Law Council OF AUSTRALIA

Office of the President

6 October 2023

Senator Nita Green
Chair
Senate Legal and Constitutional Affairs Legislation Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

By email: legcon.sen@aph.gov.au

Dear Senator

Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023 [Provisions]

1. The Law Council of Australia is pleased to make a submission to the Senate Legal and Constitutional Affairs Legislation **Committee** in response to its inquiry into the provisions of the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023 (the **Bills**).

2. The Law Council is grateful for the assistance of the Privacy Law Committee of its Business Law Section in preparing this submission. Regrettably, in the brief time available to provide views on the Bills, the Law Council has been unable to consult more broadly with its membership. The views expressed in this submission should, therefore, be considered preliminary.

3. It is troubling that such a short reporting period has been imposed on this inquiry, providing a little over two weeks for stakeholders to make submissions about a proposed legislative framework for identity verification services—services that have been utilised by government and industry for several years, without any apparent legislative basis.

4. This truncated consultation period of 12 business days is even more unfortunate, given the extent to which verification services are currently relied upon in Australia. It is critical that an appropriate balance is struck between the secure and efficient verification of identities, and the need for adequate privacy safeguards and oversight. The Law Council is concerned that the timeframe for this inquiry does not reasonably enable the Committee to carefully scrutinise whether the Bills strike the correct balance.

5. As noted in the Attorney-General's second reading speech on the Bill, the Document Verification Service (**DVS**) was used more than 140 million times by approximately 2,700 government and industry sector organisations in 2022 alone, while there were approximately 2.6 million Facial Verification Service (**FVS**) transactions in the 2022–23 financial year.[1] There is no opportunity for individuals to opt out of being subject to these

[1] Commonwealth, *Parliamentary Debates,* House of Representatives, 13 September 2023, 13 (Mark Dreyfus, Attorney-General).

schemes, placing an even greater onus on the Government to ensure that adequate safeguards and oversight mechanisms are in place.

6. While this submission predominantly focuses on the provisions of the Identity Verification Services Bill 2023 (the **Bill**), the Law Council notes that the Explanatory Memorandum for the Bills contains several typographical errors. This is perhaps an indication of the expedited approach taken on this occasion.[2]

Context

7. The previous iteration of the Bill, the Identity-Matching Services Bill 2019 (the **2019 Bill**), intended to provide the legislative underpinning for the use of facial recognition technology by Commonwealth authorities based on a government database.

8. However, the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) recommended that the 2019 Bill not proceed before it could be redrafted to address the lack of attention to privacy and human rights safeguards.[3] The Law Council supported those recommendations at that time.[4]

9. Despite the PJCIS's recommendations for holistic improvement to the legislative framework prior to reintroduction, the development and reliance on the database nevertheless proceeded, seemingly without legislative authority. The Commonwealth website *idmatch.gov.au* indicates that the relevant services are already available and advises that the 'full range of services will become available to government over the next two years'.[5]

10. Pleasingly, the Bills appear to be more robust, both in terms of privacy and human rights safeguards, compared to the 2019 Bill. Subject to the below remarks and suggestions for improvement, the Law Council supports the Bills progressing, as it is vastly preferable to have a legislative foundation in place for an identity verification framework which, as noted above, has already been in use for several years.

Key concepts in the Bill

11. The Bill creates a legislative framework that will authorise the one-to-one matching of identity, occurring by way of identity verification services matching biometric information (such as a photograph or biographic information) with an existing government record. This process will be enabled by the DVS and the FVS.

12. The Bill also authorises one-to-many matching services, albeit for the limited purposes of protecting a shielded person—who has been authorised to use an assumed identity under law—or someone associated with such a person. This process, which allows a facial image, like a photograph, to be matched against other facial images, is to be conducted through the Face Identification Service (**FIS**).

---

[2] Explanatory Memorandum, [6]: '*verifiy*', [18]: '*verifiy*', [122]: '*The FIS is a 1:many matching service that' / 'The FIS is a 1:many matching identity verification service that*', [210]: '*Privcy*'.
[3] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* (October 2019).
[4] Law Council of Australia, Report on identity-matching strikes the right balance (Media Release, 24 October 2019), <https://lawcouncil.au/media/media-releases/report-on-identity-matching-strikes-the-right-balance>.
[5] Australian Government, ID Match (Web Page, 2023) <www.idmatch.gov.au>.

13. All entities accessing identity verification services will be required to be a party to a 'participation agreement' (defined in clause 8) in respect of the relevant service. Clause 39 requires that the agreement be published on the Attorney-General's Department's website.

14. The Explanatory Memorandum says that the Bill 'contains a number of additional transparency, accountability and oversight measures to ensure privacy standards are upheld.'[6] The Law Council recommends that the principles of transparency, accountability and oversight be legislated as express requirements forming part of the proposed framework.

<u>Definitions</u>

15. Many of the proposed definitions in the Bill relating to 'identification information'[7] naturally overlap with terminology related to data management, and obligations attaching to personal information, as defined by the *Privacy Act 1988* (Cth). That said, some of the operative provisions in the Bill use slightly different terminology, for example:

- the definition of 'personal information' in the Privacy Act references information 'about' an individual;[8] while
- the provisions in the Bill defining 'Face-matching service information'[9] and 'DVS information'[10] use the words 'relating' or 'relates to' an individual[11].

16. Although the words 'relate to' and 'about' are often used interchangeably in general usage, they have come to have specific meaning in privacy and data protection matters. These words have also been the subject of judicial consideration,[12] and subsequent application by regulators.[13] In this respect, the Law Council notes that the definition of 'personal information' in the Privacy Act is currently under review and the Government has agreed, in principle, to amend it.[14]

17. There is a significant need for consistency and certainty of key concepts across Australia's digital identity, privacy, and identity verification frameworks. However, the fragmented and expedited reform approach that the Government is taking is not conducive to promoting harmonisation and clarity. Apart from the ongoing review of the Privacy Act, a separate consultation is being undertaken at present on exposure drafts of the Digital ID Bill 2023 and the Digital ID Rules 2023.[15]

18. The Law Council reiterates its calls for a roadmap for the harmonisation of Australia's privacy and data laws, to ensure the development of a national privacy framework that is consistent, clear and accessible.[16]

---

[6] Explanatory Memorandum, [57].
[7] Identity Verification Services Bill 2023 (Cth), cl 6.
[8] *Privacy Act 1988* (Cth) s 6.
[9] Identity Verification Services Bill 2023 (Cth), sub-cl 6(1).
[10] Ibid sub-cl 6(2).
[11] Ibid sub-cl 6(2)-(3).
[12] *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4*.
[13] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) [2021] AICmr 50 (29 September 2021)*.
[14] Government Response to the Privacy Act Review Report (September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.
[15] Australian Government, 2023 Digital ID Bill and Rules submissions (Web Page, September 2023) <https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions>.
[16] Law Council of Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Submission to the Senate Legal and Constitutional Affairs Committee, 8 November 2022) <https://lawcouncil.au/resources/submissions/privacy-legislation-amendment-enforcement-and-other-measures-bill-2022> 8.

One-to-many matching

19. Clause 10 of the Bill provides that parties to a participation agreement may only request an FIS for the purposes of protecting the identity of persons with a legally assumed identity, such as undercover officers and protected witnesses. As set out in the Explanatory Memorandum, all other uses of one-to-many matching through the identity verification services will not be authorised and will therefore be prohibited.[17]

20. The Law Council is pleased that the Bill restricts authorising one-to-many matching services for this narrow purpose only. In the absence of adequate privacy safeguards and oversight, FIS services have the potential to significantly infringe on the rights of individuals when applied inappropriately or inaccurately, and therefore should be limited to the greatest extent possible.

21. Concerns remain, however, given the increasing reliance on facial recognition technology by entities that will fall outside of the framework because they are not parties to a participation agreement. The Law Council particularly notes that law enforcement agencies in Australia have reportedly embraced facial recognition technologies in recent years, at times in the absence of a suitable regulatory framework (or even organisational authorisation).[18] An example of this is the use of Clearview AI's social media-derived database by the Australian Federal Police, as well as police in New South Wales, Queensland and Victoria.[19]

22. The University of Technology Sydney's Human Technology **Institute** has noted that laws in Australia do not effectively regulate the use of facial recognition technology. The Institute has, consequently, proposed a model facial recognition law.[20] The Law Council supports, in principle, a legislative framework being developed and enacted to ensure lawfulness and compliance with human rights in this field.

Obligations on parties

Compliance threshold

23. Subclause 9(1) of the Bill provides that each party to a participation agreement must agree to be bound by the Privacy Act, or a State or Territory equivalent, or agree to be subject to the Australian Privacy Principles. This requirement provides some assurance.

24. However, it is concerning that being subject to the Privacy Act is a sufficient threshold for parties authorised to engage with the framework under the Bill, when there has been an explicit acknowledgement from the Australian Government that the Privacy Act 'has not kept pace with the changes in the digital world',[21] and needs wholesale reform.

---

[17] Explanatory Memorandum, [6].
[18] See, eg., Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 *University of NSW Law Journal* 121, 122-123; Adam Fletcher, 'Government surveillance and facial recognition in Australia: a human rights analysis of recent Developments' (2023) 32(1) *Griffith Law Review* 30, 33-37.
[19] See, eg., Josh Taylor, 'Victoria Police distances itself from controversial facial recognition firm Clearview AI' The Guardian (online, 19 June 2020); Office of the Australian Information Commissioner, AFP ordered to strengthen privacy governance, Media Release, 16 December 2021; Justin Hendry, 'Facial recognition use "misunderstood": NSW Police', InnovationAus, 11 October 2022: https://www. innovationaus.com/facial-recognition-use-misunderstood-nsw-police>.
[20] Nicholas Davis, Lauren Perry and Edward Santow, *Facial Recognition Technology: Towards a Model Law* (Report, Human Technology Institute, September 2022) 5.
[21] The Hon Mark Dreyfus KC MP, Landmark Privacy Act Review report released (Media Release, 16 February 2023) <https://ministers.ag.gov.au/media-centre/landmark-privacy-act-review-report-released-16-02-2023>.

25. The ongoing, comprehensive review of the Privacy Act, in addition to recent high-profile data breaches, has highlighted serious deficiencies in the current regime, which has been in operation for more than 30 years and is in urgent need of modernisation. In February 2023, the Department released the Privacy Act Review Report, containing 116 proposals for reform.[22] In late September 2023, the Government formally responded to the Report, agreeing, or agreeing in-principle, with the majority of the proposals.[23]

26. Given the sensitive personal information, including biometric information, held within the framework, higher standards of compliance should apply to parties, beyond reliance on the existing Privacy Act, which is not fit for purpose in the digital landscape. Clause 10 of the Bill imposes minor additional privacy obligations on parties to a participation agreement that proposes to request identity verification services, however these are limited in scope and unlikely to promote public trust in the scheme.

27. The exposure draft of the Digital ID Bill, mentioned above, contains a specific division that sets out several additional privacy safeguards that go beyond those in the Privacy Act.[24] These safeguards must be adhered to by accredited Digital ID services under the proposed arrangement.[25] The inclusion of these safeguards in the draft Digital ID Bill indicates that compliance with the Privacy Act in its current form is not regarded as providing adequate protections for the collection and handling of biometric data.

28. Any additional obligations on parties to a participation agreement that extend beyond subclause 9(1) should ideally be contained in primary legislation. However, there is scope under proposed clause 44 of the Bill for the Minister to make rules by legislative instrument in relation to matters necessary or convenient to be prescribed for carrying out, or giving effect to, the Bill.

29. In the absence of additional legislative safeguards being included in the Bill, ideally consistent (where appropriate) with the safeguards in the draft Digital ID Bill, it would be prudent for rules to be developed, pursuant to clause 44, which can lift the compliance expectations on entities within the framework beyond what is currently required.

30. In relation to the development of rules under clause 44 of the Bill, regard should be had to clause 159 of the draft Digital ID Bill, which imposes a welcome requirement to publicly consult on draft rules.

Use of information

31. Additional clarity is required for the standards of compliance, set out in proposed Parts 2 and 3 of the Bill. For example, clause 28 seeks to address ‘use’ and ‘disclosure’ of identification information, but it appears to be silent on obligations that attach to ‘holding’ information.

32. The Law Council appreciates that most risks will arise from the (mis)use and disclosure of information, hence the need to expressly address these parts of the data lifecycle, as the Bill has done. However, security risks can arise from simply holding the information.

33. If there is no intention that the regulated services will hold the relevant information, this must be expressly addressed in the Bill. Conversely, if the intended process will involve

---

[22] Attorney-General’s Department, Privacy Act Review Report 2022 (February 2023) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.
[23] Government Response to the Privacy Act Review Report (September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.
[24] Exposure Draft - Digital ID Bill 2023, Chapter 3, Part 2, Division 2.
[25] Ibid.

the holding, or other processing, of information, the Bill should address the relevant responsibilities attaching to these processes. It is important these anomalies be clarified to avoid ambiguities and potentially unintended consequences, and limit the costs of compliance for entities.

Compliance with Australia's international human rights obligations

34. The Explanatory Memorandum acknowledges that the Bill engages several of Australia's international human rights obligations, including with respect to non-discrimination, privacy, freedom of expression and social security.[26]

35. Commentary on previous developments in this space, including this Bill's predecessor (the 2019 Bill) focussed primarily on the potential for false matches to have discriminatory effects.[27] Concerns were also raised regarding the potential for use and/or disclosure of the personal data involved to breach individuals' right to privacy under Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).[28]

36. Although it is relatively clear that official photographs from passports and drivers' licences are the sources for the FVS, FIS and National Driver Licence Facial Recognition Solution (**NDLFRS**) databases, it is much less clear which algorithms are used for matching faces, and on which datasets those algorithms have been trained.[29] This gives rise to concerns about accuracy and potentially discriminatory effects of incorrect findings.[30]

37. In terms of privacy, many of the most pressing privacy concerns emerge from the one-to-many applications of the FIS previously proposed (sometimes termed 'facial identification' rather than 'facial verification'[31]), which are not authorised by the present Bill. Nevertheless, there remain significant concerns about the scale of the federal identification databases that have been established, and the potential for personal data to be disclosed inappropriately. The Explanatory Memorandum explains that the system is justified largely on the basis that:

> *… secure and efficient identity verification is critical to minimising the risk of identify fraud and theft, and protecting the privacy of Australians when seeking to access government and industry services and engage with the digital economy*.[32]

[26] Explanatory memorandum, [19].
[27] There are guarantees of non-discrimination in multiple treaties to which Australia is party, including the ICCPR (Articles 2 and 26), ICESCR (Article 2) and ICERD. A leading article on this topic is Buolamwini and Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.
[28] 999 UNTS 171, adopted 16 December 1966 (entry into force 23 March 1976). Articles on the implications of the proposed Australian implementation include: Mann and Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 *University of NSW Law Journal* 121 and Fletcher, 'Government surveillance and facial recognition in Australia: a human rights analysis of recent developments' (2023) 32 *Griffith Law Review* 30.
[29] This information is not available, for example, on the idmatch.gov.au website: <https://www.idmatch.gov.au/faqs>.
[30] The *Gender Shades* research found that many facial recognition products are less accurate for matching non-white and female faces. Buolamwini and Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 *Proceedings of Machine Learning Research* 1: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.
[31] See e.g. Davis, Perry and Santow, *Facial Recognition Technology: Towards a model law,* September 2022: <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf>, 15.
[32] Explanatory memorandum, [1].

38. Along with safeguards, such as secure data handling, informed consent is key to compliance with both domestic and international privacy protections.[33] Australians are, as noted above, already precluded from opting out of inclusion in the federal databases. In addition, the Explanatory Memorandum acknowledges that access to crucial Government services often depends on the DVS and FVS. The informed consent requirements in the Bill are likely to be of little value to those who lack reasonable alternative means to access the relevant services.[34]

39. On the other hand, the Bill's requirements for privacy impact assessments, complaints mechanisms (with the ability to alter incorrect information), publication of 'participation agreements' and breach notifications are welcome from a privacy perspective.

40. The Law Council has been unable to conduct a thorough human rights law analysis of the Bill—including, importantly, an assessment of whether it is proportionate to its stated aims[35]—in the brief time available for review. The Statement of Compatibility with Human Rights in the Explanatory Memorandum is insufficient for this purpose.

41. The Law Council recommends, therefore, that the Bill be assessed for compatibility with Australia's international obligations by the Parliamentary Joint Committee on Human Rights.

Additional comments

Delegation of Secretary's powers

42. Clause 38 of the Bill enables the Secretary to delegate all or any of their powers or functions under the Bill to a Senior Executive Service (**SES**) employee (or acting SES employee) in the Department.

43. While the Explanatory Memorandum provides that Clause 38 'facilitates the practical implementation of the Bill',[36] the Law Council queries whether the broad scope of this delegation power is appropriate, given the invasive powers in the Bill and the enormity of the information held within the framework. Beyond matters of mere practicality, adequate justification has not been provided for such an expansive delegation power.

44. Consideration should therefore be given to limiting the scope of the Secretary's delegation power, such as by:

    - specifying certain powers that can be delegated (rather than 'all or any' powers); or

    - providing that the Secretary's powers can only be delegated to a certain level of SES employee (such as SES Band 2 and above).

Review of operations

45. Clause 43 of the Bill provides that the Minister must cause a review of the operation of the Bill, and of the provision of identity verification services, to be started within two years of the commencement of the framework.

---

[33] See e.g., OAIC, *Consent to the handling of personal information:* <https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information>.
[34] See Identity Verification Services Bill 2023, sub-cl 9(2)-(3).
[35] This is a general requirement of compliance with the international right to privacy – see e.g. UN Human Rights Committee, *General Comment 16*, UN Doc HRI/GEN/1/Rev.1, 8 April 1988 [2]; *General Comment 31*, UN Doc CCPR/C/21/Rev.1/Add.13, 26 May 2004 [6] and *Report of the special rapporteur on the right to privacy*, UN Doc A/HRC/40/63, 27 February 2019, [11–12].
[36] Explanatory Memorandum, [362].

46. The Law Council welcomes the statutory requirement for review, which will provide a clearer picture of how the identity verification scheme operates in practice. However, given the very limited timeframes provided to engage with the Bill at the Committee stage, this mandatory review should instead take place 12 months after commencement. This change will ensure that any unintended consequences can be identified and addressed in a timelier manner.

Oversight by the Information Commissioner

47. The Law Council welcomes the role of the Information Commissioner proposed in clause 40 of the Bill. However, it notes that the clause merely grants the Information Commissioner the function, or power, to conduct an assessment. It appears that there would be no obligation on the Information Commissioner to conduct the assessment. Consideration should be given to legislating such an obligation.

48. The Explanatory Memorandum provides that 'the Information Commissioner would be required to perform both aspects of the assessment within 6 months of the end of each financial year'.[37] The Bill should explicitly provide for this requirement, rather than merely providing for the 'function' of assessing and reporting on the operation and management of the approved identity verification facilities.

49. Regard should also be had to potentially replicating clause 40 of the draft Digital ID Bill, which provides the Information Commissioner with an advisory role in relation to the operation of that Bill at the request of the Minister.

General privacy obligations of authorities, persons or bodies operating in New Zealand

50. Paragraph 9(1)(e) of the Bill outlines that, when a party to a participation agreement seeking to access the DVS is an authority of New Zealand or a person or body operating in New Zealand, that authority, person or body must be subject to the *Privacy Act 1993* of New Zealand. The Explanatory Memorandum notes that this 'supports the arrangements currently in place with New Zealand, providing for the use of the DVS by New Zealand based entities and a reciprocal arrangement for Australian entities to use the similar New Zealand service'.[38]

51. The Law Council notes this reciprocal arrangement requires ongoing structures (such as a memorandum of understanding) to be in place.

Contact

52. If the Law Council can be of any further assistance to the Committee in the course of its inquiry, please contact

Yours sincerely

Luke Murphy
President

[37] Ibid [378].
[38] Ibid [171].