Law Council
OF AUSTRALIA

Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 [Provisions]

Senate Environment and Communications Legislation Committee

30 January 2023

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

Table of Contents

About the Law Council of Australia

The Law Council of Australia represents the legal profession at the national level, speaks on behalf of its Constituent Bodies on federal, national and international issues, and promotes 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 its Constituent Bodies: 16 Australian State and Territory law societies and bar associations, and Law Firms Australia. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Law Society of the Australian Capital Territory
- New South Wales Bar Association
- Law Society of New South Wales
- Northern Territory Bar Association
- Law Society Northern Territory
- Bar Association of Queensland
- Queensland Law Society
- South Australian Bar Association
- Law Society of South Australia
- Tasmanian Bar
- Law Society of Tasmania
- The Victorian Bar Incorporated
- Law Institute of Victoria
- Western Australian Bar Association
- Law Society of Western Australia
- Law Firms Australia

Through this representation, the Law Council acts on behalf of more than 90,000 Australian lawyers.

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 Directors' meetings, responsibility for the policies and governance of the Law Council is exercised by the Executive members, led by the President who normally serves a one-year term. The Board of Directors elects the Executive members.

The members of the Law Council Executive for 2023 are:

- Mr Luke Murphy, President
- Mr Greg McIntyre SC, President-elect
- Ms Juliana Warner, Treasurer
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member
- Ms Tania Wolff, Executive Member

The Chief Executive Officer of the Law Council is Dr James Popple. The Secretariat serves the Law Council nationally and is based in Canberra.

The Law Council's website is www.lawcouncil.asn.au.

Acknowledgements

The Law Council is grateful for the contributions of the Law Society of New South Wales and the New South Wales Bar Association in the preparation of this submission. It also appreciates the input of its National Human Rights Committee and its Business Law Section's Privacy Law Committee.

Introduction

1. The Law Council is pleased to provide this submission to the Senate Environment and Communications Legislation Committee (**the Committee**) on the Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (Cth) (**the Bill**).

2. The Law Council is supportive of measures to promote the safety and welfare of individuals and acknowledges the role of information disclosures permitted under the *Telecommunications Act 1997* (Cth) for purposes connected to the prevention of a serious threat to the life or health of a person.

3. However, the lowering of legislative thresholds relating to the disclosure of potentially sensitive information must be carefully scrutinised in terms of necessity and proportionality. This is of particular importance, given that data privacy has naturally been at the forefront of minds in the wake of recent cyber incidents involving the theft and misuse of personal data.

4. The Law Council's focus is therefore on the privacy implications of the Bill as drafted, especially the justifications for the Bill's proposed expanded use and disclosure regime under Part 13 of the Telecommunications Act and the adequacy of safeguards and oversight to ensure the scheme operates appropriately.

5. As set out in this submission, the Law Council recommends additional safeguards and clarification in relation to the measures contained in the Bill, including that:

   - The Bill (or at a minimum, its Explanatory Memorandum) should be drafted with greater clarity regarding:
     - the meaning and applicability of 'matters raised by a call to an emergency service number' and the parameters of 'dealing with the matter or matters raised by' a call to an emergency service number in new paragraph 285(1B)(c) so that there is a sufficient nexus between the matters raised, the dealings and an established emergency situation;
     - the safeguards that would apply to the use and handling of information disclosed under section 285, as amended; and
     - the parties to which disclosure could occur.
   - Clarification should be provided in relation to how sensitive circumstances will be managed in practice, such as where individuals do not want to be located, or where there is a risk to the individual if their location is disclosed.
   - Guidance should be developed on circumstances where it would be 'unreasonable or impracticable' to obtain a person's consent for disclosure or use in proposed paragraphs 287(ab) and 300(2)(a).
   - Record-keeping requirements in Part 13, Division 5 of the Telecommunications Act should be extended to disclosures made pursuant to proposed sections 287 and 300.
   - A statutory review mechanism should be added to ensure the amended disclosure regime is being used for its intended limited purpose.

6. Despite the explicit acknowledgement in the Bill's Statement of Compatibility with Human Rights (**Statement of Compatibility**) that the proposed measures will limit privacy,[1] the Law Council understands that civil liberties organisations were not consulted during the Bill's development, with external stakeholder consultations confined to 'major telecommunications providers and the Communications Alliance'.[2] While the Law Council is aware that certain civil liberties organisations were consulted in early December 2022, this occurred after the Bill was introduced in the House of Representatives.[3]

7. This limited engagement—coupled with the truncated time provided over the holiday period for submissions to the Committee to be prepared—is unfortunate, given the human rights implications of this Bill. In addition to limiting privacy, the Law Council notes that the Bill engages the right to an effective remedy[4] by extending the immunity of carriers and carriage service providers from civil liability.[5] The Bill's Statement of Compatibility does not identify this right; in the Law Council's view, this is an oversight.

Part 1—Information use and disclosure

8. Part 1 of Schedule 1 to the Bill introduces amendments to the information disclosure and national interest provisions within Part 13 of the Telecommunications Act. These measures seek to:

   - authorise the use and disclosure of unlisted phone numbers and associated addresses for the purposes of dealing with matters raised by a call to an emergency service number;
   - permit the use and disclosure of information for purposes connected to the prevention of a serious threat to the life or health of a person by removing the existing 'imminent' threat qualifier in sections 287 and 300; and
   - confer civil immunities on telecommunications companies for the provision of reasonably necessary assistance if a national emergency declaration is in force.

9. These measures are discussed further below.

[1] Explanatory Memorandum, Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (Cth) ('Telecommunications Bill') 7.
[2] Commonwealth, *Parliamentary Debates*, House of Representatives, 10 November 2022, 2 (Michelle Rowland, Minister for Communications).
[3] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Telecommunications Legislation Amendment (Information Disclosure, National Interest, and Other Measures) Bill 2022 (Submission, 16 January 2023) 8.
[4] Parliamentary Joint Committee on Human Rights ('PJCHR'), *Human Rights Scrutiny Report* (Report 6, 24 November 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2022/Report_6_of_2022> 63-65.
[5] Telecommunications Bill, sch 1 item 10.

Expansion of the use and disclosure regime to unlisted numbers

10. The Integrated Public Number Database (**IPND**) is a record of Australian phone numbers and associated customer data,[6] including:

    - the name and address of the customer;
    - the customer's service location;
    - the name of the carriage service provider; and
    - whether the telephone is to be used for government, business, charitable or private purposes.[7]

11. The IPND contains data for listed numbers, where a person has agreed it can be shown in phone number directories and related services, as well as unlisted (silent) numbers, which are not made publicly available.[8] Of the approximately 72 million active phone numbers in Australia, five per cent are currently listed on the IPND.[9] This is largely because mobile phone numbers are unlisted by default.[10]

12. The use and disclosure of information in the IPND is subject to Part 13 of the Telecommunications Act. Under section 285, Telstra (the carrier who currently maintains the database) will commit an offence under Division 2, Part 13 if it discloses information associated with unlisted numbers, unless an exception applies.[11]

13. The Bill seeks to add subsection 285(1B) to the Telecommunications Act providing a carve-out for the disclosure and use offences in sections 276 and 277 if:

    - the use or disclosure is made for purposes connected with dealing with the matters raised by a call to an emergency service number; and
    - it is unreasonable or impracticable to obtain the other person's consent to the disclosure or use.[12]

14. Unlike the existing section 285 disclosure regime, proposed subsection 285(1B) applies to both listed and unlisted numbers.

Law Council view

15. The Law Council acknowledges that the Bill amends section 285 of the Telecommunications Act in a manner consistent with the recommendation of the Australian Law Reform Commission (**ALRC**) in its 2008 report, *For Your Information: Australian Privacy Law and Practice* (**Privacy Report**),[13] and agrees with the ALRC's proposition that 'most individuals would reasonably expect the disclosure of an unlisted number in an emergency call situation'.[14] The Law Council similarly

---

[6] Australian Communications and Media Authority ('ACMA'), Accessing the IPND (Web page, 15 November 2022), <https://www.acma.gov.au/accessing-ipnd>.
[7] *Telecommunications (Carrier Licence Conditions – Telstra Corporation Limited) Declaration 2019* (Cth) cl 10 (3).
[8] ACMA, Accessing the IPND (Web page, 15 November 2022), <https://www.acma.gov.au/accessing-ipnd>.
[9] Ibid.
[10] Explanatory Memorandum, Telecommunications Bill 9.
[11] *Telecommunications Act 1997* (Cth) pt 13 div 3.
[12] Telecommunications Bill sch 1 item 6.
[13] Australian Law Reform Commission ('ALRC'), *For Your Information: Australian Privacy Law and Practice* (Report 108, Vol. 3, 12 August 2008) <https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol3.pdf> 2460-2461, recommendation 72-13.
[14] Ibid 2460.

acknowledges the argument in the Bill's Explanatory Memorandum that section 285 'can seemingly be a barrier in responding to emergencies'.[15]

16. However, while noting the important objective of protecting lives which underpins the amendments to section 285 and the broader measures in the Bill, the Law Council has reservations regarding the impact of these amendments on the right to privacy under the International Covenant on Civil and Political Rights, which provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.[16] The Parliamentary Joint Committee on Human Rights (**PJCHR**), when scrutinising the Bill, expands on this right, stating:

> *The right to privacy includes … respect for private and confidential information, particularly the storing, use and sharing of such information. It also includes the right to control the dissemination of information about one's private life, and protects against arbitrary and unlawful interferences with an individual's privacy and attacks on reputation.*[17]

17. The Law Council considers that, even if permitting the disclosure of information relating to unlisted phone numbers on the IPND in emergency situations has 'the potential to save lives',[18] this does not necessarily mean that these amendments provide a 'reasonable, necessary and proportionate'[19] limit on the right to privacy, as the Statement of Compatibility asserts. In particular, there are several practical matters relating to the amendments to section 285 which the Law Council would like to see clarified in the Bill and/or its Explanatory Memorandum, noting that their proposed wording is somewhat loosely expressed. These include:

- whether 'matters raised by a call to an emergency service number' in new paragraph 285(1B)(c) would:
  - restrict disclosure to police, fire, and ambulance services; or
  - allow disclosure to any person, so long as it related to a matter originally raised by the emergency services call;
- the parameters of 'dealing with the matter or matters raised by' a call to an emergency service number in new paragraph 285(1B)(c), as it does not appear to connect such follow-up with a risk of harm to any person; and
- what safeguards would apply to information disclosed under section 285, as amended, including restrictions in terms of how the data must be handled, used, stored, and destroyed.[20]

18. Finally, as pointed out by the PJCHR, the explanatory materials to the Bill do not identify to whom information or documents obtained under this measure may be disclosed, and it is unclear whether the wording 'matters raised by a call to an emergency service number' would restrict disclosure to police, fire and ambulance services, or allow disclosure to any person so long as it related to a matter originally

---

[15] Explanatory Memorandum, Telecommunications Bill 9.
[16] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.
[17] Parliamentary Joint Committee on Human Rights ('PJCHR'), *Human Rights Scrutiny Report* (Report 6, 24 November 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2022/Report_6_of_2022> 54, footnote 21.
[18] Explanatory Memorandum, Telecommunications Bill 6.
[19] Ibid.
[20] These queries were similarly raised by the PJCHR in its *Human Rights Scrutiny Report* (Report 6, 24 November 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2022/Report_6_of_2022> 57-58.

raised by the emergency services call. The Law Council is supportive of further clarification in this regard.

Recommendations

- **The Bill (or at a minimum, its Explanatory Memorandum) should be drafted with greater clarity regarding:**
  - **the meaning and applicability of 'matters raised by a call to an emergency service number' and the parameters of 'dealing with the matter or matters raised by' a call to an emergency service number in new paragraph 285(1B)(c) so that there is a sufficient nexus between the matters raised, the dealings and an established emergency situation;**
  - **the safeguards that would apply to the use and handling of information disclosed under section 285, as amended; and**
  - **the parties to which disclosure could occur.**

Removal of the 'imminent' threat qualifier and introduction of 'reasonable belief' requirement

19. Section 287 of the Telecommunications Act currently provides an exception to the disclosure or use offences under Division 2, Part 13 if:

- the relevant information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person;[21] and
- the disclosing party believes, on reasonable grounds, that the disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person.[22]

20. Section 300 provides that, where information is disclosed to a person under section 287, that person must not disclose or use the information or document unless:

- the disclosure or use is for the purpose of, or in connection with, preventing or lessening a serious and imminent threat to the life or health of another person; or
- the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of another person.[23]

21. A 'serious and imminent threat to the life or health of another person' is not defined, and it is the person being asked to disclose the information who must themselves believe, on reasonable grounds, both the seriousness of the threat and the necessity of disclosing the information or documents requested.

22. The Bill seeks to broaden the grounds on which the use and disclosure of personal information are allowed for purposes connected to the prevention of a serious threat

[21] *Telecommunications Act 1997* (Cth) para 287(a).
[22] Ibid para 287(b).
[23] Ibid, section 300.

to the life or health of a person. Specifically, the Bill would remove the current requirement in sections 287 and 300 of the Telecommunications Act for the relevant threat to the life or health of a person to be 'imminent'.[24]

23. The Bill would also incorporate a purported safeguard through proposed paragraph 287(ab), which provides that the entity or person being asked to disclose the information must be satisfied that it is unreasonable or impracticable to obtain the other person's consent to the disclosure or use.[25] The Law Council notes that this is consistent with the *Australian Privacy Principles Guidelines*.[26]

24. In practice, these amendments would mean that a person can only disclose information or documents if the following criteria are met:

- the information or document relates to the affairs or personal particulars of another person; and
- the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious threat to the life or health of a person; and
- the first person is satisfied that it is unreasonable or impracticable to obtain the other person's consent to the proposed disclosure or use.[27]

25. In addition, the Bill would introduce a new section 300 of the Telecommunications Act, which contains equivalent provisions relating to the secondary disclosure of information, received under proposed section 287, by law enforcement agencies.[28]

Law Council view

26. The Law Council supports, in principle, amending sections 287 and 300 of the Telecommunications Act by deleting the word 'imminent'. Reform in this context has been recommended as a priority by several New South Wales coroners, most recently by Magistrate Erin Kennedy, the Deputy State Coroner in September 2022.[29] The Deputy State Coroner's recommendation also referred to a similar recommendation made by the ALRC in its Privacy Report, advocating for amendments to sections 287 and 300 which remove the requirement for the threat to be imminent.[30] These recommendations highlight that the current requirement for the threat to be imminent (in addition to serious) may restrict the disclosure of information about the location of missing persons by telecommunications providers, which, in turn, may hinder the ability of law enforcement to take meaningful preventative action in missing persons cases.[31]

[24] Telecommunications Bill, sch 1 items 8, 9.
[25] Ibid sch 1 item 7.
[26] Office of the Australian Information Commissioner ('OAIC'), Chapter C: Permitted general situations, (Australian Privacy Principles Guidelines, July 2019) <https://www.oaic.gov.au/__data/assets/pdf_file/0011/1244/app-guidelines-chapter-c-v1.1.pdf>.
[27] Telecommunications Bill, sch 1 item 7 (proposed new section 287(ab)).
[28] Ibid sch 1 item 9.
[29] Coroners Court of New South Wales, Inquest into the death of CD (Findings Report, 16 September 2022) <https://coroners.nsw.gov.au/coronerscourt/download.html/documents/findings/2022/Inquest_into_to_the_Disappearance_of_CD_-_Findings.pdf> 40-41, Recommendation 2.
[30] ALRC, *For Your Information: Australian Privacy Law and Practice* (Report 108, Vol. 3, 12 August 2008) <https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol3.pdf> 2430-2433, recommendation 72-7.
[31] Ibid 2432.

27. However, the Law Council considers that mobile phone data, including location information, is inherently sensitive due to the potential for this data to be used to track an individual or identify them by drawing insights from their location. Notwithstanding the Bill's intention to expand data access to promote public safety, regard must be had to the proportionality of this measure and the potential for the misuse and mismanagement of the resulting data. This is critical, given agencies (including law enforcement agencies) have, in the past, contravened existing measures to protect private data, including failing to properly store, protect and destroy it.[32]

28. There must be a strong regime for the protection of any data obtained under the amended disclosure regime. However, the Bill and its explanatory materials do not offer assurances relating to the access, use and protection of this sensitive information. This lack of certainty is troubling, and the Law Council reiterates the queries of the PJCHR in this regard.[33]

29. In the Law Council's view, the privacy risk to individuals from the Bill is heightened by the lack of independent adjudication or oversight for proposed sections 287 and 300 of the Telecommunications Act. As noted in the Explanatory Memorandum, it is intended that telecommunications providers will predominantly be reliant on representations made by law enforcement agencies or emergency services to determine the seriousness of a threat.[34] Relatedly, the Law Council refers to the Commonwealth Ombudsman's submission to the Environment and Communications Legislation Committee in the course of this inquiry and shares his concern that there is currently no Commonwealth body responsible for comprehensive oversight of Commonwealth, state and territory agencies' use of existing section 280 of the Telecommunications Act.[35] The Law Council suggests that the Ombudsman would be well-placed to perform this oversight role.

30. The Law Council sees benefits in clarifying how the Bill would, if passed, address circumstances where individuals do not want to be located or where there is a risk to the individual's safety if their location becomes known. In this respect, consideration should be given to requiring a disclosing party to first consider the wishes and circumstances of the person to whom the information relates before making a disclosure under new sections 287 or 300. This may include, for example, whether the person has expressed a view about not wanting to be located in the event of their disappearance and whether the person may have been experiencing family or domestic violence or seeking to escape from another dangerous situation.

31. It is clear that the proposed scheme will rely heavily on the judgement of the disclosing party as to the nature of the threat in the relevant circumstances. This discretion is also central to the statutory task of assessing whether it is 'unreasonable or impracticable' to obtain a person's consent for disclosure or use in proposed paragraphs 287(ab) and 300(2)(a) of the Telecommunications Act. In light of these subjective and broadly framed elements, it is critical that appropriate

[32] See, for example, Greg Miskelly and Peta Doherty, Inside the police database that holds 40 million private records and any officer can access, *ABC News* (Online, 23 June 2019) <https://www.abc.net.au/news/2019-06-23/nsw-police-database-privacy-breach-exposed-in-abc-investigation/11224426> and Matilda Marozzi and Josie Taylor, Victoria Police allegedly use LEAP database to pursue, stalk, harass women prompting calls for inquiry, *ABC News* (Online, 15 December 2022) <https://www.abc.net.au/news/2022-12-15/victoria-police-leap-database-pursue-stalk-harass-women/101663452>.
[33] PJCHR, *Human Rights Scrutiny Report* (Report 6, 24 November 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2022/Report_6_of_2022> 60.
[34] Explanatory Memorandum, Telecommunications Bill 10.
[35] Commonwealth Ombudsman, Inquiry into the Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (Submission, 9 January 2023) 1-2.

guidance is provided to those individuals who will seek to rely on the measures as amended by the Bill.

32. It will also be important to ensure accurate records are maintained as to how the proposed measures are applied. The Law Council therefore suggests that regard be given to expanding the record-keeping requirements in Part 13, Division 5 of the Telecommunications Act to disclosures pursuant to proposed sections 287 and 300, including maintaining records relating to steps taken to obtain consent for disclosure.

33. Finally, given the need to ensure the amended disclosure regime is being used for its intended limited purpose and the correct balance has indeed been struck, the Law Council considers that a legislated statutory review mechanism ought to be considered.

Recommendations

- **Clarification should be provided in relation to how sensitive circumstances will be managed in practice, such as where individuals do not want to be located, or where there is a risk to the individual if their location is disclosed.**
- **Guidance should be developed on circumstances where it would be 'unreasonable or impracticable' to obtain a person's consent for disclosure or use in proposed paragraphs 287(ab) and 300(2)(a).**
- **Record-keeping requirements in Part 13, Division 5 of the Telecommunications Act should be extended to disclosures made pursuant to proposed sections 287 and 300.**
- **A statutory review mechanism should be added to ensure the amended disclosure regime is being used for its intended limited purpose.**

Privacy Impact Assessment

34. A Privacy Impact Assessment (**PIA**) is currently required to be conducted by Australian Government agencies subject to the *Privacy Act 1988* (Cth) for 'high privacy risk' projects, in addition to the current practice of assessing privacy impacts through the Statement of Compatibility. For a project to be deemed a 'high privacy risk', the agency is required to reasonably consider that the project involves new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.[36]

35. While it is unclear whether a PIA was conducted in relation to this Bill,[37] the Law Council considers it unlikely, considering that the Attorney-General's Department advised the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the **Department**) in October 2022 that it had concluded there were no privacy risks associated with the information disclosure aspects of the Bill.[38] In addition, at the time of writing, the Bill is not listed on the

[36] Privacy (Australian Government Agencies – Governance) Australian Privacy Principles Code 2017 s 12.
[37] OAIC, Privacy impact assessments (Web page, 2022) <https://www.oaic.gov.au/privacy/privacy-impact-assessments>.
[38] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (Submission, 16 January 2023) 9.

Department's PIA register[39] and the Explanatory Memorandum does not state whether a PIA was completed.

36. The Law Society of New South Wales and the Business Law Section's Privacy Law Committee are of the view that the practices outlined above (Statement of Compatibility, plus a PIA for 'high privacy risk' projects) are insufficient to properly examine the wide ranging economic and social impacts of privacy and data security issues in the context of modern law reform. They suggest that a formal Privacy and Data Impact Statement/Assessment be incorporated into the explanatory memorandum for bills as a matter of course, in addition to the statements on financial impacts and human rights.

37. While the Law Council considers there may be merit in considering a more extensive and sophisticated process of assessing the privacy and data security implications of proposed legislation, it acknowledges that any such change would likely involve structural reform which would require corresponding funding and resourcing. As this is a matter on which the Law Council has not yet had the opportunity to expressly consult the legal profession, it does not seek to express a view at present.

38. At a minimum, the Law Council supports measures to ensure that the Office of the Australian Information Commissioner's comprehensive online guidance materials are given adequate consideration by Commonwealth agencies to promote privacy compliance and identify best practice.[40]

[39] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Privacy Impact Assessment (PIA) Register (Web page, 23 August 2022) <https://www.infrastructure.gov.au/department/media/publications/privacy-impact-assessment-pia-register>.
[40] OAIC, Guide to undertaking privacy impact assessments (Web page, 2 September 2021) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>.