular DIBP should adopt safeguards consistent with the UNHCR in relation to use of biometric data on the basis of bogus documents provided by asylum seekers.**

Collection of biometric data from children

66. The Bill provides that, when collecting personal identifiers from minors under section 257A, the consent and presence of a parent, guardian or independent person is not required, and proposes to change the age for consent from 15 to 5 years of age.[57]

67. The Law Council has concern that the provisions enabling officers to obtain biometric information from children without consent or without the presence of a parent, guardian or independent person may, in certain circumstances, not always be in the best interests of the child and have the potential to be inconsistent with recognised rights of children.[58] More particularly, it may also potentially place children in confronting and compromising situations without the aid of a responsible adult.

68. The Law Council suggests the Committee consider these provisions closely, particularly to determine whether such an approach is proportionate and necessary. If the Committee is convinced that this approach is warranted, the Law Council recommends that specific legislative protections and guidelines are implemented and published that aim to obtain this information in a respectful way, including ensuring that younger children are not separated from their parent, guardian or independent person unnecessarily.

69. The Explanatory Memorandum states the rationale for the collection of biometric data from children amendments as:

    (a) child smuggling/trafficking cases where minors have been brought into Australia, both with and without parental consent, as part of a family unit of which they are not a member;[59]

    (b) recent terrorist-related incidents that have focused attention on the involvement of minors in terrorist activity in the Middle East and Africa;[60] and

    (c) the age limit in the Migration Act is inconsistent with all other Five Country Conference Partners.[61]

[57] Clause 261AL(1) of the Bill.
[58] See for example – Article 16 of the United Nations *Convention on the Rights of the Child 1989* (CROC) provides that 'No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation' and that 'The child has the right to the protection of the law against such interference or attacks'. See also Article 37(b) relating to arbitrary deprivation of liberty.
[59] Explanatory Memorandum to the Bill, pp. 44-45.
[60] Ibid.
[61] Ibid.

70. The first reason is clear and understandable and the Law Council is aware of such cases occurring. However, the presence of an independent person is still required to ensure that personal identifiers are collected in an appropriate manner.

71. The second reason is unclear. The Explanatory Memorandum states that 'the conflict in the Middle East has provided evidence of involvement of children'.[62] However, it is unclear as to why this necessitates an amendment to no longer require the presence of a parent, guardian or independent person or to change the age for consent from 15 to 5 yeas of age. The Explanatory Memorandum should be amended to clarify the number of children and the threat younger children may pose which justifies these amendments.

72. The Law Council also queries the third justification for reducing the age limit on the basis that it would be consistent with the age limit of the Five Country Conference partners. The Five Country Conference, similar to the Five Eyes Partnership, is a grouping of Australia, Canada, New Zealand, the UK and the US to coordinate and work together on immigration issues. However, there is a key difference in terms of rights protection compared to those other countries. A notable omission in a Statement of Compatibility with Human Rights to the Bill, is that Australia, unlike the UK, Canada and New Zealand, does not have a human rights act, nor does it have the same degree of constitutional protection for human rights as the US (e.g. from the Fourth Amendment). This is significant difference in the protection of rights of the child.

73. A child may be incapable of understanding the nature and effect of biometric data collection due to age. Where a person does not understand the nature and effect of the collection, he or she cannot freely and fully consent to the collection. This means that it is vital that the rights of the child are protected.

74. In this context, the UK's *Immigration Act 2014* (UK) at section 13[63] amended the *Immigration Act 1971* (UK) to include certain safeguards for children under 16 years of age regarding biometric. These include a requirement that the biometric information is to be provided in the presence of the child's parent, guardian or a person who is temporarily taking responsibility of the child (excluding a person who is entitled to require the provision of information and an officer of the Secretary of State).

75. The Law Council reiterates its position that the *Immigration (Guardianship of Children) Act 1946* (Cth) is amended such that an independent guardian is appointed for unaccompanied minors, and that, if the Committee is minded to recommend the passage of the Bill, the Committee also recommend similar safeguards to protect minors as those that exist under the *Immigration Act 2014* (UK) insofar as they are consistent with Australia's commitments under the CROC.

Recommendations:

- **Specific guidelines should be implemented and published in relation to obtaining biometric information from children, to ensure that information is obtained in a respectful way, including ensuring that younger children are not separated from their parent, guardian or independent person unnecessarily.**
- **The Explanatory Memorandum should be amended to clarify the number of children and the threat younger children may pose which justifies the**

[62] Ibid, p. 45.
[63] See: http://www.legislation.gov.uk/ukpga/2014/22/part/1/crossheading/biometrics/enacted

amendments to no longer require the consent and presence of a parent, guardian or independent person and to change the age for consent from 15 to 5 years of age.

- **An independent guardian should be appointed to an unaccompanied minor if biometric information is required to be taken from the minor under the Act.**
- **Consideration should be given to amending the Bill to include safeguards to protect minors as set out in the *Immigration Act 2014* (UK) (insofar as they are consistent with Australia's commitments under the CROC).**

Collection of biometric data from incapable persons

76. The Law Council is concerned about the potential impact of the collection of biometric data from incapable persons and that this data may be used to discriminate against individuals in a manner that is inconsistent with recognised rights of persons with a disability.[64] The amendments provide that, when collecting personal identifiers from 'incapable persons' under new section 257A, the consent and presence of a parent, guardian or independent person is not required.

Criteria for assessing an individual as 'incapable'

77. Under section 65 of the Migration Act the Minister may grant or refuse visa applications on a number of grounds, including whether the health criteria has been satisfied. Schedule 4 of the Migration Regulation 1994 also sets out the 'public interest criteria' for granting residence visas, which includes a requirement that the applicant be free from a condition that the provision of the health care or community services would be likely to result in a significant cost to the Australian community.

78. Personal identifiers may be used to discriminate against a person with a disability or a mental illness[65] by requiring that person to undergo additional tests to determine if they meet the health requirements under the Migration Act and Regulations before granting a visa. This situation may arise in circumstances where a personal identifier is linked to information about an assessment by an officer that they are 'incapable' at the time of collecting the personal identifier.

79. The Bill and the Migration Act do not provide any clear guidance on what criteria should be met before a person is assessed as being 'incapable' for the purposes of collecting a personal identifier. The Migration Act provides that an '*incapable person* means a person who is incapable of understanding the general nature and effect of, and purposes of, a requirement to provide a personal identifier'[66]. The Migration Act provides that authorised officers must simply have reasonable grounds to believe that a person is incapable.[67]

[64] See *Convention on the Rights of Persons with Disabilities: Declarations and Reservations (Australia)*, opened for signature 30 March 2007, 999 UNTS 3 (entered into force 3 May 2008) and ratified by Australia on 17 July 2008.
[65] Disability covers both physical illnesses and other conditions as noted by the Joint Standing Committee on Migration final report on its *Inquiry into the Migration Treatment of Disability* (21 June 2010) 17.
[66] See section 5 of the *Migration Act 1958* (Cth).
[67] Section 258E(e) of the *Migration Act 1958* (Cth).

80. Given the significant impact that an officer's assessment of a person as 'incapable' may have on an individual, the Law Council considers that there should be clear legislative criteria setting out the circumstances for the assessment.

Recommendations:

- **Guidance be provided in the Bill on what criteria need to be satisfied before a person is assessed as 'incapable' and that the Government consult with stakeholders in the disability and trauma sector on what criteria should be used.**

Extraterritorial application of human rights obligations and offshore collection

81. The Explanatory Memorandum to the Bill notes that the *Convention on the Rights of Persons with Disabilities* (the Disabilities Convention) does not apply to the collection of personal identifiers offshore as it only applies to the territory of State Parties.[68]

82. Nonetheless, by ratifying the Disabilities Convention, Australia made commitments to recognise that persons with a disability enjoy legal capacity on an equal basis to others in all aspects of life, and to take appropriate measures to provide persons with disability access to the support they may require in exercising their legal capacity.[69] Further, while the Disabilities Convention does not apply to the collection of personal identifiers offshore such as in a regional processing centre, the Convention may nonetheless apply where it is used, disclosed or retained within the territory of Australia.

83. The Joint Standing Committee on Migration report, *Enabling Australia: Inquiry into the Migration Treatment of Disability* (21 June 2010), stated that while the Disability Convention is not enforceable on state parties, it requires that domestic law and government programs be in harmony with treaty obligations. In particular, Articles 4 and 5 require state parties to ensure laws are not in contravention to obligations for non-discrimination under the treaty.[70] In reaching this conclusion, the Committee referred to the High Court decision of *Minister for Immigration and Ethnic Affairs v Teoh*,[71] which established a principle that Government and its agencies will act in accordance with the terms of a treaty, even where those terms had not been incorporated into Australian law[72]

84. Australia has also made an interpretive declaration in relation to its obligations under the Disabilities Convention, in the following terms:

> *Australia recognizes the rights of persons with disability to liberty of movement, to freedom to choose their residence and to a nationality, on an equal basis with others. Australia further declares its understanding that the Convention does not create a right for a person to enter or remain in a country of which he or she is not*

[68] Explanatory Memorandum to the Bill, p. 39.
[69] See *Convention on the Rights of Persons with Disabilities: Declarations and Reservations (Australia)*, opened for signature 30 March 2007, 999 UNTS 3 (entered into force 3 May 2008) and ratified by Australia on 17 July 2008.
[70] Joint Standing Committee on Migration final report on its *Inquiry into the Migration Treatment of Disability* (21 June 2010) para 7.9.
[71] *Minister for Immigration and Ethnic Affairs v Teoh* (1995) 183 CLR 273, 288.
[72] Joint Standing Committee on Migration final report on its *Inquiry into the Migration Treatment of Disability* (21 June 2010) para 7.30.

a national, nor impact on Australia's health requirements for non-nationals seeking to enter or remain in Australia, where these requirements are based on legitimate objective and reasonable criteria.[73]

Recommendation:

- **The collection, and subsequent use of personal identifiers from 'incapable' people under the Bill, regardless of whether it is collected outside of Australia's territory, should be consistent with the *Convention on the Rights of Persons with Disabilities.***

Consent

85. As noted, the Bill negates the requirement for consent by a guardian or independent person in collecting personal identifiers from an 'incapable' person. While the use of force to obtain personal identifiers is not permitted against an 'incapable person',[74] it is nonetheless silent on whether the consent of the 'incapable' person themselves is required. For example, a personal identifier could be collected without the knowledge of an incapable person.

86. This is particularly concerning in light of the fact that the current criteria used to assess whether a person is 'incapable' is discretionary, i.e. that authorised officers must simply have reasonable grounds to believe that a person is incapable.[75]

87. This is problematic because it may be inconsistent with Article 12 of the Disabilities Convention which provides that people with disabilities should enjoy legal capacity to make decisions for themselves on an equal basis with others.

88. Article 12 also requires that persons with disabilities be given support in decision-making. This provision provides that where a person has a disability, for example, due to cognitive impairment, a State Party should do all it can to provide 'supports' to enable that person to make a decision or to provide consent.[76]

89. Support may involve a support person who provides the person with disability information in such as way that they can better understand the decision they are being asked to make. This is termed 'supported decision-making' and is the opposite to 'substituted decision-making' where a guardian makes a decision on behalf of a person with disability based on subject's 'best interests'.

90. The Government should ensure adequate support is given to 'incapable' people so that they can exercise legal capacity on an equal basis with others by either agreeing to or abstaining from providing personal identifiers. This is particularly important given the significant consequences of not providing personal identifiers.[77]

[73] Ibid.
[74] Pursuant to s261AE of the *Migration Act 1958* (Cth).
[75] Section 258E(e) of the *Migration Act 1958* (Cth).
[76] See http://www.un.org/disabilities/convention/conventionfull.shtml.
[77] These consequences include, for example, visa invalidity or refusal; refusal to enter Australia (i.e., the person would be refused immigration clearance and returned to the destination they embarked from); delayed departure from Australia; or immigration detention. See Explanatory Memorandum to the Bill, p. 37.

Recommendations:

- **That consent is sought from the 'incapable' person themselves where a guardian or independent person is not available to provide that consent on behalf of the 'incapable' person.**
- **The Government should ensure adequate support is given to 'incapable' people so that they can exercise legal capacity on an equal basis with others by either agreeing to or abstaining from providing personal identifiers.**

Safeguards as policy intent or guidance

91. The LIV and the Law Council are concerned that many apparent safeguards in the Bill exist only as 'policy intent' and therefore do not provide adequate express or specific protections. For example, as noted in the Explanatory Memorandum, the circumstances in which personal identifiers will be collected from minors and incapable persons will be set out in policy,[78] and that policy guidance will be issued to departmental officers to ensure that they exercise their discretion appropriately[79].

92. Safeguards should be provided in the legislation itself to ensure adequate protection of all people affected by the legislation, including vulnerable groups. Policy guidance should then be issued to departmental officers as to how to ensure compliance with the legislative protections. Policy guidance that is issued to departmental staff on collection of biometric data should also comply with the APPs. Appropriate training should also be provided to ensure that the implementation of the policy is also compliant with the APPs.

Recommendations:

- **Safeguards should be provided in the Bill to ensure adequate protection of all people affected by the legislation, including vulnerable groups. Policy guidance should then be issued to departmental officers as to how to ensure compliance with the legislative protections.**
- **Policy guidance that is issued to departmental staff on collection of biometric data should also comply with the APPs. Appropriate training should also be provided to ensure that the implementation of the policy is also compliant with the APPs.**

[78] Explanatory Memorandum to the Bill, p. 43.
[79] Ibid, p. 47.

Attachment A: Profile of the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Large Law Firm Group, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- The Large Law Firm Group (LLFG)
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2015 Executive are:

- Mr Duncan McConnel, President
- Mr Stuart Clark, President-Elect
- Ms Fiona McLeod SC, Treasurer
- Dr Christopher Kendall, Executive Member
- Mr Morry Bailes, Executive Member
- Mr Ian Brown, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.