Law Council
OF AUSTRALIA

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

5 May 2020

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 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 Law Firms Australia, 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
- Law Firms Australia
- 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 2020 Executive as at 1 January 2020 are:

- Ms Pauline Wright, President
- Dr Jacoba Brasch QC, President-elect
- Mr Tass Liveris, Treasurer
- Mr Ross Drinnan, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

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

Acknowledgement

The Law Council is grateful for the assistance of its National Criminal Law Committee, National Human Rights Committee, Administrative Law Committee and Privacy Law Committee in the preparation of this submission.

Executive Summary

1. The Law Council welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (**the Bill**).

2. The Law Council acknowledges concerns about the timeliness and efficiency of the mutual legal assistance regime, in the context of investigating serious crime in the digital environment. The Law Council supports measures to equip relevant agencies to conduct their investigations in this environment, provided that those measures are accompanied by commensurate safeguards and are proportionate to the threat.

3. The Law Council has a number of specific concerns about the adequacy of safeguards in nearly all aspects of the proposed regime. These concerns arise principally from the design of the proposed scheme as a minimal framework, with an apparent intention for many critical details, including safeguards, to be governed by the terms of individual executive agreements.

4. The Law Council is also concerned about some broader implications arising from the establishment of the International Production Orders (**IPO**) regime, without addressing persistent problems in the existing framework governing domestic interception and access activities.

Specific concerns about aspects of the proposed IPO framework

5. The Law Council is concerned that the framework proposed in the Bill leaves many essential details, including critical safeguards, to the content of individual, future executive agreements that would be prescribed by regulation as a Designated International Agreement (**DIA**).

6. This approach to the agreement-making framework renders it impossible, at the present time, to undertake a complete identification and assessment of the safeguards that will apply when the scheme is operational. The adoption of this approach is particularly problematic in Australia, in the absence of a Charter of Rights that confers rights and remedies of general application, which would apply to the IPO regime (as is the case in the United States and the United Kingdom, in relation to those countries' agreement-making frameworks).[1]

7. The Law Council considers that the above circumstances make it necessary for Australia's primary legislation creating the framework for the domestic implementation of individual executive agreements to include additional and stronger safeguards than those in the Bill as introduced.

8. To this end, the Law Council makes a number of recommendations to amend the Bill to implement strengthened safeguards, including the following measures:

    - imposing further conditions on the exercise of delegated legislative power to enliven the statutory IPO regime by making regulations to prescribe an

[1] For completeness, the Law Council acknowledges that the Australian administrative law system operates to protect a range of individual rights, through establishing grounds of review and facilitating access to review mechanisms. However, for reasons explained in this submission, many of those mechanisms would not appear to be available or may not operate effectively in the context of IPOs. In the absence of an applicable general mechanism for restraining executive action, such as a Bill or Charter of Rights, the source of any such restraint must therefore be found in the provisions of the IPO legislation itself.

agreement as a DIA. These conditions are modelled on equivalent provisions in the US *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**), and are directed to ensuring that an agreement meets certain minimum human rights standards, in order to be prescribed as a DIA;

- ensuring that proposed DIAs (that is, bilateral or multilateral agreements **before** they are prescribed in regulations) are subject to the same degree of Parliamentary scrutiny as mutual assistance treaties, via reviews conducted by the Parliamentary Joint Standing Committee on Treaties (**JSCOT**);
- creating statutory requirements for the timely publication and Parliamentary tabling of the full text of an agreement that is proposed to be prescribed as a DIA, to ensure that the Parliament has immediate access to that agreement when considering whether to disallow regulations prescribing it as a DIA;
- ensuring that the Parliament can effectively exercise its discretion to disallow DIA regulations, and maximising legal certainty for agencies, by providing that these regulations commence after the disallowance period has ended;
- strengthening the issuing criteria for national security IPOs obtained by the Australian Security Intelligence Organisation (**ASIO**)with respect to the assessment of the privacy impacts of the proposed collection activity;
- enhancing the independence and rigour of the issuing process for IPOs, through some amendments to the classes of people whom the Attorney-General may appoint as issuing authorities;
- strengthening mechanisms for the independent review of issuing authorities' decisions to issue IPOs, including upon the objection of a designated communications provider (**DCP**);
- ensuring that responsibilities for administering and enforcing the regime are invested in agencies or officials who are demonstrably independent from the issuing process for IPOs and the agencies able to request them;
- placing appropriate limits on overly broad powers of delegation and authorisation by all agencies who obtain and administer IPOs;
- strengthening requirements for the proactive identification and deletion of material obtained under an IPO that is stored in an agency' s holdings and is no longer relevant to the performance by that agency of its functions;
- strengthening Parliamentary and public reporting requirements on the operation of the scheme; and
- making appropriate provision for the independent and Parliamentary monitoring and review of the operation of the IPO scheme.

9. The Law Council also recommends that the Government provides, as a matter of priority, a public explanation of the proposed inclusion of ASIO in the IPO regime, given that the policy justification for its establishment focuses on addressing limitations identified in mutual legal assistance arrangements, and not the existing arrangements by which ASIO may cooperate with foreign bodies for intelligence collection purposes.

Concerns about broader implications of the Bill

10. The Law Council notes that there does not appear to be any public commitment, or proposed legislation before the Parliament, to make substantive reforms to the domestic interception and access scheme in the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**). Accordingly, the Bill perpetuates, in the context of the new international arrangements, many of the ongoing problems identified in the domestic regime.

11. The Law Council considers that there is a need for a comprehensive revision of the TIA Act with, for example, urgent amendments of the following kind, which should also be given effect in corresponding provisions of the IPO regime:

    (a) defined limits on the issue of B-party warrants and the derivative use of material collected by a B-party warrant;

    (b) any increases to penalty thresholds for obtaining stored communications warrants should apply only to criminal offences; and

    (c) the threshold for sharing stored communications should be aligned with that prescribed in sections 110 and 139 of the TIA Act.

12. The Law Council would also support a greater level of oversight and accountability of the domestic regime. This includes the establishment of a warrant-based authorisation system to give agencies authority to access and disclose prospective telecommunications data, which would replace the internal authorisation-based model.

13. Further, neither the provisions of the Bill nor its extrinsic materials explain the intended interaction of the proposed IPO regime with the assistance and access regime enacted in Part 15 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**). The Law Council notes that the Independent National Security Legislation Monitor (**INLSM**) will shortly be making a number of recommendations for reform to this regime, and the PJCIS will examine those recommendations as part of its current inquiry into aspects of the TOLA Act. Importantly, the INSLM has indicated that he is considering issues arising from the interaction of the assistance and access regime with international agreements of the kind provided for in the CLOUD Act.[2]

14. Accordingly, the Law Council would prefer to see a suite of proposed amendments, ideally through the public release of a package of exposure draft Bills, so that issues concerning the interaction, alignment and combined impact of proposed measures can be identified and assessed collectively. Regrettably, the introduction of the present Bill, in the absence of broader reforms to telecommunications legislation, continues the practice of making piecemeal amendments to highly intrusive investigatory powers.

Outline of the proposed amendments

Key amendments

15. The primary objective of the Bill is to establish a framework to give domestic legal effect to future bilateral and multilateral agreements that Australia may enter into with foreign countries, for the purpose of reciprocally obtaining and granting cross-border access to electronic communications and related data. Australia is presently negotiating a bilateral agreement of this kind with the United States, which is supported on the United States' side by the CLOUD Act.

16. The key amendments are in Part 1 of Schedule 1 to the Bill. They propose to insert Schedule 1 to the TIA Act to establish the new framework to implement domestically

[2] James Renwick SC, Independent National Security Legislation Monitor, *What are the Right Encryption Laws for Australia*, Speech to the Lowy Institute, Sydney, 5 March 2020 <https://www.lowyinstitute.org/publications> 10-11.

executive agreements between Australia and foreign countries, and make consequential amendments to other legislation to enable the framework to operate.

17. In particular, Schedule 1 to the Bill proposes to amend the TIA Act to:

    (a) Insert Schedule 1 to that Act to provide a framework for Australian law enforcement agencies and ASIO to obtain independently-authorised IPOs. These orders, which may be described as 'outgoing IPOs', will request DCPs located outside Australia to intercept electronic communications, and access stored communications and communications data. IPOs will extend beyond telecommunications-related information, and cover a wide range of electronic communications, including social media forums and private messaging applications. The framework under proposed Schedule 1 to the TIA Act will be enlivened if Australia has entered into an executive agreement with a foreign country, which has been prescribed by regulations as a DIA.

    (b) Make amendments to provisions of the TIA Act and related legislation (including the Telecommunications Act and the *Privacy Act 1988* (Cth)) to enable DCPs located in Australia to comply with 'incoming IPOs', which are requests made by foreign countries with which Australia has a DIA for Australian communications providers to intercept electronic communications, or access stored communications and communications data. The proposed amendments remove otherwise applicable statutory prohibitions on interception and access and subsequent disclosure of information, by deeming compliance with an 'incoming IPO' to be lawful authority for those activities.

18. The proposed legislative framework is not directed to the making of agreements with any particular country. However, the prospect of a bilateral agreement with the United States is likely to be a significant impetus for the introduction of the Bill, given that many major global communications providers are based in that country. The Law Council is aware that the United States and the United Kingdom concluded a bilateral agreement in October 2019,[3] which is before their respective legislatures for scrutiny and is anticipated will commence on 8 July 2020. To the Law Council's knowledge, this is the first agreement that the United States has made under the CLOUD Act, and the first that the United Kingdom has made under its framework legislation, the *Crime (Overseas Production Orders) Act 2019* (UK).

19. The Law Council notes that the movement of the United States and the United Kingdom towards a system of executive agreements for reciprocal access to cross-border electronic communications and data directly from communications providers has arisen from law enforcement agencies' concerns about the operation of the present framework for the provision of mutual legal assistance in criminal matters. It has been said that present arrangements operate too slowly to be effective in the investigation and enforcement of serious crime and other national security matters in the fast-paced digital environment.[4] It appears that the new framework would effectively supersede existing mutual legal assistance treaties with respect to electronic communications information and telecommunications data.

[3] *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, United Kingdom-United States of America, signed 3 October 2019, (not yet in force).
[4] Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth), [5].

Other amendments

20. Parts 3 and 4 of Schedule 1 to the Bill also propose minor and technical amendments to the TIA Act and the *Surveillance Devices Act 2004* (Cth) to update or remove spent provisions, correct drafting errors that had no legal effect, and make amendments contingent on the commencement of the proposed *Federal Circuit and Family Court of Australia Act 2020* to manage the circumstance that the two Bills are before Parliament concurrently. The Law Council makes no comment on these provisions.

Parliamentary scrutiny of Designated International Agreements

21. A bilateral or multilateral agreement between Australia and foreign governments for the cross-border collection and sharing of electronic communications information will trigger the application of the IPO scheme under proposed Schedule 1 to the TIA Act **only** if it is prescribed in regulations made under that Schedule.[5]

22. Regulations designating an agreement as a DIA are subject to Parliamentary disallowance under Part 2 of Chapter 3 of the *Legislation Act 2003* (Cth) in the absence of any contrary provision in the Bill.[6] The Explanatory Memorandum states that the Government intends to publish DIAs in the Australian Treaties Library (a publicly available online database, hosted by the Australasian Legal Information Institute and funded by the Australian Government).[7]

23. In broad terms, the proposed arrangements are similar to the existing process for the domestic implementation of mutual legal assistance treaties as between Australia and foreign countries.[8] However, there are some apparent limitations in the scope of Parliamentary scrutiny of proposed DIAs. These limitations, which are outlined below, may amount to a diminution of the role of Parliament in comparison with its present role in relation to the scrutiny of mutual legal assistance treaties.

24. Given the apparent policy intention that the IPO regime would largely replace the mutual legal assistance framework in relation to intercepting and accessing electronic communications in criminal law enforcement investigations, the Law Council considers that the arrangements for the Parliamentary scrutiny of DIAs under the proposed IPO regime should be consistent with the existing arrangements for the scrutiny of mutual legal assistance treaties. The Law Council notes that the concerns identified about inefficiencies in the mutual legal assistance framework are specifically about its operation, and not the process of Parliamentary scrutiny of proposed treaty actions, or regulations giving effect to those actions.

Role of JSCOT in the scrutiny of proposed DIAs

25. The extrinsic materials to the Bill do not contain an explicit statement as to whether there is a policy intent for agreements prescribed as DIAs to be binding upon Australia under international law, and therefore classified as 'treaties' for the purpose of the Australian Treaty Making Framework.

---

[5] Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) ('Bill'), item 43, inserting proposed Schedule 1 to the TIA Act, subclauses 3(1) and 3(3).
[6] *Legislation Act 2003* (Cth), sections 42 and 44.
[7] Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth) [71].
[8] *Mutual Assistance in Criminal Matters Act* 1987 (Cth), section 7.

26. This framework prescribes a series of administrative measures for the making and domestic implementation of treaties by Australia, and was developed and implemented in its contemporary form in 1996 as part of a package of reforms to improve the openness and transparency of the treaty-making process in Australia, following a number of executive and parliamentary reviews.[9] A 'treaty' for the purpose of the framework is an agreement as between two States (countries) that is binding at international law, irrespective of the particular name given to the instrument recording the agreement.[10]

27. Significantly, the Australian Treaty Making Framework includes provision for the Parliamentary tabling of all treaties entered into by Australia, together with an accompanying statement of National Interest Analysis (**NIA**). It also provides for the routine scrutiny of each treaty by JSCOT.[11] Presently, mutual assistance treaties as between Australia and foreign countries are subject to this framework, and JSCOT routinely examines and reports to both Houses of Parliament on new treaties.[12]

28. The IPO regime is likely to substantially supersede the mutual legal assistance framework with respect to the reciprocal collection and sharing of foreign electronic communications information in law enforcement investigations, in circumstances in which there is a choice between proceeding under the IPO regime or the mutual assistance regime. Consequently, any exclusion of DIAs from the Australian Treaty Making Framework would mean that the new agreement-making framework would be subject to reduced Parliamentary scrutiny as compared to mutual assistance treaties, which presently cover the electronic communications information that is the subject of the new IPO regime.

29. In the absence of an express statement of contrary policy intent in the extrinsic materials to the Bill, the Law Council considers it unlikely that the efficiency-related objectives of the Bill are intended to be achieved through an effective reduction in the Parliamentary scrutiny of Australia's international agreement-making activities.

30. To avoid any doubt, and to maintain transparency and openness in the international agreement-making process, the Law Council considers it important that the Government makes a public commitment to utilising the existing Parliamentary scrutiny mechanisms under the Australian Treaty Making Framework, principally through JSCOT, in relation to international agreements that are proposed to be prescribed by regulations as DIAs. Conversely, if there is an intention to reduce Parliamentary scrutiny of international agreements as compared to existing arrangements for mutual assistance treaties, any such proposal should be directly acknowledged and justified. The Law Council is not aware of any suggestion that the process of Parliamentary scrutiny of proposed treaty actions is perceived to be causing or contributing to inefficiencies. The Law Council considers that the role of JSCOT enhances the treaty making and implementation process.

31. This process of scrutiny would involve the Parliamentary tabling of each agreement **before** regulations are made under the TIA Act to prescribe it as a DIA under Australian law, and the preparation and simultaneous tabling of an accompanying NIA with respect to the agreement. JSCOT would then conduct a review of the agreement

[9] Department of Foreign Affairs and Trade, *Australia International Treaty-Making Kit,* (web page, July 2000) <http://www.austlii.edu.au/au/other/dfat/reports/infokit.html>.
[10] Ibid.
[11] See further: JSCOT, Parliament of Australia, *Role of the Committee*, (web page) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Treaties.html>.
[12] For example, in the 45th Parliament, the Committee examined a mutual assistance treaty with the Hashemite Kingdom of Jordan. See: JSCOT, Parliament of Australia, *Extradition – Jordan; Mutual Assistance – Jordan* (Report 177, February 2018).

and provide an advisory report to Parliament on the proposed treaty action (which, in this case, would be the making of regulations to prescribe the agreement as a DIA under proposed Schedule 1 to the TIA Act).

Recommendation

- **The Government should provide a public assurance that the Australian Treaty Making Process, including the existing arrangements for Parliamentary scrutiny by JSCOT, will apply to all agreements made by Australia with foreign countries that are intended to be prescribed as DIAs in regulations made under Clause 3 of proposed Schedule 1 to the TIA Act.**

Requirement for DIAs to be appended to regulations and tabled in Parliament

32. The Bill contains a requirement for an agreement to be listed by name in regulations made under Clause 3 of proposed Schedule 1 to the TIA Act, in order for it to be recognised as a DIA for the purpose of the IPO scheme. However, there is no express statutory obligation imposed on the Government to proactively publish, or table in Parliament, the text of each DIA when the relevant regulations are made or tabled.

33. Although the Explanatory Memorandum notes an intention to publish individual DIAs in the Australian Treaties Library, it is silent as to whether such publication is intended to occur at the same time as, or before, the regulations are registered on the Federal Register of Legislation (which triggers the obligation to table them in Parliament and, in turn, the commencement of the statutory disallowance period).[13] The Explanatory Memorandum is also silent as to whether there is a policy intention to adopt a consistent approach with the making of regulations under section 7 of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) (**Mutual Assistance Act**) to designate agreements between Australia and foreign countries as 'mutual legal assistance treaties' so as to enliven the framework in the Mutual Assistance Act. The text of the relevant mutual assistance treaties is routinely reproduced, in full, in schedules to those regulations.[14]

34. The absence of a legal requirement for the publication of the contents of DIA at the same time the regulations are registered creates a risk that the Parliament may have insufficient information or time to make informed decisions about the exercise of its disallowance power in individual cases. That is, there is no legal guarantee that the Parliament will have timely access to the text of the agreement whose name is contained in the regulations deeming it to be a DIA.

35. The Law Council acknowledges that it would be open to each House of Parliament, once regulations are tabled in Parliament, to exercise the discretionary power in section 41 of the Legislation Act to require the Government to make available the text of a DIA that is named in regulations made under Clause 3, at a specified time and

[13] See: *Legislation Act 2003* (Cth), ss 12, 15G-15K, 38, 39 and 42. (A legislative instrument must be registered on the Federal Register of Legislation once made, and generally commences on registration. Legislative instruments must be tabled in Parliament within six sitting days of registration. Disallowable legislative instruments may be disallowed if a Parliamentarian gives notice to move a disallowance motion within 15 sitting days of tabling, and the motion is carried or has not been disposed of within that 15-sitting day period.)
[14] See, eg, Schedule 1 to each of the following regulations: Mutual Assistance in Criminal Matters (United Kingdom) Regulations 1999; Mutual Assistance in Criminal Matters (United States of America) Regulations 1999; and Mutual Assistance in Criminal Matters (Canada) Regulations 1990.

place. The Law Council further acknowledges that it would be open to each House of Parliament to exercise its power to disallow the regulations if a request made under section 41 of the Legislation Act was not complied with. This may provide some practical assistance in ensuring that the text of a DIA is made publicly available within the statutory disallowance period for the relevant regulations.

36. However, the Law Council is concerned that this outcome would be reliant on the exercise of political discretion in individual cases. A model of request-based disclosure in reliance on section 41 of the Legislation Act may also reduce the time available to the Parliament to consider the exercise of its disallowance power, due to the time involved in issuing and awaiting compliance with a request to produce the text of a DIA during the disallowance period for the regulations. The Law Council considers that the availability of political discretion in these circumstances is not an acceptable substitute for a legal requirement that the Parliament and the public are routinely and pro-actively given timely access to the contents of all DIAs.

37. In contrast, in the United States, §2523(d)(2) of the CLOUD Act contains a requirement that the text of all international agreements must be presented to Congress. That provision also establishes a Congressional disallowance period of 180 days from the date of presentation, which is much longer than the 15 sitting day period in Australia under the *Legislation Act 2003* (Cth) (**Legislation Act**). Similarly, in the United Kingdom, subsections 1(5) and (6) of the *Crime (Overseas Production Orders) Act 2019* (UK) provide that, for an agreement between the United Kingdom and a foreign country (or countries) to be a taken as a 'relevant treaty' for the purpose of its equivalent cooperative scheme, a copy of that agreement must have been tabled in Parliament, in accordance with an existing statutory tabling requirement under section 20 of the *Constitutional Reform and Governance Act 2010* (UK) for all treaties entered into by the United Kingdom.

38. The Law Council considers that the most straightforward way to ensure that the Parliament has timely access to the text of a DIA is to amend the Bill to include an express requirement that regulations made under Clause 3 of proposed Schedule 1 to the TIA Act prescribing an agreement as a DIA must reproduce the full text of that agreement (for example, as a schedule to the regulations, as is the established practice for equivalent mutual assistance regulations).

39. This would ensure that the contents of all DIAs are made available publicly, immediately upon the making and registration of the relevant regulations. It will ensure that members of the Parliament have the maximum possible access to the text of the agreement, as soon as the regulation itself is available, to inform their decisions about moving or voting on a disallowance motion during the standard 15-day disallowance period. It will remove any risk that Parliamentarians may have to use part of the disallowance period to request and await provision of the text of the agreement. It will also remove any risk that there could be a lengthy delay between the making and registration of regulations, and the provision of the text of the agreement upon the tabling of the regulations in Parliament six sitting days after registration (which would otherwise be possible if the regulations were made and registered during a Parliamentary adjournment).

Recommendation

- **Clause 3 of proposed Schedule 1 to the TIA Act should be amended to provide that the regulations prescribing an agreement between Australia and a foreign country, or countries, as a DIA must reproduce the relevant agreement in full (for example, as a schedule).**

Commencement of regulations listing an agreement as a DIA

40. The Law Council supports the suggestion of the Senate Standing Committee for the Scrutiny of Bills that consideration should be given to deferring the commencement date for regulations made under Clause 3 of proposed Schedule 1 to the TIA Act until the Parliamentary disallowance period for those regulations has expired, to ensure that Parliament has an adequate opportunity to scrutinise the regulations in advance of their commencement.[15] The Law Council considers that this measure is important in view of the novel nature of the agreement-making framework proposed to be established by the Bill and the extensive intrusive and coercive powers it would confer.

41. In particular, the Law Council notes that the relevant timeframes under the Legislation Act for the Parliamentary tabling and disallowance of legislative instruments are calculated by reference to Parliamentary sitting days rather than calendar days.[16] Consequently, if a regulation listing an international agreement as a DIA is made, registered and commences[17] while the Parliament is adjourned, there may be a significant lapse of time before an opportunity for Parliamentary disallowance arises. This means it will be possible for the IPO regime to have been operational in relation to that DIA for a protracted period of time before the Parliament has an opportunity to scrutinise the regulation and consider whether it should be disallowed.

42. This circumstance may create a significant practical barrier to the Parliament's exercise of its disallowance power, in that the Parliament would need to weigh the disruption caused by the effective termination of the IPO regime for that DIA against any concerns it may have about the substance of the DIA. (For example, the allocation of significant public and private resources into taking actions and making arrangements in reliance on the DIA being implemented under Australian law; and the potential for disruption to, or complete frustration of, extant investigations that are utilising the IPO scheme to obtain evidence or intelligence.)

43. If the regulations did not commence until after the end of the Parliamentary disallowance period, the Parliament would have greater freedom to focus its decision-making on the prospective merits of implementing the agreement under Australian law, without being constrained by practical considerations arising from the cancellation of implementation measures that are already operational. Deferred commencement would also provide certainty for Australian IPO agencies, Australia's foreign partners and DCPs who may be required to provide information under the scheme.

---

[15] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 34-35.
[16] *Legislation Act 2003* (Cth), ss 38, 39 and 42. (A legislative instrument must be tabled within six sitting days of registration, and will be disallowed if a notice of motion for disallowance is given, and is carried or not disposed of, within 15 sitting days of tabling.)
[17] *Legislation Act 2003* (Cth), s 12. (A legislative instrument commences the day after it is registered, or at such other time as is specified in the instrument, subject to some limitations on retrospective commencement and application.)

Recommendation

- **Proposed Schedule 1 to the TIA Act should be amended to provide that regulations made under Clause 3 (listing an agreement as a DIA) do not commence until after the statutory disallowance period for those regulations under the *Legislation Act 2003* (Cth) has expired.**

Prohibition on prescribing classified agreements as DIAs

44. The statement of commitment in the Explanatory Memorandum that all DIAs will be made publicly available in the Australian Treaties Library appears to suggest that there is a policy intention for **all parts** of these agreements to be unclassified. The Law Council strongly supports this position. It is essential to the effective Parliamentary and public scrutiny of these agreements that their complete contents are publicly available. It is also critical to Australia's obligations under the *International Covenant on Civil and Political Rights* (**ICCPR**), under which permissible limitations to rights must be provided for 'by law', which requires the content of the relevant laws to be sufficiently certain and accessible, such that people are able to understand when an interference with their rights may be justified. Accordingly, the Law Council considers that DIAs must not include any classified information, including in annexures or schedules that are withheld from public dissemination.[18]

45. To remove any risk that a policy intention may arise in future for DIAs to include classified information, the Law Council recommends that the statutory definition of a DIA in Clause 3 of proposed Schedule 1 to the TIA Act is amended to provide expressly that, in order to be recognised as a DIA, an agreement must be unclassified **in its entirety**. This would prevent any classified provisions of individual agreements from triggering the application of the statutory IPO scheme to incoming and outgoing requests made to, and by, Australian authorities in accordance with the classified requirements in the agreement.

46. The Law Council notes that such an amendment to the Bill would only regulate the domestic statutory implementation of the agreements that Australia makes with foreign countries under proposed Schedule 1 to the TIA Act. It would not limit the existing prerogative of the executive government to enter into classified agreements with foreign countries (for example, in cross-border intelligence-sharing agreements).

Recommendation

- **Clause 3 of proposed Schedule 1 to the TIA Act should be amended to provide that, for an agreement with a foreign country or countries to be prescribed in regulations as a DIA, that agreement must be unclassified, in its entirety.**

[18] While the discussion in this submission focuses on the Parliamentary review and human rights compatibility of delegated legislation incorporating security classified materials, the Law Council also notes that this circumstance is likely to be material to the legality of the exercise of delegated legislative power to prescribe agreements as DIAs. In particular, it may be open a court to entertain a judicial review application seeking a declaration of invalidity in relation to regulations that purport to prescribe as a DIA an agreement whose contents are classified (in full or in part) on the basis of uncertainty or unreasonableness. Consequently, the Law Council's suggested amendment to expressly provide that a DIA must not contain classified information would also be a prudent means of managing legal risk to the validity of regulations. See further: DC Pearce and S Argument, *Delegated Legislation in Australia* (LexisNexis Butterworths 5th edition, 2017) chs 12, 22, 24.

Incorporation of agreements 'as in force from time-to-time'

47. The Law Council is concerned that Clause 182 of proposed Schedule 1 to the TIA Act purports to disapply an important protection in subsection 14(2) of the Legislation Act to regulations made under Clause 3 to list an agreement as a DIA.

48. Subsection 14(2) of the Legislation Act is an important safeguard to ensure that, when a legislative instrument (such as a regulation) incorporates other written material by reference, the legislative instrument only 'picks up' and makes part of the law the version of that other written material that was in force **at the time** the regulation was made. In other words, the regulation will not automatically be updated to incorporate the latest versions of the written material it has incorporated by reference. Rather, if the contents of the other written material are amended, a new regulation would need to be made to incorporate the latest version. This would invoke a new opportunity for Parliamentary scrutiny and disallowance of the amending regulation. This rule ensures that the content of the law, as contained in delegated legislation, is stable, readily known and accessible and is subject to appropriate Parliamentary scrutiny. However, an Act can displace the protective rule in subsection 14(2) of the Legislation Act by including an expression of contrary intention. Clause 182 of proposed Schedule 1 to the TIA Act is an expression of contrary intention.

49. The result of Clause 182 of the Bill disapplying subsection 14(2) of the Legislation Act is that, once regulations are made under Clause 3 to prescribe a named agreement with a foreign country as a DIA (and thereby enliven the IPO regime), the regulations will continue to recognise that agreement as a DIA even after it is amended. This means that the executive government is not required to table new regulations in Parliament (with a new disallowance period) whenever the relevant agreement is amended. Consequently, the Parliament is deprived of the opportunity to disallow potentially significant amendments to the agreement, in respect of which it may have exercised its disallowance power had those matters been included in the original version of the agreement when the regulations were tabled.

50. The Law Council submits that this is an inappropriate delegation of legislative power, as it gives the executive an almost unfettered capacity to change the substance of an agreement (including the removal of safeguards) without an opportunity for Parliamentary scrutiny to determine whether the agreement as amended should continue to attract the application of the statutory IPO regime. In view of the novel nature of the agreement-making framework proposed to be established by the Bill, and its authorisation of highly intrusive investigatory powers and the suspension of significant legal prohibitions under Australian laws, the Law Council considers that the Parliament should have a legally mandated role to scrutinise and disallow changes to agreements that are already prescribed as DIAs. In particular, the Parliament should have the power to disallow regulations purporting to enliven the IPO scheme to amended agreements, if the Parliament considers that the amendments render the agreement unsuitable to continue to trigger the domestic IPO scheme.

51. Further, the Law Council observes that the proposal to disapply the important protection conferred by subsection 14(2) of the Legislation Act to regulations made under Clause 3 makes it even more important that the primary legislation in proposed Schedule 1 prescribes the critical safeguards and other parameters that must be present in an agreement in order for it to be listed by regulation as a DIA. Otherwise,

safeguards in the individual agreement are vulnerable to unilateral removal by the executive government.[19]

52. The Law Council is also of the firm view that its comments and recommendations above about the publication of DIAs must apply equally to any amendments to the relevant international agreements, so that copies of the full text of any amendments must be made publicly available. This result would follow automatically if Clause 182 was amended so that it does not apply to regulations made under Clause 3, as it would be necessary to make amending regulations to prescribe amended agreements as DIAs for the purpose of enlivening the IPO scheme in Schedule 1 to the TIA Act. If Clause 182 is not amended as suggested, then it would be necessary for the Bill to impose a specific publication requirement for amendments to agreements.

53. The Law Council's previous comments and recommendation about the deferred commencement of regulations until after the Parliamentary disallowance period has ended should apply equally to amendments.

Recommendation

- **Clause 182 of proposed Schedule 1 to the TIA Act should be removed to the extent it applies to regulations made under Clause 3 to list an agreement as a DIA, so that subsection 14(2) of the Legislation Act applies to agreements named in those regulations**.

Adequacy of legislative human rights safeguards in the Bill

54. The IPO regime in proposed Schedule 1 to the TIA Act does not purport to legislatively limit the executive power of the Commonwealth to enter into cross-border information-sharing agreements with foreign countries, including on the basis of their human rights records. Rather, it applies a limitation to the delegation of legislative power that would enable the executive government to effectively 'trigger' the application of the domestic statutory IPO regime to implement those agreements, via the making of regulations prescribing them as DIAs.

55. It is therefore open to the Parliament to impose certain conditions on the exercise of this delegated legislative power, which are directed to the protection of human rights in relation to the use of information that Australian DCPs may provide to foreign countries pursuant to an 'incoming' IPO. In particular, it would be open to the Parliament to make the regulation-making power conditional on Ministerial satisfaction that the laws and practices of the foreign parties to the agreement contain adequate human rights protections. A statutory condition of this kind would provide an assurance that the electronic communications information obtained and shared by Australian DCPs with foreign governments under 'incoming' IPOs will not be used by those governments for purposes, or in a manner, that would conflict with Australia's human rights obligations, both under specific treaties and general international law.

[19] That is, if the Bill is not amended to remove Clause 182 (contrary to the Law Council's recommendation) then some protection could be derived from the fact that any amendments to an agreement which is already prescribed by regulation as a DIA must ensure that the agreement still has the character of a DIA, by complying with all applicable limitations, restrictions and conditions built into the statutory definition of a DIA. This tends in favour of including further human-rights based conditions as recommended in this submission, to help ensure that they cannot be subsequently removed from a DIA by making amendments to the agreement.

56. However, as drafted, Clause 3 of proposed Schedule 1 to the TIA Act imposes only one explicit human rights-based condition on the regulation-making power to prescribe an agreement as a DIA. This concerns the right to life, and specifically the use of Australian-sourced information in foreign criminal proceedings in which the death penalty is an available punishment. As explained below, the Law Council considers that this proposed condition, in its present form, does not adequately protect the right to life in death penalty cases.

57. Further, the Law Council considers that the proposed domestic legislative framework for IPOs contains inadequate safeguards in relation to several other human rights that are commonly engaged in the exercise of intrusive evidence and intelligence collection powers, and the subsequent use of the relevant information. These matters include:

- the prohibition on torture, cruel, inhuman or degrading treatment and punishment;
- the right to liberty and security of the person, particularly the prohibition on arbitrary detention; and
- the rights to privacy, freedom of expression, freedom of association, peaceful assembly and a fair trial.

58. In addition, the Law Council is concerned that the Bill provides inadequate safeguards for the rights of the child, in the case of 'incoming IPOs' that foreign countries may issue to Australian DCPs for the purpose of foreign authorities conducting investigations of children for law enforcement or intelligence purposes.[20]

59. The Law Council acknowledges that there may be an intention for individual DIAs to prescribe detailed safeguards with respect to these matters, which may be specific to the circumstances of each agreement. However, the Law Council considers that it would be unacceptable for Australia to leave these matters **entirely** to executive discretion, as factors influencing executive decisions about whether to enter into an agreement with a particular foreign country or countries, and the terms of individual agreements. This reflects that Australia lacks a comprehensive domestic legal framework for the protection of human rights, in the nature of a Federal Charter or Bill of Human Rights, that could invalidate incompatible actions. It is also notable that Australia's mutual assistance legislation and extradition legislation contains explicit limits on the matters that may be the subject of a mutual assistance or extradition request, which are directed to the protection of human rights. For example, there are limitations on the provision of assistance in respect of the investigation and enforcement of 'political offences' (essentially covering non-violent offences of a political character).[21]

60. The Law Council notes that the absence of an overarching Charter or Bill of Righs in Australia is a fundamental difference to the domestic legal frameworks of our Five Eyes partners. The individual enactments in the US and UK establishing their respective agreement-making frameworks for IPOs, and the bilateral agreement they have made pursuant to that legislation, operate in the context of those countries' broader legislative and constitutional arrangements for the protection of human rights, which do not have an equivalent under Australian law. Consequently, the Law Council

[20] The PJCHR has also expressed concern about the absence of human rights-based safeguards, and the inadequacy of conditions in relation to the use of information in death penalty proceedings to safeguard the right to life: PJCHR, *Scrutiny Report 4* (2020), 22-25. The Senate Standing Committee for the Scrutiny of Bills has made similar comments about an absence of privacy safeguards: Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 34-35.
[21] *Mutual Assistance in Criminal Matters Act 1987* (Cth), ss 8(1A) and 8(1B); *Extradition Act 1988* (Cth), s 7.

considers it is necessary for the primary legislation establishing the IPO regime under Australian law to include specific and detailed human rights protections.

61. Key issues with respect to the protection of particular human rights are set out below. In broad terms, the approach recommended by the Law Council is for the Bill to impose stronger conditions on regulation-making power in Clause 3 of proposed Schedule 1 to the TIA Act to prescribe agreements as DIAs. In particular, the Law Council supports a statutory prohibition on the making of regulations prescribing an agreement as a DIA, unless the Attorney-General has issued a certificate stating that he or she is reasonably satisfied that the agreement is compatible with key international human rights requirements, as listed in the recommendations below. The Law Council considers that regulations should be invalid if they do not comply with these conditions.[22] The Law Council notes that the Attorney-General's assessments of compatibility would include an assessment of whether any limitations imposed on those rights which can be permissibly limited are, in fact, permissible limitations (for example, by conducting an assessment of their necessity and proportionality to the achievement of a legitimate objective).

Protection of the right to life in foreign death penalty cases

62. Subclauses 3(2) and (5) of proposed Schedule 1 to the TIA Act require the Minister for Home Affairs to obtain an assurance from the relevant foreign country 'relating to the use, or non-use' in death penalty proceedings of 'Australian-sourced information' that is provided to a foreign country by an Australian DCP under an IPO. This is a pre-condition to the exercise of the regulation-making power to prescribe an agreement with a foreign country as a DIA. The Explanatory Memorandum states:

> *The policy intention of this provision is to give effect to Australia's long-standing bipartisan opposition to the death penalty in the context of reciprocal cross-border access to communications data, and complements existing death penalty safeguards across the full spectrum of Australia's international crime cooperation frameworks.*[23]

63. The Explanatory Memorandum argues that the Bill is compatible with the right to life because the regulation-making power is conditional on the Minister obtaining an assurance of the kind specified in subclauses 3(2) and 3(5), and in the absence of such an assurance, Australian DCPs will not have lawful authority under the IPO scheme to provide information requested by a foreign country.[24]

64. The Law Council has concerns with this assessment due to the breadth of the conditions prescribed in subclauses 3(2) and 3(5). These provisions use the broad ambulatory words 'relating to' to prescribe the requisite nexus between 'Australian-sourced information' and **either** its use or non-use by foreign countries in death penalty cases. There is no explicit requirement for the Minister to be reasonably satisfied that Australian sourced information will **only** be used in a manner that is compatible with international human rights obligations with respect to the right to life, and is consistent with Australia's bipartisan foreign policy position of opposing the death penalty in all countries.

---

[22] The Law Council considers that invalidity would be the legal consequence of non-compliance with a condition on the exercise of delegated legislative power, in the absence of a statutory 'no-invalidity' Clause which provides that the regulations are not invalidated by failure to comply with the condition. The Law Council would strongly oppose the inclusion of a 'no-invalidity' Clause, because its effect would be to remove the legal force from the human rights safeguards created by the relevant conditions.
[23] Explanatory Memorandum, [64].
[24] Ibid, [74].

65. For example, the conditions in subclauses 3(2) and 3(5) do not require the Minister to seek, or obtain, a categorical assurance from the relevant foreign government that Australian sourced information will not be used in death penalty proceedings in that foreign country; or will only be used for exculpatory purposes in such proceedings; or the death penalty will not be sought or carried out any case in which the foreign country has obtained Australian-sourced information for the purpose of its investigation and enforcement of offences that are punishable by death.[25]

66. Accordingly, in the absence of robust legislative parameters for the nature of the assurance that must be obtained from a foreign country, it may be possible to assert that the conditions under proposed subclauses 3(2) and (5) are capable of being satisfied by the receipt of an assurance from a foreign country that it intends to use Australian-sourced information in a manner that is **incompatible** with the general human right to life, and Australia's foreign policy position on the death penalty.

67. While the Law Council acknowledges that there is no apparent subjective policy intention for the IPO scheme to operate in this manner, it is concerned that the Bill does not provide a clear statutory limitation on the aberrant or improper exercise of the regulation-making power to prescribe agreements as DIAs. Although Parliament could decide to disallow regulations prescribing agreements as DIAs, if it formed the view that an agreement was incompatible with the right to life, a discretionary political decision to effectively 'veto' the individual exercise of a delegated legislative power is a considerably more limited form of protection than the imposition of a clear legal limitation on the delegation of the relevant legislative power in the first place.

68. In contrast, section 16 of the *Crime (Overseas Production Orders) Act 2019* (UK) amends section 52 of the *Investigatory Powers Act 2016* (UK) (**IPA**), which makes provision for telecommunications carriers and carriage service providers in the UK to intercept telecommunications pursuant to 'incoming' requests made by competent authorities of foreign countries with which the United Kingdom has made an agreement. This is provided that the relevant Secretary of State has made regulations designating the international agreement as a 'relevant foreign agreement' for the purpose of the IPA. The 2019 amendments inserted the requirement in subsection 52(7) of the IPA that the Secretary of State must not make such regulations unless he or she has sought from the other state party to the agreement 'a written assurance, or written assurances, relating to the **non-use** of information obtained by virtue of the agreement in connection with proceedings for a death penalty offence' (emphasis added).

69. The statutory obligation on the Secretary of State to seek an explicit 'non-use' undertaking before making regulations prescribing a 'relevant international agreement' is supplemented by the terms of the bilateral agreement between the US and the UK, in relation to the substance of undertakings provided by the US about the use of particular information in death penalty cases.

70. Article 8.4 of the agreement imposes limitations on the use and transfer of electronic communications information where an 'essential interest' of either country may be implicated. The United Kingdom has declared that its essential interests:

[25] These are identified as the key circumstances arising under subsection 8(1A) of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) in which the Attorney-General may make an exception to the statutory prohibition on sharing information in cases in which a person has been arrested for, charged with, or convicted of, an offence under the laws of another country which is punishable by death, if the Attorney-General's is satisfied that 'special circumstances' exist. See: Australian Government Attorney-General's Department, *Mutual Assistance – Foreign Requests to Australia* (web page) <https://www.ag.gov.au>.

> *… may be implicated by the introduction of such data as evidence in the prosecution's case in the United States for an offense for which the death penalty is sought;*[26]

71. The apparent effect of Article 8.4 is that the US is required to obtain the UK's permission prior to using electronic communications information obtained from the UK in criminal proceedings in which the prosecution seeks the imposition of the death penalty. The Law Council notes that the provisions of section 52 of the IPA and the above terms of the bilateral agreement between the UK and the US appear to fall short of imposing a wholesale prohibition on the UK providing information to foreign law enforcement authorities, including those of the US, for inculpatory purposes in foreign matters concerning the investigation and enforcement of offences which are punishable by death.

72. Nonetheless, the statutory requirement in subsection 52(7) of the IPA for the UK Secretary of State to seek an explicit undertaking from a foreign government with respect to the non-use of UK interception information in death penalty cases (to the exclusion of an undertaking about its use in some form) appears to be a stronger safeguard than the provisions in subclauses 3(2) and 3(5) of proposed Schedule 1 to the TIA Act.

Recommendation

Clause 3 of proposed Schedule 1 to the TIA Act should be amended to implement one of the following options.

<u>Option 1</u>

- **Clause 3 of proposed Schedule 1 to the TIA Act should be amended to provide that regulations prescribing an agreement as a DIA cannot be made unless the assurance obtained by the Minister for Home Affairs under Subclause 3(2) or 3(5) includes an assurance that Australian-sourced information will not be used by an authority of the foreign country in the prosecution of any offence for which the death penalty is a sentencing option.**

<u>Option 2</u>

- **Clause 3 of proposed Schedule 1 to the TIA Act should be amended to strengthen the conditions in subclauses 3(2) and 3(5) so that regulations prescribing an agreement as a DIA cannot be made unless the Minister for Home Affairs has obtained one of the following assurances from the foreign country or countries that are parties to the agreement:**

  (a) Australian sourced information will not be used in death penalty cases; or

  (b) Australian sourced information will be used, but the death penalty will not be sought or carried out; or

  (c) Australian sourced information will be used only for exculpatory purposes.

[26] *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, United Kingdom-United States of America, signed 3 October 2019, (not yet in force).

Statutory conditions for the protection of other human rights

73. The Law Council is concerned that the proposed regulation-making power in Clause 3 of proposed Schedule 1 to the TIA Act to prescribe individual agreements as DIAs does not impose further preconditions for the protection of human rights in addition to the right to life.

74. As discussed below, the Bill does not contain any explicit conditions for the protection of rights which are commonly engaged in the exercise of intrusive collection powers in law enforcement and intelligence investigations. In particular, the Law Council notes that the proposed regulation-making power is not subject to conditions that would require Australia to obtain prior assurances from foreign countries about their adherence to a range of international human rights obligations, and to be satisfied about the adequacy of those assurances.

75. This is in contrast with the approach taken under § 2523(b)(1) of the United States CLOUD Act, which prescribes conditions that bilateral or multilateral agreements between the United States and foreign countries must meet, in order to trigger the application of the cooperative framework under United States law, to enable United States-based communications providers to comply with foreign countries' requests for information. The CLOUD Act relevantly prescribes a condition in § 2523(b)(1)(B)(iii) that the Attorney-General (with the concurrence of the Secretary of State) has certified that he or she is satisfied that the relevant foreign country 'adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights'. This includes a certification requirement in relation to the specific human rights listed in § 2523(b)(1)(B)(iii)(I)-(V), which cover: rights to privacy, freedom of expression, freedom of association and peaceful assembly; and prohibitions on arbitrary arrest and detention, and torture and cruel, inhuman or degrading treatment or punishment.

76. As set out below, the Law Council considers that the Australian IPO regime should adopt further statutory pre-conditions to the exercise of the regulation-making power in Clause 3 of proposed Schedule 1 to the TIA Act. This should include an analogous condition for the Attorney-General's certification of the foreign country's respect for and adherence to the human rights listed in § 2523(b)(1)(B)(iii)(I)-(V) of the CLOUD Act.

Prohibitions on torture and cruel, inhuman or degrading treatment or punishment

77. The Law Council considers that it is particularly important for Australia to obtain assurances from is foreign partners that Australian sourced information will not be used by an authority of a foreign country to subject a person to torture, cruel, inhuman or degrading treatment or punishment, or to arbitrarily detain a person (for example, the incommunicado detention of a person as part of a prolonged interrogation, or as a means of punishing a person without affording them a fair trial or hearing).

78. The inclusion of ASIO in the IPO framework suggests that Australia may intend to use the new scheme to enter into DIAs to enable the reciprocal cross-border collection of electronic communications information for security intelligence purposes, in addition to largely replacing mutual assistance in law enforcement investigations. The generally covert nature of intelligence agencies' activities makes it especially important that Australia is satisfied its foreign partners have enacted, and observe in practice, robust legal protections against these violations of human rights.

Rights to freedom of expression, association and peaceful assembly

79. Further, it is important that Australian-sourced information is not used by a foreign country to prosecute a person for politically motivated reasons. Notably, Australia's mutual assistance and extradition laws include specific exclusions and other limitations in relation to the foreign investigation or prosecution of individuals for 'political offences' (essentially covering non-violent offences of a political character).[27]

80. It is conceivable that foreign countries may seek to utilise the IPO regime for the investigation and enforcement of their domestic national security offences, including offences in the nature of terrorism, sabotage, sedition, treason and the disruption of public order. The inclusion of an equivalent safeguard in the IPO regime with respect to cooperation in cases involving 'political offences' will be important to ensure that Australian-sourced information is not provided to foreign governments for improper purposes, such as suppressing acts of non-violent advocacy, protest, dissent, discussion or debate and assembly.

Right to privacy

81. Given that the information which may be subject to an IPO includes the contents of, and other data pertaining to, private electronic communications, it is important that Australia is satisfied that its foreign partners have implemented arrangements under their domestic laws for the protection of personal privacy in relation to Australian-sourced information. This includes appropriate domestic legal thresholds for the issuing of orders authorising the collection of the relevant information, which ensure that the proposed collection is necessary for and proportionate to a legitimate objective. It also includes arrangements for the subsequent use, handling, dissemination, retention or destruction of that information by foreign authorities.

Recommendation

- **Clause 3 of proposed Schedule 1 to the TIA Act should be amended to provide that the power to make regulations prescribing an agreement as a DIA must not be exercised unless the Attorney-General has issued a certificate attesting that he or she is reasonably satisfied of all of the matters listed in § 2523(b)(1)(B)(iii) of the US CLOUD Act, with respect to the foreign country's adherence to, and respect for, human rights. Regulations that do not comply with this requirement would be invalid.**

Rights of the child

82. The regulation-making power in Clause 3 of proposed Schedule 1 to the TIA Act does not contain any conditions that would require Australia to assess and be satisfied of the adequacy of safeguards in the laws and practices of foreign countries with respect to their use of Australian-sourced information in the investigation or prosecution of children. The absence of specific safeguards in relation to children, which would apply in addition to the general safeguards discussed above, may be incompatible with Australia's obligations under the *Convention of the Rights of the Child* (**CRC**).[28]

83. In particular, the Bill does not contain dedicated statutory safeguards to eliminate the possibility that Australian DCPs could be issued with requests by foreign authorities,

[27] *Mutual Assistance in Criminal Matters Act 1987* (Cth), ss 8(1A) and 8(1B); *Extradition Act 1988* (Cth), s 7.
[28] *Convention on the Rights of the Child,* opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990), art 11.

seeking information for the purpose of investigating or prosecuting children who are under the minimum ages of criminal responsibility in Australia. Further, the Bill does not contain specific statutory safeguards against the possibility that the Australian legislative framework for IPOs could operate to provide Australian-sourced information to a foreign authority for the purpose of that authority prosecuting, as adults, young people who are 16 or 17 years of age. For example, the US is not a party to the CRC, and 33 of its states have no minimum age of criminal responsibility.[29] Additionally, 9 US states have an 'upper age' of juvenile court jurisdiction of less than 17 years (being the oldest age at which an individual can come under the original jurisdiction of a juvenile court).[30]

84. The Law Council therefore recommends the imposition of an additional statutory condition on the regulation-making power to prescribe an agreement as a DIA. Such a condition should make specific provision for the protection of the rights of children in relation to the use by foreign countries of Australian-sourced information obtained under an IPO. In particular, it should provide that regulations cannot be made unless the Attorney-General certifies that he or she is reasonably satisfied that the relevant foreign country has implemented, and observes in practice, appropriate domestic legal protections for the rights of children in its jurisdiction. This should be additional to the certification condition recommended above, in relation to the human rights listed in § 2523(b)(1)(B)(iii) of the US CLOUD Act, which apply to all persons.

Recommendation

- **Clause 3 of proposed Schedule 1 to the TIA Act should be amended to include a specific condition on the power to make regulations listing an agreement as a DIA, to effectively limit the use by foreign countries of Australian-sourced information in their investigations and prosecutions of children. This should include an express condition to ensure that a foreign country will not use Australian-sourced information in the prosecution of children below the applicable age of criminal responsibility in Australia.**

Applications for IPOs by Australian authorities

Justification for including ASIO in the IPO scheme

85. The justification given in the Explanatory Memorandum for the establishment of the IPO scheme appears to focus on limitations in the timeliness and efficiency of the mutual legal assistance process.[31] That process is limited to the investigation of serious criminal offences by law enforcement agencies. It does not extend to arrangements for the collection outside Australia of intelligence for ASIO.[32]

86. No specific justification appears to be given for the inclusion of ASIO in the IPO scheme, in the form of 'national security IPOs' issued on that agency's application. ASIO is presently governed by the provisions of section 19 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) with respect to its cooperation with foreign entities, subject to further requirements of the TIA Act and

[29] Juvenile Justice, Geography, Policy, Practice & Statistics: A project from the National Center for Juvenile Justice, 'Jurisdictional Boundaries', *Jurisdictional boundaries - JJGPS - Juvenile Justice, Geography, Policy, Practice & Statistics* (Web page) <http://www.jjgps.org/jurisdictional-boundaries#age-boundaries>.
[30] Ibid.
[31] Explanatory Memorandum, [5].
[32] See, eg, *Mutual Assistance in Criminal Matters Act 1987* (Cth), section 5.

Telecommunications Act regulating disclosures of various types of telecommunications information.

87. Consequently, no evidence has been presented publicly about perceived shortcomings in these provisions that would require ASIO to be given the ability to obtain IPOs under proposed Schedule 1 to the TIA Act. This is a significant measure, as the enforceable nature of ASIO's national security IPOs against foreign DCPs could expose those entities to significant civil penalties of up to $9.6 million, and may therefore effectively amount to the conferral of a new coercive collection power upon, or for the benefit of, an intelligence agency. The Law Council considers that measures that directly or indirectly confer coercive collection powers on intelligence agencies are extraordinary, and all proposals for the enactment of such measures must be supported by a specific and rigorous public justification.

88. The absence of a clear case in the extrinsic materials to the present Bill for the inclusion of ASIO in the IPO regime renders it impossible to assess the perceived necessity of the proposed category of 'national security IPOs'.[33] In particular, the absence of this information precludes an assessment of the intended interaction of the proposed IPO regime with ASIO's existing foreign cooperation mechanisms to obtain relevant intelligence directly or indirectly from foreign DCPs. It is unclear, on the face of the individual provisions, when it is intended that ASIO will rely on its existing statutory cooperation arrangements with foreign entities, and when it will have recourse to national security IPOs.

89. The Law Council notes that, in contrast to the present Bill, the statutory agreement-making frameworks established under the US CLOUD Act and the *Crime (Overseas Production Orders) Act 2019* (UK) are restricted to the purpose of providing information for law enforcement activities in relation to serious crime (namely, prevention, detection, investigation and prosecution).[34]

90. However, the Law Council acknowledges that the UK's Investigatory Powers Act also makes separate provision for the extraterritorial operation of certain warrants issued to its domestic investigatory agencies under that Act, for the purpose their accessing telecommunications data that is not covered by the UK's Overseas Production Orders regime.[35] Further, the authorisation under section 52 of the IPA for entities in the UK to intercept domestic telecommunications pursuant to a request made by a 'competent authority' of a foreign country under a 'relevant international agreement' between the UK and the relevant foreign country is not limited to requests made by foreign law enforcement agencies, or for the purpose of investigating serious crime. It therefore appears capable of supporting agreements governing requests made to UK-based communications providers by foreign intelligence agencies.

91. Consequently, it would **not** appear possible for ASIO to be part of arrangements contained in a bilateral DIA between Australia and the US that is made under the domestic framework established by the CLOUD Act on the US's side and proposed Schedule 1 to the TIA Act on Australia's side. However, it may be possible for ASIO to

[33] The PJCHR made a similar observation: PJCHR, *Scrutiny Report 4* (2020), 15-16.
[34] *CLOUD Act*, §2523(b)(4)(D)(i); (Attorney-General must certify that an executive agreement between the US and a foreign country would enable the foreign country to issue production orders to US-based entities for purposes relating to serious crime); and *Crime (Overseas Production Orders) Act 2019* (UK), s 2 (definition of an 'appropriate officer' who is authorised to apply for an overseas production order under s 1). Article 1 of the US-UK bilateral agreement defines a 'serious crime' as an offence which is punishable by a maximum penalty of imprisonment of at least three years.
[35] See, eg, *Investigatory Powers Act 2016* (UK), section 85 (extraterritorial application of authorisations for obtaining communications data under Part 3) and section 97 (extra-territorial application of data retention notices issued under Part 4).

be included in certain cooperative arrangements made under bilateral or multilateral DIAs between Australia and other foreign partners, such as the UK, whose domestic legislative frameworks support the making of agreements for the reciprocal issuing of requests for cross-border intelligence collection.

Recommendation:

- **The Government should provide an unclassified explanation of the perceived need to include ASIO in the IPO scheme, including an explanation of the reasons that ASIO's existing foreign cooperation mechanisms are considered inadequate. The Explanatory Memorandum to the Bill should be amended to include that explanation. There should be an adequate opportunity for Parliamentary and public scrutiny of that explanation before the Bill is passed.**

Agencies that may obtain law enforcement IPOs

Inappropriate delegation of legislative power – prescription of additional 'criminal-law enforcement' and 'enforcement' agencies by legislative instrument

92. The Bill relevantly provides that 'criminal-law enforcement' and 'enforcement' agencies may respectively obtain IPOs to access offshore stored communications and telecommunications data.[36] These terms take their meanings from the existing provisions of the TIA Act governing domestic interception and access.[37] In addition to listing certain 'criminal-law enforcement' and 'enforcement' agencies by name, the definitions of these terms in the existing provisions of the TIA Act empower the Minister for Home Affairs to make legislative instruments designating further agencies in respect of some, or all, of their functions.[38]

93. The legal effect of the proposed IPO regime applying the definitions of 'criminal-law enforcement' and 'enforcement' agencies under the domestic interception and access regime is that the agencies which can obtain law enforcement IPOs will be varied administratively, as the Minister makes or repeals legislative instruments prescribing agencies for the purpose of the domestic regime. The Law Council is concerned that the Bill does not contain any requirement for the Minister to **specifically** consider whether the agencies prescribed by legislative instrument as 'criminal-law enforcement' and 'enforcement' agencies under the domestic regime are **also** suitable to exercise the powers under the IPO regime. This is compounded by the fact that, to the Law Council's knowledge, there are presently no such agencies prescribed as 'criminal-law enforcement' and 'enforcement' agencies for the purposes of the domestic interception and access regime under existing sections 110A and 176A of the TIA Act. The Parliament has therefore not had occasion to consider the appropriateness of any agencies prescribed for the purpose of the domestic regime, before being called upon to enable any such agencies to also apply for IPOs.

94. Further, the absence of a dedicated statutory requirement for the Minister to specifically consider and be reasonably satisfied of the suitability of 'criminal-law enforcement' and 'enforcement' agencies to exercise powers under the IPO scheme creates a risk to the effectiveness of parliamentary scrutiny of the relevant legislative

[36] Bill, item 43 (inserting proposed Schedule 1 to the TIA Act). See paragraphs (b) and (c) of the definition of 'relevant agency' in proposed Clause 2 of Schedule 1.
[37] *Telecommunications (Interception and Access) Act 1979* (Cth) s 110A (criminal law-enforcement agency) and s 176A (enforcement agency).
[38] Ibid s 110A(3) (criminal-law enforcement agencies) and ss 176A(1)(b) and (7) (enforcement agencies).

instruments prescribing those agencies. For example, there is a risk that explanatory statements accompanying legislative instruments made under the domestic interception and access regime may not consistently identify and justify their impacts on the IPO scheme. This may mean that Parliament is not consistently alerted to the issue, and the matter may go unnoticed in individual instances.

Recommendation

- **Proposed Schedule 1 to the TIA Act should be amended to define the terms 'criminal-law enforcement agency' and 'enforcement agency' for the purpose of the IPO scheme, by reference to the entities that are listed by name in existing ss 110A and 176A of the *TIA Act.***
- **The Bill should further provide that the Minister for Home Affairs may make a separate, disallowable legislative instrument under proposed Schedule 1 to the TIA Act declaring further entities to be 'criminal-law enforcement' or 'enforcement' agencies for the purpose of the IPO scheme (in respect of some or all of their functions).**

Anomalies in certain powers of authorisation and delegation

95. There are some anomalies in provisions of proposed Schedule 1 to the TIA Act that authorise officials of relevant agencies to apply for law enforcement IPOs for the interception of communications;[39] and other provisions which confer certain powers of delegation on the Director-General of Security with respect to the revocation of ASIO's national security IPOs.[40] The Law Council recommends some targeted amendments to the Bill to remove these anomalies, as outlined below:

Statutory authorisations of staff members of 'relevant agencies' to apply for law enforcement interception IPOs

96. Various senior officials, members and other staff of 'interception agencies'[41] (as a subset of the 'relevant agencies') are authorised to apply for a law enforcement IPO for the interception of communications.[42] However, only one authorisation provision, in relation to applications made by the Australian Commission for Law Enforcement Integrity, requires the relevant agency head to personally authorise their staff members to make such an application.[43] The remaining provisions directly authorise various officials of the other interception agencies to make IPO applications without the need for specific approval by the agency head.

[39] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, subclauses 22(3), 33(3)(a), 52(3)(a) and 63(3)(a).
[40] Ibid Clause 119.
[41] An 'interception agency' for the purpose of proposed Schedule 1 to the TIA Act is defined in existing section 5 of the TIA Act. It relevantly includes 'Commonwealth authorities' (being the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Commissioner for Law Enforcement Integrity) and certain 'eligible State authorities' (being State and Territory police and anti-corruption bodies that are prescribed in legislative instruments made by the Minister for Home Affairs, on the request of a State or Territory premier).
[42] Bill, Schedule 1 to the TIA Act, Subclause 22(3) (applications for law enforcement interception IPOs for the purpose of interception). See also corresponding application requirements in Subclause 33(3)(a) (law enforcement stored communications IPOs), and subclauses 52(3)(a) and 63(3)(a) (control order interception and stored communications IPOs).
[43] Bill, item 43, inserting Schedule 1 to the TIA Act, Subclause 22(3)(b)(iii) (applications for law enforcement interception IPOs for the purpose of interception). See also corresponding application requirements in Subclause 33(3)(a) (law enforcement stored communications IPOs), and subclauses 52(3)(a) and 63(3)(a) (control order interception and stored communications IPOs).

97. In contrast, the provisions governing the making of applications for ASIO's national security IPOs state that the only persons who may apply for an IPO for interception or access to stored communications are the Director-General of Security, a Deputy Director-General or an ASIO employee who is authorised by the Director-General (either individually or as part of a specified class of employees).[44]

98. The Director-General's power to authorise **any** ASIO employee or class of employees is broad, as it is not limited by reference to the seniority of individual ASIO employees or classes of employees.[45] However, the requirement for Director-General to personally make authorisations is a stronger degree of oversight than the corresponding provisions governing the making of applications for law enforcement IPOs. The Director-General of Security, as the head of ASIO, is required to specifically consider the appropriateness of particular authorisations.

99. In the absence of an explanation for the differential treatment of provisions authorising individual applicants for law enforcement and national security IPOs, the Law Council considers that these provisions should be aligned.

Recommendation

- **The provisions authorising 'interception agencies' to apply for IPOs in subclauses 22(3), 33(3)(a), 52(3)(a) and 63(3)(a) of proposed Schedule 1 to the TIA Act should be amended to require agency heads to personally authorise any applicant for an IPO who is a 'member', 'staff member', 'official' whose position is not explicitly identified by reference to a designated level of seniority.**
- **Consideration should also be given to amending subclauses 83(3) and 92(3) of proposed Schedule 1 to the TIA Act, to limit the Director-General of Security's power of authorisation to a defined class of ASIO employees by reference to seniority, such as 'senior position holders' as defined in section 4 of the ASIO Act.**

Delegation of Director-General's power to revoke ASIO's national security IPOs

100. Clause 116 of proposed Schedule 1 to the TIA Act confers mandatory and discretionary powers on the Director-General of Security to revoke ASIO's national security IPOs. Clause 119 empowers the Director-General to delegate their powers to revoke IPOs to a Deputy Director-General or **any** ASIO employee.

101. This is in contrast to the corresponding power of delegation conferred on 'criminal-law enforcement' and 'enforcement' agency heads under Clause 118, who may only delegate their powers of revocation under Clause 114 to 'certifying officers' of the agency. The latter term is defined in existing section 5AC of the TIA Act, by reference to the seniority of particular position-holders within the agency.

102. In the absence of explanation for this apparent discrepancy, the Law Council considers that the power of delegation in relation to the revocation of ASIO's national

[44] Bill, item 43, inserting Schedule 1 to the TIA Act, subclauses 83(3) (applications for national security interception IPOs) and 92(3) (applications for national security stored communications IPOs).
[45] The Law Council notes that the Senate Standing Committee for the Scrutiny of Bills has queried whether the Director-General's power of authorisation could be limited to a prescribed class of ASIO officials: Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 28-29.

security IPOs should be made consistent with the scope of the power of delegation in relation to the revocation of law enforcement IPOs.

103. Relevantly, section 5AD of the TIA Act defines a 'certifying person' in relation to ASIO (which is the equivalent concept to a 'certifying officer' of a 'criminal-law enforcement' or 'enforcement' agency) as a 'senior position holder' as defined in section 4 of the ASIO Act (being a position that is classified as Senior Executive Service Band 1 or is designated as Coordinator).

Recommendation

- **Clause 119 of proposed Schedule 1 to the TIA Act should be amended so that the Director-General of Security may only delegate their powers under Clause 116 to revoke national security IPOs to a Deputy Director-General and 'senior position holders' within the meaning of that term in section 4 of the *ASIO Act,* rather than any ASIO employee.**

Issuing of IPOs

Law enforcement IPOs

Appropriateness of AAT members as an issuing authority

104. Under Parts 2 and 3 of proposed Schedule 1 to the TIA Act, law enforcement and control order IPOs may be issued by a judicial officer who is appointed *persona designata* by the Attorney-General; or a member of the Administrative Appeals Tribunal (**AAT**) of any level who is appointed by the Attorney-General, provided that the person has been admitted as a lawyer for at least five years.[46]

105. The Law Council welcomes, in principle, the requirement that an IPO be approved by an independent third party, who is demonstrably at arm's length from IPO agencies and Ministers. However, the Law Council considers that responsibility for issuing an IPO for law enforcement agencies should be limited to judicial officers; or in the alternative, extended only to an AAT Deputy President, senior member or a member of the Security Division who has been admitted as a lawyer for at least five years.

106. In particular, the Law Council considers that the requirement for a judicial officer to authorise the issue of an IPO provides greater independence, both substantive and perceived, in the approval process for IPOs. Even while acting *persona designata*, a judicial officer must act consistently with the essential requirements of the judicial process. This includes the independence and impartiality of their decision making, their application of the rules of natural justice, and their ascertainment of the law and facts followed by an application of the law to the facts as determined.[47]

107. Further, judicial officers are typically people of exceptionally high integrity, intellect, seniority and standing in the community, and have extensive experience and proficiency in the adjudication of matters involving the identification and application of the law to the ascertained facts of a case. The Law Council considers that focusing

[46] Ibid, clauses 14-16 (definitions of 'issuing authority' for the purpose of stored communications and telecommunications data IPOs, and 'eligible judge' and 'nominated AAT member' for the purpose of interception IPOs).
[47] See, for example, *Harris v Caladine* (1991) 172 CLR 84 [18] (Gaudron J). See also: Parliamentary Joint Committee on Human Rights, *Scrutiny Report 4* (2020), 9; and Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 25-26.

the pool of persons able to be appointed as issuing authorities to judicial officers would materially assist Australia to enter into an 'executive agreement' with the US under the CLOUD Act by implementing the type of safeguards required for Australia to be eligible for such an agreement. The Law Council notes that the UK (which has recently concluded its bilateral agreement with the US) has appointed judicial officers as issuing authorities for its 'outgoing' overseas production orders.[48]

108. While the Law Council has a very strong preference for the functions of issuing authorities to comprise judicial officers alone, it also acknowledges the considerable workload of judicial officers in discharging their judicial functions, and the need for a sizeable pool of experienced issuing authorities of appropriate seniority, to ensure their availability including in urgent cases. Accordingly, while it is not the preferred option, if there is no intention to remove AAT members as issuing authorities under the Bill, the Law Council would not oppose the inclusion of Deputy Presidential and Senior Members of the AAT, and members of the Security Division in the pool of officers eligible for appointment as issuing authorities.

Recommendation

- **The issuing of law enforcement and control order IPOs should be restricted to 'eligible judges', rather than members of the AAT.**
- **Alternatively, AAT members who can issue law enforcement IPOs should be restricted to Deputy Presidential and senior members, and members of the Security Division who have been admitted as Australian lawyers for a minimum of five years.**

ASIO's national security IPOs

Issuing authorities – exclusion of judicial officers

109. The Bill proposes to establish a two-staged mechanism for the authorisation ASIO's national security IPOs seeking the interception of telecommunications or access to stored communications. This is in contrast to existing requirements for ASIO's domestic telecommunications and special powers warrants, which are issued by the Attorney-General.[49]

110. The first stage is a requirement that ASIO must obtain the consent of the Attorney-General to make an application for an IPO to an independent issuing authority, who is a 'nominated member' of the Security Division of the AAT appointed by the Attorney-General as an issuing authority for the purpose of ASIO's national security IPOs.[50] The second stage is a decision on that application by a nominated member of the Security Division of the AAT.[51]

111. However, there is an unexplained discrepancy as between the second stage for the issuing of ASIO's national security IPOs under Part 4 of proposed Schedule 1 to the TIA Act, and issuing authorities appointed to determine applications by law

[48] *Crime (Overseas Production Orders) Act 2019* (UK) s 1(7). Further, investigatory powers warrants with extraterritorial application are subject to the 'double lock' authorisation process in the *Investigatory Powers Act 2016* (UK) which mandates review by retired senior judges ('Judicial Commissioners') of ministerial approval.
[49] TIA Act, Part 2-2 (interception warrants) and Part 3-2 (stored communications warrants); and ASIO Act, Part III, Division 2 (special powers warrants)
[50] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, subclauses 83(5)-(7) (interception IPOs) and subclauses 92(5)-(6) (stored communications IPOs).
[51] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, clauses 89-90 (interception IPOs) and clauses 98-99 (stored communications IPOs).

enforcement agencies for law enforcement and control order IPOs under Parts 2 and 3. This discrepancy concerns the identity of the relevant issuing authorities.

112. The sole class of persons who may be appointed by the Attorney-General as issuing authorities for ASIO's national security IPOs are members of the Security Division of the AAT.[52] However, as mentioned above, law enforcement and control order IPOs may be variously issued by a judicial officer who is appointed *persona designata*, or by nominated AAT members.[53]

113. No justification is given for the differential treatment of ASIO's national security IPO applications in this regard.[54] It may potentially reflect a level of comfort with the established procedures, experience and security infrastructure of the AAT Security Division in dealing with reviewable matters pertaining to ASIO's activities (primarily the merits review of eligible security assessment decisions under Part IV of the ASIO Act).[55] There may also be a desire to limit the dissemination of sensitive information about ASIO's operations by limiting the classes of persons who may be appointed to issue national security IPOs.

114. However, the Law Council is of the firm view that the legitimate national interest in protecting sensitive information about ASIO's operations does not rationally preclude the *persona designata* appointment of judicial officers as issuing authorities for national security IPOs. The Law Council supports amendments to the Bill that would make **both** judicial officers and members of the AAT Security Division eligible for appointment as issuing authorities for ASIO's national security IPOs.

115. In the absence of an explanation in the extrinsic materials to the Bill, there does not appear to be a cogent basis upon which to support the apparent policy position that judicial officers are considered to be suitable issuing authorities for law enforcement IPOs, but not in relation to ASIO's national security IPOs.

116. This distinction seems particularly anomalous in view of the potential for considerable overlap between entities of security interest to ASIO (who may be the target of a national security IPO),[56] and persons of interest in relation to suspected offences against the security of the Commonwealth,[57] or persons who are subject to control orders (who may be the subject of a law enforcement or control order IPO).[58] It is conceivable that issuing authorities for all types of IPO may encounter similarly sensitive information. This may include the potential for law enforcement agencies to

[52] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, Clause 2 (definition of 'nominated AAT Security Division member') and Clause 17 (appointment of persons as 'nominated AAT Security Division members'). See further Part 4 (national security IPOs).
[53] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, Clause 2 (definition of 'issuing authority' for the purpose of issuing stored communications IPOs; and 'eligible judge' and 'nominated AAT member' for the purpose of issuing interception IPOs); and clauses 14-16 (appointment by Attorney-General of 'eligible judges', 'nominated AAT members' and 'issuing authorities'). See further, Parts 2-3 (law enforcement and control order IPOs).
[54] The PJCHR made a similar observation: PJCHR, *Scrutiny Report 4* (2020), 16-17.
[55] ASIO Act, Part IV, Division 4.
[56] See the definition of 'security' in ASIO Act, s 4. This term covers the protection of Australia and its people from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference. It also covers the protection of Australia's territorial and border integrity from serious threats, and the carrying out of Australia's responsibility to other countries in relation to all of the above matters.
[57] *Criminal Code Act 1995* (Cth), Chapter 5 (offences against the security of the Commonwealth, which include terrorism, treason and related offences, espionage and foreign interference, foreign incursions and recruitment, and harming Australians.)
[58] *Criminal Code Act 1995* (Cth), Division 105 (control orders).

make use of intelligence shared by ASIO in their applications for law enforcement and control order IPOs.[59]

117. The Law Council considers that the *persona designata* appointment of judicial officers as issuing authorities for **both** ASIO's national security and law enforcement IPOs could usefully facilitate consistency, where appropriate, in decision-making about the interpretation and application of equivalent issuing criteria for each type of IPO. It could enable the creation of a reasonably sized 'core' of judicial officers who have a sophisticated understanding of the security and law enforcement environment; possess a high degree of proficiency in making decisions involving the application of the law to identified facts; have deep familiarity with the requirements of the IPO regime; and are demonstrably impartial and independent from the relevant agencies whose applications are under consideration.

118. The *persona designata* appointment of judicial officers as issuing authorities for ASIO's national security IPOs could also usefully facilitate the establishment, for those officers, of appropriate security arrangements for the ongoing determination of IPO applications. (For instance, the provision of necessary physical infrastructure, and the establishment of appropriate procedures for handling classified information.) This could assist in ensuring that highly qualified, experienced and equipped issuing authorities – comprising judicial officers appointed *persona designata* and nominated AAT Security Division members – are readily available to consider ASIO's applications for IPOs, particularly with respect to any urgent applications.

119. Further, as discussed above in relation to issuing authorities for law enforcement IPOs, the power to appoint judicial officers as issuing authorities for ASIO's national security IPOs would provide the strongest possible assurance to the Australian community, and Australia's current and prospective international partners, of the rigour and independence of the issuing process for those IPOs. This is likely to further enhance public trust and confidence in ASIO's exercise of these powers, notwithstanding that the necessarily covert nature of its activities means that specific information about its activities cannot be disclosed publicly.

Recommendation

- **Parts 1 and 4 of proposed Schedule 1 to the TIA Act should be amended to enable the Attorney-General to appoint judicial officers (comprising at least judges of the Federal Court of Australia) as issuing authorities for ASIO's national security IPOs, in addition to the power to appoint members of the Security Division of the AAT as issuing authorities.**

[59] See, for example, ASIO Act, s 19A(1)(d) (ASIO cooperation with Commonwealth, State and Territory law enforcement agencies, in connection with the performance by those agencies of their functions).

Issuing criteria – privacy impact assessment

120. The issuing criteria for law enforcement IPOs require an assessment of the privacy impacts of the particular collection method on **all** persons.[60] In contrast, the issuing criteria for ASIO's national security IPOs only require an assessment of the intrusion on the privacy of the target of an intelligence investigation, or if applicable, a 'B-Party' whose communications are intercepted or accessed.[61] There is no legislative requirement for the issuing authority to assess the likely impacts of the proposed collection activity on the privacy of other persons ('third parties') whose communications or other data may be collected incidentally.[62]

121. The Explanatory Memorandum acknowledges this limitation in the issuing criteria for ASIO's national security IPOs, but states that ASIO is required to adhere to the *Minister's Guidelines to ASIO* (**ASIO Guidelines**) made under section 8A of the ASIO Act in making applications for IPOs.[63] The ASIO Guidelines require ASIO to ensure that its actions are 'proportionate to the gravity of the threat posed and the probability of its occurrence' and to conduct its investigations 'with as little intrusion into privacy as possible'.[64]

122. However, the Law Council considers that an administratively binding obligation about the manner in which an intrusive collection power is to be exercised is a considerably weaker safeguard than a statutory pre-condition to the availability of that power. The consequences for contravening an administrative obligation are purely administrative in character (for example, internal disciplinary action or receiving a Ministerial reprimand). Such contravention does not obviate the legal basis for the collection activity. In this regard, the Bill perpetuates, in the IPO regime, a significant and unjustified imbalance between the statutory prerequisites under the TIA Act for the authorisation of domestic law enforcement powers, and ASIO's intelligence collection powers. The Law Council does not support the continuation of that approach, and recommends that national security, law enforcement and control order IPOs are subject to consistent statutory issuing criteria, in relation to assessing the privacy impacts of the proposed activity on all persons who may be affected by the exercise of the relevant intrusive collection powers.

123. The Law Council acknowledges that it would be possible for an issuing authority in relation to ASIO's national security IPOs to exercise their discretion to consider privacy impacts on third parties in making an issuing decision on an individual IPO application. This matter could be considered under the issuing criterion enabling the consideration of 'other matters (if any) as the nominated AAT Security Division member considers relevant'.[65] However, the Law Council considers that the explicit statutory prescription of third-party privacy impacts as an issuing criterion would

[60] Bill, item 43, inserting proposed Schedule 1 to the TIA Act, subclauses 30(5)(a)(i) and (b)(i) (interception IPOs); Subclause 39(3)(a) (stored communications IPOs); Subclause 48(5) (telecommunications data IPOs); and subclauses 60(5)(a), 60(5)(f), 60(6)(a), 60(6)(f), 69(3)(a) and 78(5)(a) (control order IPOs).
[61] Bill, item 43, inserting proposed Schedule 1 to the TIA Act, subclauses 89(5)(a)(i) and (b)(i) (interception IPOs) and Subclause 98(3)(a) (stored communications IPOs).
[62] The PJCHR made a similar point: PJCHR, *Scrutiny Report 4* (2020), 15-16.
[63] Explanatory Memorandum, [22], [36], [50] and [299].
[64] Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation in its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence), (Guidelines issued under section 8A of the Australian Security Intelligence Organisation Act) 10, [10.4] .
[65] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, subclauses 89(5)(a)(iv) and 89(5)(b)(iv) (interception IPOs), Subclause 98(3)(d) (stored communications IPOs) and Subclause 107(5)(d) (telecommunications data IPOs).

ensure that this matter is given a consistent degree of consideration and weight in the determination of all IPO applications.

Recommendation

- **Clauses 89, 98 and 107 of proposed Schedule 1 to the TIA Act should be amended to require the issuing authority for ASIO's national security IPOs to consider the impacts of the proposed collection activity on the privacy of the target of the investigation, the B-Party (if applicable) and any other persons whose privacy may be impacted by the collection activity.**

Disparity in issuing processes for ASIO's onshore and offshore activities

124. While the two-staged authorisation mechanism described above is an important safeguard with respect to national security IPOs, the Law Council notes that its broader effect is to create two disparate authorisation processes for the exercise by ASIO of security intelligence collection powers 'onshore' and 'offshore'.

125. This reflects that ASIO's existing telecommunications interception and special powers warrants for domestic collection activities are issued by the Attorney-General, without the involvement of a second stage as there is in the IPO scheme, with the ultimate issuing decision being made by a member of the Security Division of the AAT.

126. The Law Council is concerned that the sole basis for imposing a highly significant difference in the respective issuing processes for ASIO's domestic collection warrants and its national security IPOs is the geographical location of the relevant communications data, and not its sensitivity. The national security IPO regime highlights the significant misalignment of the Australian domestic intelligence collection framework with that of our key international partners in the Five Eyes, which have adopted 'double lock' processes for their intelligence collection activities.

127. Although the present Bill is limited to the establishment of an IPO regime rather than amending the domestic interception and access regime, the Law Council considers that efforts should be made to prevent the IPO scheme from entrenching two fundamentally different issuing processes for domestic and overseas collection activities, where the only difference is the geographical location of the information, not its sensitivity or the purposes for which it is collected.

128. Accordingly, the Law Council recommends that the passage of the IPO Bill should be made contingent on the Government making a public commitment to expanding the two-staged authorisation requirement proposed in relation to ASIO's IPOs to all of that agency's warrants under the TIA Act (with respect to telecommunications interception and access to stored communications) and all of its special powers warrants under the ASIO Act (covering the exercise of other intrusive collection powers, including entering and searching premises, accessing computers including incidental telecommunications interception, using surveillance devices and intercepting postal and delivery service articles).

Recommendation

- **Passage of the IPO Bill should be contingent on the Government making a public commitment to introduce legislation, as soon as practicable and no later than within 12 months from the commencement of the IPO scheme, to amend the TIA Act and ASIO Act to align the thresholds and process for the issuing of ASIO's domestic telecommunications and special powers warrants with those applying to national security IPOs. In particular, ASIO's domestic warrants should be made subject to a two-staged authorisation equivalent to the requirements for its national security IPOs.**

Control order IPOs

129. In addition to law enforcement IPOs and ASIO's national security IPOs, Part 3 of proposed Schedule 1 to the TIA Act will enable law enforcement agencies to obtain an IPO for the purpose of monitoring a person who is subject to a control order issued under Division 105 of the *Criminal Code Act 1995* (Cth) (**Criminal Code**). This implements an equivalent international power to the domestic control order monitoring warrants presently available under the TIA Act.

130. The Law Council maintains its longstanding view that the control order scheme is neither necessary nor appropriate and, as such, should be repealed.[66] Accordingly, the Law Council's preference is that control order monitoring warrants are not retained in the domestic regime, or enacted in the IPO regime. Rather, the Law Council considers that IPOs should be limited to the investigation of serious offences, and potentially to security intelligence collection but only if adequate information is provided to justify the extension of the scheme to this activity.[67]

Recommendation

- **IPOs should not be available for the purpose of monitoring compliance with control orders.**

Procedural support and resourcing for IPO issuing authorities

131. Separately to the question of the classes of persons who are eligible to be appointed as issuing authorities for IPOs, the Law Council emphasises the importance of providing appropriate procedural support to all issuing authorities, and ensuring that the necessary legislative and resourcing arrangements are in place to do so.

132. In particular, decision-making is only one of the skills needed for the effective performance by IPO issuing authorities of their functions. Issuing authorities would operate in a unique context. Namely, there may be sporadic occasions for issuing IPOs within short timeframes. Applications may raise specialised questions of fact about the operating environments for security and law enforcement activities, and about the technical specifications of interception and access capabilities. Other than the limited functions of the Queensland and Victorian Public Interest Monitors (**PIMs**) in applications made by relevant law enforcement agencies of those States, there

[66] See, eg, Law Council of Australia, *Anti-Terrorism Reform Project*, October 2013, 104.
[67] The PJCHR has also questioned the need for control order IPOs: PJCHR, *Scrutiny Report 4* (2020), 15.

would be no effective contradictor to test the evidence and case advanced by the agency applying for an IPO.

133. Consequently, the Law Council considers that the following measures (and accompanying resourcing commitments) are needed to support issuing authorities to effectively perform their functions:

- effective education about the parameters of the security and law enforcement environment (both on their induction, and ongoing briefings as part of continuing professional education and current awareness training);
- access to independent technical expertise (that is, experts who are not in any way affiliated with IPO agencies or the government). This may include, for example, expertise in relation to communications technologies, in order for issuing authorities to assess the privacy impacts of a proposed IPO;[68] and
- access to an effective, independent contradictor in IPO applications, such as a special advocate. (Noting that the Bill accommodates such a role for Victorian and Queensland PIMs, and that the *National Security* (*Criminal and Civil Proceedings) Act 2004* (Cth) also enables the appointment of special advocates in control order proceedings under Division 105 of the Criminal Code.[69]

Recommendations

- **Proposed Schedule 1 to the TIA Act should be amended to establish**:
  - **a panel of independent technical experts to support issuing authorities in considering all IPO applications; and**
  - **a regime of 'special advocates' or 'public interest monitors' who can perform the role of contradictor in all IPO applications.**
- **The Government should commit to providing the necessary administrative support and resourcing to all IPO issuing authorities, including commitments with respect to**:
  - **providing regular briefings to all issuing authorities on the operational environment as relevant to IPO agencies;**
  - **providing adequate resourcing for independent technical expertise and 'special advocates' or 'public interest monitors' to perform the role of contradictor in IPO applications; and**
  - **amending the Explanatory Memorandum to identify the financial impacts of these measures. If there is a requirement under the Government's budget rules to offset any new funding allocated to these measures against existing expenditure, those offsets must not be drawn from the existing budgets of the federal courts, the AAT, oversight bodies or legal assistance programs.**

[68] See, for example, the Technology Advisory Panel under s 246 of the *Investigatory Powers Act 2016* (UK).
[69] The PJCHR and Senate Scrutiny of Bills Committees have also questioned why the Bill does not provide for an equivalent role to the Queensland and Victorian PIMs in all IPO applications: PJCHR, *Scrutiny Report 4* (2020), 12-13; Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 26-27.

Review of decisions to issue IPOs

134. The Law Council is concerned that the Bill does not provide adequate rights for DCPs and other aggrieved persons to seek independent review of decisions to issue IPOs.[70] For the reasons outlined below, the Law Council recommends that proposed Schedule 1 to the TIA Act is amended to establish an independent statutory merits review and dispute resolution process for decisions to issue an IPO.

Limited practical utility of judicial review in original jurisdiction

135. Decisions to issue IPOs would not be subject to statutory judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth). This is consistent with the existing treatment of issuing decisions for domestic warrants and authorisations under the TIA Act.[71] As the Explanatory Memorandum notes, judicial review under the original jurisdiction of the High Court in section 75 of the *Constitution,* and the jurisdiction of the Federal Court in section 39B of the *Judiciary Act 1903* (Cth), remains available due to a constitutional limitation on its legislative exclusion.

136. The Explanatory Memorandum comments that judicial review in original or section 39B jurisdiction will 'ensure that an affected person or a [DCP] has an avenue to challenge unlawful decision-making'.[72] It also states that 'the decision to issue an IPO may be challenged by a defendant during court proceedings on the basis that the evidence was improperly or illegally obtained. The court has the discretion not to admit such evidence should a challenge on this basis be successful'.[73]

137. However, this statement does not appear to take account of some significant limitations on these mechanisms, which may substantially reduce or remove their utility to persons, such as DCPs or defendants in criminal proceedings, who are aggrieved by decisions to issue an IPO. For example, an application for judicial review under original or section 39B jurisdiction of a decision to issue an IPO is unlikely to be of practical utility to an aggrieved person if the Commonwealth, as respondent to the application, claims public interest immunity over relevant evidence pertaining to the IPO (such as the facts and grounds provided in the IPO application and assessed by the issuing authority). In the result, it may be impossible for the application to proceed in the absence of that evidence. Claims for public interest immunity may be particularly likely to arise in applications for the judicial review of decisions to issue ASIO's national security IPOs, given the highly classified and necessarily covert nature of most of ASIO's security intelligence investigations and collection activities.

138. Additionally, the regime of conclusive evidentiary certificates able to be issued by DCPs about acts and things done under an IPO[74] may further limit the ability of a defendant in a criminal prosecution to challenge the admissibility of evidence obtained under an IPO, on the basis it was obtained unlawfully or improperly. (Namely, it may be argued that the collection activities carried out by the DCP went further than what was requested or required under the IPO and asserted by the DCP

[70] The PJCHR has also expressed concerns about the adequacy of review rights: Ibid, 19-21.
[71] *Administrative Decisions (Judicial Review) Act 1977* (Cth), section 3 (definition of 'decision to which this Act applies') and Schedule 1, paragraph (d) (prescription of decisions made under the TIA Act as decisions to which the ADJR Act does not apply).
[72] Explanatory Memorandum, [77].
[73] Ibid, [78].
[74] Bill, Schedule 1, item 43 inserting proposed Schedule 1 to the TIA Act, Clause 161.

in the evidentiary certificate, and in doing so, breached applicable conditions or limitations in the terms of that IPO.) As explained later in this submission, the Law Council does not support the conclusive nature of these evidentiary certificates. This includes because they may operate oppressively, to remove the ability of a defendant in a criminal prosecution to collaterally challenge the validity of an IPO in the circumstances described above.

139. The Law Council considers that these limitations in judicial review mechanisms warrant the establishment of an independent review entity. For the reasons outlined the next section of this submission, the Law Council does not consider that the Australian Designated Authority (**ADA**) is sufficiently independent to perform such review functions.

Limitations in ADA review of DCP objections to IPOs

No mandatory review or cancellation requirements in Part 7

140. Clause 121 of proposed Schedule 1 to the TIA Act provides that a DCP may raise a formal objection to an IPO issued by Australia, by registering a written objection with the ADA, on the basis that the IPO does not comply with the underlying DIA.[75]

141. However, the Bill does not impose a requirement on the ADA to consider and determine this application, or prescribe minimum requirements for the conduct of a review of the objection, including timeframes. (In particular, neither the provisions of the Bill nor the Explanatory Memorandum identify whether there is an intention for the ADA to make arrangements with the corresponding competent authority of the foreign country to establish procedures for the joint or consultative determination of the DCP's objection.) Further, there is no requirement for the ADA to give reasons to the DCP or relevant IPO agencies for its decision on a DCP's objection.

142. The power conferred on the ADA in Clause 122 of proposed Schedule 1 to the TIA Act to cancel an IPO after it has been given to a DCP is discretionary rather than mandatory.[76] Subclause 122(1) simply provides that the ADA **may** cancel an IPO,[77] without specifying the minimum matters to which it must have regard in exercising that discretion or the process it must follow to make a decision. Clause 122 does not impose a requirement on the ADA to cancel an IPO if it upholds a DCP's objection made under Clause 121 and determines that the IPO does not comply with the underlying DIA. This appears to raise the legal possibility that the ADA may form a view that its previous assessment made under Subclause 111(1)(b) or 112(1)(b) that the IPO complied with the underlying DIA was incorrect, but may nonetheless decline

[75] Ibid Clause 121.
[76] Cf the **mandatory** cancellation power in Part 5 of proposed Schedule 1 to the TIA Act, in clauses 111(1)(d) and 112(1)(d), which applies only **before** the ADA has given an IPO to a DCP. If the ADA is satisfied that an IPO is not compatible with the underlying DIA, then it must cancel the IPO and must not give it to the DCP. The Law Council considers that the mandatory review and cancellation provisions in clauses 111 and 112 evince an intention to displace the application of the interpretive rule in subsection 33(1) of the *Acts Interpretation Act 1901* (Cth) which would otherwise allow a decision about the compatibility of the IPO with the DIA under clauses 111 and 112 to be remade at a later time, and the mandatory cancellation requirement in those provisions to be enlivened. (Subsection 33(1) of the Acts Interpretation Act provides, 'where an Act confers a power or function or imposes a duty, then the power may be exercised and the function or duty must be performed from time to time as occasion requires'.) The basis for the Law Council's view is that the multiple parts of proposed Schedule 1 to the TIA Act establish a sequential process for requesting, issuing, giving and cancelling or revoking IPOs. On that basis, the obligations in Part 5 (concerning the giving of IPOs to DCPs) under clauses 111 and 112 are necessarily temporally limited to the point in time **before** the ADA has given the IPO to the DCP. Decisions made under those provisions could not be 'remade' after the IPO is given to the DCP. Cancellation of an IPO at the latter point in the process would be governed solely by the discretionary cancellation power in Part 7 (Clause 122).
[77] *Acts Interpretation Act 1901* (Cth), s 33(2A) (general rule that the word 'may' denotes a discretion).

to exercise its discretionary power to cancel the IPO after giving it to the DCP and considering the DCP's objection.

143. The Law Council considers that there should be a mandatory cancellation power that is applicable after the ADA has given an IPO to a DCP. That is, if the ADA considers that an IPO is incompatible with the underlying DIA (despite its earlier assessment under clauses 111 and 112) then it should be required to cancel that IPO.

144. The Law Council considers that it is unjustifiable to create a legal possibility that the ADA could effectively decide to keep an IPO in force, despite knowing that the IPO is not compliant with the underlying DIA. This would unfairly put a DCP (or other aggrieved persons) to the expense and inconvenience of seeking judicial review to have the issuing decision quashed on the basis of illegality, despite the Commonwealth being aware of that circumstance.

Lack of independence by the ADA as a review body

145. The Law Council is doubtful that the ADA has the necessary independence, both substantive and perceived, to perform a review or dispute resolution function in relation to objections made by DCPs. The Law Council has three principal concerns in this regard.

146. First, when the ADA is performing its review functions under Part 7 of proposed Schedule 1 to the TIA Act, it would necessarily have formed a prior view on the matters that are the subject of the DCP's objection under Clause 121, when it was performing its functions under Part 5 concerning the giving of IPOs to DCPs after they are issued. (Part 5 includes a requirement in subclauses 111(1)(b) and 112(1)(b) for the DCP to review the compatibility of the IPO with the underlying DIA. Subclauses 111(1)(c)-(d) and 112(1)(c)-(d) provide that, if the IPO is determined to be consistent with the DIA, the ADA must give it to the DCP. If the IPO is determined to be inconsistent with the DIA, the ADA must cancel it.)

147. Secondly, the ADA is the Secretary of the Attorney-General's Department or a departmental employee to whom the Secretary has delegated their functions.[78] It is conceivable that the Attorney-General's Department may also play a role in advising the Attorney-General on decisions about whether to consent to a request by ASIO to make an application for a national security IPO under Part 4 of proposed Schedule 1 to the TIA Act. This could conceivably include providing advice to the Attorney-General on the compatibility of the proposed national security IPO with the DIA (especially any conditions or limitations in that agreement that are directed to the protection of human rights or civil liberties).[79] It is also possible that the ADA may give

[78] Bill, Schedule 1, item 43 inserting proposed Schedule 1 to the TIA Act, clauses 2 (definition of ADA) and 179 (power of delegation by ADA).

[79] The Law Council notes that the Attorney-General is not expressly required to consider whether a proposed national security IPO complies with the underlying DIA, as part of determining whether to give consent to ASIO to make an application for that IPO. However, the requirements of subclauses 83(6)-(7) and 92(6) do not prescribe exhaustively the totality of matters that the Attorney-General must assess in deciding whether or not to give consent, but rather are prohibitions on the Attorney-General granting consent if those minimum conditions are not met. (The requirements prescribed in these provisions concern an assessment of the security case supporting the proposed application, namely that there are grounds for suspecting that the target is engaged in, or is likely to engage in, activities prejudicial to security; and the information sought under the IPO would be likely to assist ASIO in carrying out its function of obtaining intelligence in relation to security.) It would be open to the Attorney-General to consider, and receive advice from their Department, about other factors, including whether the IPO would be compatible with the underlying DIA (especially any restrictions or limitations for the purpose of protecting human rights or civil liberties, given the responsibilities of the Attorney-General for those matters, as First Law Officer of Australia).

preliminary advice to a law enforcement agency or ASIO about whether a prospective IPO application would comply with the terms of the underlying DIA.

148. Accordingly, it is conceivable that the ADA or their delegate (or other departmental employees providing administrative assistance to these persons) could have provided an opinion about the compatibility of an IPO with the DIA on multiple occasions, before a DCP ultimately lodges an objection to an IPO under Clause 121 of Schedule 1 to the TIA Act, on the grounds of non-compliance with the DIA. This may raise doubts about the substantive and perceived independence of the ADA to make an impartial decision about objections raised by DCPs on the basis that an IPO did not comply with the underlying DIA. There may be a reasonable apprehension that the ADA has pre-judged the basis of the DCP's objections through the previous performance of its functions under Part 5, which require it to make decisions on the same issue, or its advice to the Attorney-General in relation to the Attorney-General's decisions under Part 4 about whether to grant consent to ASIO.

149. Thirdly, the Attorney-General's Department has portfolio responsibility for the Australian Commission for Law Enforcement Integrity,[80] which is an agency that can obtain IPOs under Parts 2 and 3 of proposed Schedule 1 to the TIA Act. This factor may contribute to an overall perception that the ADA is not sufficiently independent to the relevant agencies who may seek IPOs, as well as being insufficiently independent to the process for the issuing and execution of those IPOs.

150. For these reasons, the Law Council considers that the Bill does not provide meaningful, accessible and genuinely independent avenues for the review of objections to decisions to issue an IPO that may be made by DCPs, or others who are aggrieved by the exercise of intrusive collection powers against them. The Law Council recommends that the Bill should be amended to establish a new body, or enable the appointment of individuals, to review objections to IPOs by DCPs and other persons. The relevant body or individual reviewers should be demonstrably separate to the processes for issuing, executing and administering IPOs, and the agencies who may obtain IPOs. Independent reviewers could include, for example, judicial officers appointed *persona designata*, retired judicial officers or qualified arbitrators.

Recommendations:

- **Part 7 of proposed Schedule 1 to the TIA Act should be amended to create an independent statutory review process for decisions to issue an IPO, including a process to resolve objections by the designated communications provider (DCP) and other persons that an IPO was not authorised by the relevant DIA, after it has been given to the DCP.**

  That review process should involve the appointment of decision-makers who are independent to the ADA (for example, judicial officers appointed persona designata, or retired judicial officers). The decision-maker on review should be required to give reasons for their decision.

- **Clause 122 of proposed Schedule 1 to the TIA Act should be amended to require the ADA to cancel an IPO it has given to a DCP, if it considers that the IPO is not consistent with the terms of the underlying DIA.**

[80] Administrative Arrangements Order (1 February 2020) (Cth), pt 2.

Reporting and oversight measures

Annual reporting requirements on the use of the IPO scheme

151. The Bill imposes obligations on agencies and the ADA to report annually on their use of the IPO scheme.[81] In the case of law enforcement agencies and the ADA, that information will be tabled in the Minister's annual reports to Parliament.[82] However, ASIO is only required to include statistical information on national security IPOs in its classified annual reports prepared under section 94 of the ASIO Act.[83]

152. The Law Council is aware that successive governments have taken a position, on the advice of ASIO, that the publication of aggregated statistical information on ASIO's covert intelligence collection activities, including warrants and authorisations obtained under the TIA Act and ASIO Act, would prejudice the performance by ASIO of its functions. While acknowledging this advice, the Law Council considers that this position, including its proposed application to ASIO's national security IPOs, requires further and continuous scrutiny to assess whether the risk of harm continues to justify the withholding of aggregated statistical information. This includes an assessment of whether the public interest in disclosure is outweighed by the perceived risk of harm.

153. It is difficult to assess the ongoing need for secrecy without access to specific information about the perceived threat, including information about the total numbers of domestic warrants or authorisations issued. In the abstract, it would seem that the annual issuing of a large number of warrants or authorisations may significantly reduce the likelihood that entities of security concern could determine or suspect, from aggregated numerical totals, that they were the targets of a security investigation. In this regard, the Law Council notes that the Independent National Security Legislation Monitor (**INSLM**) made a general observation at his public hearing on 21 February 2020 that the total number of warrants and authorisations issued by the Attorney-General in relation to ASIO 'is not a small number'.[84]

154. Further, the Law Council notes that the Bill proposes to apply a more nuanced test to the exclusion of 'control order information' from law enforcement agencies' unclassified annual reports on control order IPOs. The definition of 'control order information' means that the Minister is specifically required to consider whether aggregated statistical information would enable a reasonable person to conclude that an IPO is likely to be in force, or not in force, in relation to a particular person, or a particular electronic communication service by a particular person.[85] It is unclear why a similar test could not be applied to ASIO's national security IPOs (and, by extension, reporting requirements for its domestic warrants and authorisations).

155. Accordingly, the Law Council considers that the details of the claim for ongoing secrecy in relation to aggregate annual numbers of ASIO's national security IPOs, and by extension its domestic warrants and authorisations, should be tested by an appropriate independent entity. If the claim for secrecy is no longer justified in relation to some or all of these instruments, then section 94 of the ASIO Act should be

[81] Bill, Schedule 1, item 43, inserting proposed Schedule 1 of the TIA Act, Division 2 of Part 9 (annual reporting by law enforcement agencies and ADA). See also, Bill, Schedule 1, cl 4 (ASIO's annual reports). In addition, under Clause 129 of proposed Schedule 1 to the TIA Act, ASIO must provide reports to the Attorney-General on each of its interception IPOs (consistent with its reporting requirements in s 17 of the TIA Act for domestic interception warrants).
[82] Bill, Schedule 1, item 43, inserting proposed Schedule 1 of the TIA Act, Clause 131.
[83] Ibid, Schedule 1, cl 4 (ASIO's annual reports).
[84] Dr James Renwick SC, Independent National Security Legislation Monitor, Transcript of Public Hearing of the Review of the TOLA Act, 21 February 2020, Canberra, 202 at [30].
[85] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, Clause 132.

amended to require such information to be included in ASIO's unclassified annual reports that are tabled in Parliament.

156. The Law Council considers that the PJCIS would be well-placed to undertake this review, given its status as a bipartisan joint committee of the Parliament (being the forum in which agencies' unclassified annual reports are tabled) and its ability to take classified evidence under Part 4 and Schedule 1 to the *Intelligence Services Act 2001* (Cth) (**Intelligence Services Act**). It would also be open to the PJCIS to refer this matter to the INSLM for inquiry and report in accordance with section 7A of the *Independent National Security Legislation Monitor Act 2010* (Cth) (**INSLM Act**).

157. The Law Council considers that such an inquiry would be within the PJCIS's existing functions in 29(1)(b) of the Intelligence Services Act, to review any matter in relation to ASIO that is referred by the responsible Minister or the Attorney-General, or by resolution of either House of the Parliament. Further consideration may be required as to whether amendments to the INSLM Act are necessary to enable the INSLM to undertake such an inquiry.

Recommendation

- **The Government (or either House of Parliament, by resolution) should refer to the PJCIS the matter of whether the exemption of aggregated statistical information from ASIO's unclassified annual reports (including the proposed exemption of statistical information relating to IPOs) is necessary and appropriate in contemporary circumstances. In conducting this review, the PJCIS may request the INSLM to consider the matter and report back to the PJCIS.**

Oversight of the IPO regime

Agencies' notification obligations to independent oversight agencies

158. The Bill imposes various obligations on Commonwealth agency heads to notify their respective oversight agencies, namely, the Commonwealth Ombudsman or the Inspector-General of Intelligence and Security (**IGIS**) in the case of ASIO, of certain matters relating to applications for, and revocation of, IPOs. The Law Council supports such notification requirements, as they facilitate efficient oversight by enabling the relevant oversight agencies to focus their attention on these matters. The Law Council also notes that such oversight, which is conducted on an *ex post facto* basis through examination of agencies' records, is likely to be assisted by the record-keeping obligations imposed on agencies and the ADA under Part 9.

159. However, there some are apparent disparities between the content of the notification obligations applicable to ASIO and law enforcement agencies. In the absence of justification for their differential treatment, the Law Council considers that the requirements should be aligned. In particular, the Law Council considers that:

(a) ASIO should be required to notify IGIS as soon as practicable if it breaches its obligation in Clause 116 to revoke an IPO if satisfied that the issuing grounds have ceased to exist (to be consistent with the obligation on law enforcement agencies with respect to control order IPOs);[86] and

(b) If the Attorney-General gives oral consent to a law enforcement agency to make an application for an IPO under Part 2 or 3, the agency must give the

[86] Ibid cl 81(2).

Ombudsman a copy of a written record of that consent within 3 working days (to be consistent with the obligation on ASIO to provide that record to IGIS).[87]

Recommendation:

- **Parts 2, 3 and 4 of proposed Schedule 1 to the TIA Act should be amended to ensure that the obligations on law enforcement agencies to notify the Ombudsman of certain matters, and the obligations on ASIO to inform the IGIS of certain matters, are consistent with each other, by adopting the higher of the two standards where there is a difference.**

Limitations in permitted disclosure provisions relevant to oversight

160. Part 11 of proposed Schedule 1 to the TIA Act contains provisions that permit the sharing of information obtained under, or about, IPOs ('protected IPO information') for a broad range of prescribed purposes.

161. However, the Law Council notes that there are two apparent oversights in the drafting of the relevant provisions, which may unintentionally preclude people from giving information to the IGIS and Ombudsman for the purpose of those agencies performing their oversight functions, and may prevent those agencies from subsequently using and disclosing that information where necessary.

Exceptions for disclosures to, and by, IGIS and Ombudsman officials

162. Subclauses 153(1)(p) and (q) of proposed Schedule 1 to the TIA Act provide exceptions to the general prohibition on disclosure in Clause 152. They allow 'protected IPO information' to be used, recorded, disclosed, or admitted in evidence for the purpose of:

(a) the performance of a function or duty, or the exercise of a power, by an IGIS official under the *Inspector-General of Intelligence and Security Act 1986* (Cth); and

(b) the performance of a function or duty, or the exercise of a power, by an Ombudsman official under the *Ombudsman Act 1976* (Cth).

Reference to the performance of oversight functions under named Acts

163. These exceptions are confined expressly to the performance by IGIS and Ombudsman of functions or duties, and the exercise of powers, under named Acts. The Law Council notes that these are not the only enactments that confer functions, duties and powers on IGIS and Ombudsman, and it is possible that future enactments may separately confer further functions, duties and powers on these agencies. The reference in subclauses 153(1)(p) and (q) to particular Acts may arbitrarily limit the application of the exception, based merely upon the particular statutory source of the oversight function.

164. For example, the Ombudsman and IGIS perform functions under the *Public Interest Disclosure Act 2013* (Cth). It is conceivable that the conduct of a law enforcement agency or ASIO official in relation to an investigation conducted in reliance on an IPO could be the subject of a public interest disclosure to IGIS or Ombudsman (as applicable). Accordingly, the Law Council considers that these exceptions should refer

[87] Ibid cl 83(11) (interception IPOs), cl 92(10) (stored communications IPOs).

generically to the functions, duties and powers of IGIS and Ombudsman, without prescribing their individual statutory sources.

165. The Law Council notes that the exceptions to the official secrecy offences in Part 5.6 of the Criminal Code take the above approach suggested by the Law Council. Paragraph 122.5(3)(b) creates an exception for disclosures of information to, and by, integrity agency officials (including IGIS and Ombudsman officials) for the purpose of the relevant integrity agency 'exercising a power, or performing a function or duty'. This approach is also taken to the exceptions to the secrecy offences in relation to the assistance and access regime in paragraphs 317ZF(3)(f)-(g) and subsections 317ZF(5)-(5A) of the Telecommunications Act; and in the exceptions for disclosing 'ASIO computer access intercept information' in subsections 63AC(3)-(5) of the TIA Act.

Application of evidential burden to IGIS and Ombudsman officials

166. The Law Council also notes that the exceptions in the other Acts referred to above contain provisions removing the evidential burden from integrity agency officials as defendants to the relevant secrecy offences, in relation to their status as officials of their agency and that they disclosed or otherwise dealt with the relevant information for the purpose of performing functions or duties, or exercising powers, in their official capacity.

167. The Supplementary Explanatory Memorandum to the legislation enacting Part 5.6 of the Criminal Code noted that this approach implemented a recommendation of the PJCIS in its 2018 inquiry into the relevant Bill, which was made because the relevant integrity agencies have secrecy obligations under their governing legislation that will generally prevent them from disclosing evidence (including to a court) about information obtained in the performance of their official duties, which would be necessary for them to do in order to discharge the evidential burden in relation to a secrecy exception of this kind. Consequently, the PJCIS recommended that officials from these agencies should not be required to discharge the evidential burden.[88]

168. The Law Council supports the adoption of the approach endorsed by the PJCIS in 2018 in relation to all exceptions to offences for disclosures to, and by, integrity agency officials acting in their official capacities. This includes the exceptions in subclauses 153(1)(p) and (q) in relation to IGIS and Ombudsman officials.

Recommendation

- **Subclauses 153(1)(p) and (q) of proposed Schedule 1 to the TIA Act should be amended to:**
  - **omit the references to the *Inspector-General of Intelligence and Security Act 1986* (Cth) and the *Ombudsman Act 1976* (Cth); and**
  - **provide that IGIS and Ombudsman officials do not bear the evidential burden for these exceptions, in relation to their status as IGIS or Ombudsman officials, and the fact that they dealt with the relevant information in their official capacities.**

[88] Supplementary Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, [650]-[653].

Possible amendments to the IGIS Act – engagement with Ombudsman and ADA

169. The Law Council questions whether there may be a need for the Bill to also amend the disclosure offences in section 34 of the IGIS Act (or amend the functions of the IGIS under that Act) to enable IGIS officials to communicate with the ADA and Ombudsman in relation to the oversight of ASIO's national security IPOs.

170. In short, the offences in section 34 of the IGIS Act provide that the IGIS, or a member of staff, may not make records of, or disclose to any person or a court, or otherwise make use of, information obtained in the performance of official functions or duties, or exercise of powers, except under the IGIS Act or a series of other named Acts that confer functions, duties and powers on the IGIS (for example, the *Public Interest Disclosure Act 2013* (Cth), *Freedom of Information Act 1982* (Cth) and *Archives Act 1983* (Cth)). The term 'court' is defined broadly to cover 'any tribunal, authority or person having power to require the production of documents or the answering of questions'.

171. It appears to the Law Council that there may be circumstances in which it could be useful for IGIS to provide information to the ADA or Ombudsman, but IGIS officials may be prevented from doing so under section 34 of the IGIS Act, as the disclosure may not have a sufficient connection to the performance by IGIS of a specific oversight function in relation to ASIO (such as an inspection or an inquiry).

172. For example, there may be utility in IGIS undertaking the following activities:

Participating in certain consultations with the Ombudsman

173. There may be value in the IGIS participating in consultations with the Ombudsman for the purpose of the Ombudsman performing an inspection of, or inquiry into, the ADA, which concerns the ADA's administration of one or more of ASIO's national security IPOs. For example, the Ombudsman may wish to seek independent explanation, clarification or advice from IGIS about matters pertaining to IPOs that are obtained by ASIO, if it is considered necessary in order for the Ombudsman to understand the surrounding circumstances and context of the ADA's actions with respect to the ADA's administration of ASIO's IPOs.

174. The Law Council notes that there may otherwise be challenges for the Ombudsman in effectively overseeing the ADA's activities in relation to ASIO's IPOs, given that it is the IGIS rather than the Ombudsman who is responsible for oversight of ASIO itself, and therefore has detailed knowledge and understanding of the context of ASIO's activities and practices. It is conceivable that such contextual understanding may be important in overseeing the closely related matter of the ADA's activities in relation to ASIO's IPOs.

175. In this scenario, it would appear that Subclause 153(1)(q) would give the Ombudsman sufficient authority to give 'protected IPO information' to the IGIS, since the disclosure would be made for the purpose of the performance of its own inspection and inquiry functions. However, section 34 of the IGIS Act may not authorise an IGIS official to provide a response, since assisting the Ombudsman or another integrity agency is not among the IGIS's functions.

176. The Law Council considers that it would be preferable to equip the Ombudsman and IGIS with the ability to consult as appropriate, to make certain that the Ombudsman can perform its functions with the maximum degree of effectiveness.

Participating in certain consultations with the ADA

177. It may be desirable for IGIS and ADA to consult with each other, in the event that there is overlap between aspects of the respective functions of the IGIS and ADA in relation to ASIO's national security IPOs.

178. In particular, when IGIS conducts inspections of ASIO's IPO applications (with a view to examining the legality and propriety of its actions in seeking, as well as executing, the IPO) it may wish to examine and form a view on ASIO's assessment of whether a proposed IPO is compatible with the relevant underlying DIA.

179. The ADA would also form a view on that issue in performing its functions under Part 5 (giving an IPO to a DCP) and potentially under Part 9 (cancellation of an IPO, including on an objection lodged by a DCP on the basis that the IPO was inconsistent with the DIA). The ADA may also give preliminary advice or guidance to ASIO on a prospective IPO application.

180. It is possible that IGIS and the ADA may adopt different legal views about the compatibility or otherwise of a national security IPO with the underlying DIA, in the course of performing their respective, independent functions. In these circumstances, IGIS and the ADA may consider it desirable to discuss the relevant legal and factual issues with each other to consider whether it is possible to reach a consensus, and avoid the outcome that ASIO (and relevant Ministers) are presented with conflicting legal views about the compliance of a national security IPO with a DIA.

181. In this scenario, the ADA would appear to be authorised by Subclause 153(p) to provide 'protected IPO information' to the IGIS, to the extent that information was relevant to the IGIS's functions in relation to ASIO (for example, conducting inspections of ASIO's IPO applications).

182. However, section 34 of the IGIS Act may not authorise an IGIS official to discuss with the ADA the IGIS's views about the compatibility or otherwise of one of ASIO's IPOs with the underlying DIA. This reflects that the purpose of such discussions would be to support the overall effective operation of the IPO regime by avoiding, where possible, ASIO and relevant Ministers receiving conflicting legal views on this matter. While participation in such consultations may be beneficial to avoid uncertainty or confusion arising from conflicting opinions, they do not appear to be clearly or directly referable to an oversight function of IGIS for the purpose of permitted disclosures under section 34 of the IGIS Act. That is, the fact the ADA – whose functions are not subject to IGIS oversight – may take a different legal view to IGIS would have no legal impact upon the status of the findings of the IGIS on the same point in an inspection of, or an inquiry into, ASIO's IPO activities.

183. To remove ambiguity or doubt, the Law Council suggests that consideration is given to amending section 34 of the IGIS Act (or the statutory functions of the IGIS under that Act) to enable IGIS officials to provide assistance to the Ombudsman, and to discuss relevant matters with the ADA, in relation to ASIO's national security IPOs. This would, of course, be subject to the IGIS, Ombudsman and ADA complying with the Commonwealth Protective Security Policy Framework in making the relevant disclosures.

Recommendation

- **The Bill should amend the IGIS Act to enable IGIS officials to give protected IPO information to the Ombudsman and ADA, in relation to the oversight of ASIO's national security IPOs. The purposes of the permitted disclosures should be to:**
  - **respond to a request for assistance from the Ombudsman in relation to the Ombudsman's oversight of the ADA's administration of ASIO's national security IPOs; and**
  - **discuss with the ADA matters relating to ASIO's national security IPOs that are relevant to the functions of both IGIS and the ADA, including the compliance of those IPOs with the underlying DIAs.**

Monitoring the use of 'incoming IPOs' from foreign countries

184. Part 9 of proposed Schedule 1 to the TIA Act contains a number of record-keeping and reporting requirements, including aggregated statistical information of all outgoing IPOs issued on the request of Australian authorities and given to foreign DCPs. In particular, the ADA is required to cause a register to be kept of all outgoing IPOs issued under proposed Schedule 1.[89] Further, the ADA must provide the Minister the written report within three months after the end of each financial year.[90] Subclause 130(2) requires the Minister to cause a copy of the report to be given to the Attorney-General as soon as practicable after receiving the report.

185. The reporting and record-keeping requirements in the Bill appear to relate to all IPOs issued by Australian authorities to foreign DCPs (that is, 'outgoing IPOs'). There does not appear to be any formal obligation in the Bill requiring an appropriate coordination or administrative authority, such as the ADA, to monitor and report on all 'incoming IPOs' that are issued to Australian communications providers by foreign authorities, pursuant to any of the designated international agreements that Australia may have with its foreign partners. The ADA is only required to keep records of objections lodged by Australian DCPs to 'incoming IPOs'.[91]

186. Presumably, there may be an intention to place reliance on administrative information-sharing arrangements between the ADA and foreign designated authorities, and individual Australian communications providers. For example, Article 12(4) of the US/UK bilateral agreement provides that each country's designated authority must issue an annual report to the other, in respect of the outgoing IPOs that they have issued to the other. Those reports are required to reflect 'aggregated data concerning the use of this Agreement to the extent consistent with operational national security'.

187. The Bill also does not impose record-keeping requirements or periodic reporting obligations on Australian communications providers in relation to their compliance with 'incoming IPOs'. This appears to be anomalous with existing record-keeping and reporting obligations imposed on telecommunications carriers and carriage service providers under Division 5 of Part 13 of the Telecommunications Act, in relation to notifications received from domestic law enforcement agencies to access that the relevant agency is authorised to access telecommunications data under the domestic access regime in Part 4-1 of the TIA Act. In these circumstances, carriers and

[89] Ibid cl 139.
[90] Ibid cl 130(1).
[91] Ibid cl 138(2).

carriage service providers are required to keep records of the notifications received and disclosures made, and include this information in their annual reports to the Australian Communications and Media Authority.[92] The Australian Information Commissioner is also conferred with power to monitor carrier and carriage service providers' compliance with these record-keeping requirements.[93]

188. The Law Council queries why the Bill does not impose comparable record-keeping, reporting and oversight requirements on Australian communications providers in respect of their compliance with 'incoming IPOs' that request access to telecommunications data. The Law Council also queries why the Bill does not impose comparable requirements in relation to oversight by the Australian Information Commissioner of providers' compliance with record-keeping requirements for 'incoming IPOs' requesting the interception of communications or the accessing of stored communications.

189. In particular, the Law Council notes that the Bill proposes to give Australian communications providers who comply with 'incoming IPOs' broad immunities and exceptions from applicable prohibitions and limitations under Australian laws. This includes immunity from prohibitions on interception and access under the TIA Act, immunities from certain disclosure offences under the Telecommunications Act, and authorisation for the purpose of the Privacy Act. [94] (The latter authorisation is especially relevant to Australian Privacy Principle 6.2, which prevents an entity that is governed by the Privacy Act from making secondary uses and disclosures of personal information they have obtained, unless certain exceptions apply, one of which is that the relevant secondary disclosure or use is authorised by law.)

190. In view of the breadth of these immunities and authorisations under Australian laws that will be engaged by Australian communications providers' compliance with an 'incoming IPO',[95] the Law Council considers it would be appropriate for Australia to undertake its own monitoring of acts done by Australian communications providers, in Australia, in purported compliance with 'incoming IPOs'. This will ensure that Australia has direct awareness of the instances and circumstances in which the significant legal immunities and authorisations under Australian law are invoked in practice. The Law Council considers that the Bill should make statutory provision for these arrangements, rather than placing sole reliance on administrative measures. The measures in the Bill should include:

- Obligations on Australian communications providers (at least telecommunications carriers and carriage service providers) to:
  - keep records of incoming IPOs they receive and retain them for a set period of time (illustratively, three years to be compatible with corresponding requirements in the Telecommunications Act);
  - keep records of acts and things done in compliance with an incoming IPO (illustratively, three years to be compatible with corresponding requirements in the Telecommunications Act); and

[92] Telecommunications Act, ss 305-308.
[93] Ibid, s 309.
[94] Bill, Schedule 1, item 43 inserting proposed Schedule 1 to the TIA Act, clauses 168-169.
[95] The PJCHR and Senate Standing Committee for the Scrutiny of Bills have also commented on the breadth of these effective immunities: PJCHR, *Scrutiny Report 4* (2020), 25-26; and Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 33-34.

- notify the ADA of receipt of each 'incoming IPO' within a specified period of time after receiving it, or to report periodically to the ADA on all 'incoming IPOs' received for the reporting period.

- Obligations on the ADA to monitor and keep records of incoming IPOs received (based on reporting from communications providers and information-sharing with foreign designated authorities) and report annually to the Attorney-General or Home Affairs Minister on the number of incoming orders.
- Obligations on the Attorney-General or Home Affairs Minister to cause the tabling in Parliament of the ADA reports on incoming IPOs, unless the relevant Minister is reasonably satisfied that the disclosure of the information would prejudice the security or defence of Australia or the foreign countries; or the conduct of Australia's foreign relations with the foreign countries to which the information relates. In this event, the relevant Minister may publish a single, aggregated number of incoming IPOs in the reporting period, without identifying country sources.

Recommendation

- **The record-keeping and reporting requirements in Part 9 of proposed Schedule 1 to the TIA Act should be amended to enable the monitoring of the receipt and compliance by Australian communications providers with 'incoming IPOs' issued by foreign countries pursuant to a DIA. This should include the following requirements:**
  - **record-keeping and periodic notification or reporting obligations to the ADA on Australian communications providers, analogous to existing requirements in relation to telecommunications data under Division 5 of Part 13 of the Telecommunications Act (including provisions for the information Commissioner to conduct oversight of compliance);**
  - **record-keeping and annual reporting obligations on the ADA in relation to incoming IPOs; and**
  - **a requirement that the Attorney-General or Minister for Home Affairs table annual reports on incoming IPOs, containing at least the total aggregate number of incoming orders received.**

Independent review of the operation of the IPO legislation

191. The Bill does not propose to amend the *Independent National Security Legislation Monitor Act 2010* (Cth) to confer oversight functions on the INSLM with respect to the IPO scheme, either as part of the INSLM's annual reporting functions,[96] or a one-off statutory review, as is the case for other recent amendments including the TOLA Act.[97]

192. The Law Council considers that this omission is anomalous with the established legislative practice in relation to significant pieces of security legislation, in which the

[96] INSLM Act ss 6 and 29.
[97] Ibid s 6(1D).

INSLM Act is amended to provide that a function of the INSLM is to conduct a review of the amendments after they have been operational for a specified period of time.[98]

193. The omission of an ongoing annual reporting function may also lead to an anomalous outcome that the INLSM's existing jurisdiction could cover parts of the IPO legislation, in relation to its use by the Australian Federal Police to investigate the security offences in Chapter 5 of the Criminal Code.[99] However, it would not appear to cover ASIO's use of national security IPOs in respect of security matters that are comprised of the same or similar facts as police investigations of security offences.[100]

194. Given the ability for the IPO scheme to be used in connection with major counter-terrorism and national security investigations, the Law Council considers that there would be benefit in having the INSLM consider the ongoing necessity, proportionality, appropriate use and adequacy of safeguards in relation to the IPO regime as whole. The Law Council recommends that the Bill should amend the INSLM Act to ensure that the INSLM has full oversight of the IPO legislation. This should include amendments to:

(a) expand the definition of 'counter-terrorism and national security legislation' in section 4 to include the provisions of new Schedule 1 to the TIA Act in their entirety; and

(b) amend section 6 to confer a one-off statutory review function on the INSLM to conduct a review of the legislation governing the IPO scheme after it has been in force for a specified period of time (indicatively, 12-18 months).

Recommendation

- **The Bill should amend the *Independent National Security Legislation Monitor Act 2010* to ensure that the INSLM has full oversight of the legislation establishing the IPO scheme. This should include as part of the INSLM's annual reporting function, and a one-off statutory review after the legislation has been in force for a set period of time, between 12-18 months of operation.**

Oversight of the IPO scheme by the PJCIS

195. The Bill does not propose to confer oversight functions on the PJCIS in relation to the IPO scheme, either as part of its ongoing oversight of aspects of agencies' administration, expenditure and other specified activities; or as a one-off statutory review after the legislation has been operational for a specified period of time.

196. Consistent with the above comments in relation to INSLM oversight, this omission is also anomalous with routine legislative practice in relation to the Parliamentary review of major amendments to security legislation.[101] The Law Council is similarly concerned that the absence of amendments to the Committee's functions under Part 4 of the Intelligence Services Act may lead to anomalies in the coverage of the PJCIS's scrutiny functions in relation to the IPO regime. That is, it would appear that the Committee could examine aspects of the scheme within its existing functions.

[98] See, for example, ibid, ss 6(1B)-(1D).
[99] Ibid s 4 (definition of 'counter-terrorism and national security legislation at paragraph (d) which covers Chapter 5 of the Criminal Code and any other provision that relates to a provision of Chapter 5).
[100] Ibid s 4 (definition of 'counter-terrorism and national security legislation', paragraph (a) of which only covers ASIO's questioning and detention warrants in Division 3 of Part III of the ASIO Act).
[101] See, for example, *Intelligence Services Act 2001* (Cth) ss 29(1)(bb)-(cd).

197. Specifically, it would appear that the PJCIS's existing functions in section 29 of the Intelligence Services Act would cover: ASIO's use of national security IPOs;[102] the AFP's use of law enforcement IPOs in relation to the investigation of terrorism offences in Part 5.3 of the Criminal Code and the AFP's use of control order IPOs.[103] However, the PJCIS would not appear to have jurisdiction in relation to the AFP's use of law enforcement IPOs to investigate other security offences in other parts of Chapter 5 of the Criminal Code, such as foreign incursions, incitement of violence, espionage and foreign interference, and harming Australians.[104]

198. The Law Council recommends that the Bill should be amended to ensure consistency of the PJCIS's scrutiny functions, by amending section 29 of the Intelligence Services Act to confer the following additional functions on the PJCIS in relation to the IPO scheme:

    (a) A function with respect to the use by the AFP of the scheme in relation to all matters within Chapter 5 of the Criminal Code, thereby covering the use of IPOs for the investigation of all offences against the security of the Commonwealth;

    (b) A function with respect to reviewing relevant parts of ASIO's classified annual reports providing information on its use of the IPO scheme (equivalent to its existing functions to review those parts of ASIO's reports which provide statistical information on certain of its retained data activities under the TIA Act);[105] and

    (c) A statutory review of the operation of the IPO scheme after a period of operation (for example, in the range of 12 to 18 months).

199. The Law Council also considers it would be desirable for the Committee to have the power to require briefings from the ADA on request, via an amendment to section 30 of the Intelligence Services Act.

Recommendation

- **The Bill should amend Part 4 of the *Intelligence Services Act 2001* to:**
    - **enable the PJCIS to undertake ongoing monitoring of all of the activities of ASIO and the AFP under the IPO scheme, including consideration of relevant provisions of the AFP and ASIO's annual reports on IPOs;**
    - **require the PJCIS to conduct a review of the operation of the IPO scheme after a set period of operation, in the range of 12-18 months;**
    - **enable the PJCIS to require the ADA to provide it with briefings on request.**

[102] Ibid s 29(1)(b) (any matter in relation to ASIO on the referral of the Minister for Home Affairs or the Attorney-General, on the resolution of either House of Parliament).
[103] Ibid ss 29(1)(baa)-(bac) (monitoring and inquiries on own-motion or Ministerial or parliamentary referral)
[104] Ibid s 29(1)(baa)-(bac) and (bba). The Committee's ongoing monitoring functions in relation to the AFP are specifically limited to Part 5.3 of the Criminal Code and certain provisions of the Crimes Act, and not Chapter 5 of the Criminal Code more broadly (other than one-off statutory reviews of certain provisions).
[105] Ibid, s 29(1)(be).

Australian Designated Authority

200. The Bill proposes to establish the ADA) to review IPOs for compliance with the relevant DIA (both before they are given to DCPs and in response to any objections lodged by DCPs) and act as an intermediary between Australian law enforcement and national security agencies and DCPs.[106] The ADA is designated as the Secretary of the Attorney-General's Department, who may delegate their functions and powers to Departmental employees holding a minimum classification of acting Executive Level 1.[107] The ADA has significant powers, including the cancellation of IPOs.[108]

201. The ADA is subject to oversight by the Commonwealth Ombudsman. This includes under the specific inspection function conferred by the Bill, under which the Ombudsman may inspect records of the ADA (and the relevant Commonwealth law enforcement agencies able to obtain IPOs) to determine their compliance with the requirements of IPO scheme.[109] The Ombudsman must table the findings of these inspections in an annual report to the Minister, and the Minister is obliged to table the report in Parliament. [110]

Independence of the ADA

202. The Law Council is concerned that locating the ADA within the Attorney-General's Department is incompatible with the degree of independence, both substantive and perceived, that is necessary to perform its important functions.

203. As mentioned in the Law Council's earlier comments about the adequacy of review arrangements concerning issuing decisions for IPOs, the Law Council is concerned that the Secretary's dual responsibilities – as adviser to the Attorney-General in the issuing process for IPOs, and as the ostensibly independent ADA – may give rise to at least a perceived conflict of interest or lack of independence.

204. That is, the Department is likely to play a role of some kind in advising or supporting the Attorney-General in the performance of his or her functions in the issuing process for ASIO's national security IPOs.[111] This could conceivably include advice on the compatibility of a prospective IPO with a DIA (particularly compliance with any human rights-related safeguards). Once an IPO is issued, the ADA's responsibilities under Part 5 are enlivened, including a requirement to assess the compliance of the IPO with the underlying DIA.[112] It is also possible that the Secretary or delegate, as ADA, may give preliminary advice or guidance to agencies considering applying for an IPO about whether the proposed activities are likely to be compatible with the underlying DIA. This may raise concerns that the Department has given, or may have given, prior advice to the government or IPO agencies on the same matters in respect of which its officials must subsequently perform their functions as ADA under Part 5 (and potentially part 9) of proposed Schedule 1 to the TIA Act.

205. To avoid the potential for an actual or perceived conflict of interest and ensure public confidence in the independence of the ADA, the Law Council suggests that the role of the ADA would be better performed by an independent entity. Consideration should be given to creating the position of the ADA as an independent statutory office-holder

[106] See, eg, ibid Parts 5 and 7.
[107] Ibid cl 2.
[108] Ibid, cl 111, 112, and 122.
[109] Ibid cl 142-143.
[110] Ibid cl 150.
[111] Ibid cl 83(5)-83(7).
[112] Ibid cl 112(1).

appointed by the Attorney-General, or alternatively conferring the functions on the head of an existing agency that is demonstrably at arm's length from the process for the issuing of IPOs.

Recommendation

- **Proposed Schedule 1 of the TIA Act should be amended to establish the Australian Designated Authority as an independent statutory office holder.**

Powers of delegation by the ADA

206. Irrespective of the particular public official who is appointed to the role of ADA, the Law Council is concerned about overbreadth in the ADA's powers of delegation. The Bill empowers the ADA to delegate their powers to departmental employees who occupy a position at a minimum classification of acting Executive Level 1, and are not required to possess any particular qualifications (for example, legal qualifications) or apply clear statutory criteria to the exercise of discretion to cancel an IPO. [113]

207. The Law Council considers that the scope of this power of delegation is not commensurate with the significant powers of the ADA to create and affect legal rights and obligations, in the context of a scheme authorising highly intrusive evidence and intelligence collection powers. For example, the ADA has powers to cancel IPOs, to make significant legal decisions about the compliance of an IPO with a DIA, and to issue evidentiary certificates.

Recommendation

- **Clause 179 of proposed Schedule 1 to the TIA Act should be amended to provide that the Australian Designated Authority may only delegate their functions and powers to an employee who is admitted as an Australian legal practitioner, and is in a position classified as Senior Executive Service Band 1 or higher.**

Retention and deletion of information obtained under IPOs

Records of intercepted and stored communications

208. Clause 140 of proposed Schedule 1 to the TIA Act imposes obligations on agency heads to cause the deletion of information in their agencies' possession that is obtained under an outgoing IPO which authorises access to electronic communications content (via interception or access to stored communications). The obligation applies if the relevant agency head becomes satisfied that retention is not likely to be required for the performance by their agency of a permitted purpose in Part 11, clauses 153 and 158 of which provide wide coverage of their functions. This includes, for ASIO, the performance of **any** of its statutory functions.[114] The Explanatory Memorandum suggests that Clause 140 'will ensure that records of sensitive, personal communications are not kept by agencies where no longer needed'.[115]

[113] Ibid cl 179.
[114] Bill cl 140 especially cl 140(4)(d). See also cl 153(1)(h) (permitted purposes for ASIO).
[115] Explanatory Memorandum, [455].

No obligation on agency heads to cause periodic reviews of agency holdings

209. The Law Council is concerned that Clause 140 does not provide the strong guarantee described in the Explanatory Memorandum. In particular, the provision falls short of imposing a positive obligation on agency heads to periodically review their holdings of that content and assess **whether** it remains relevant. The absence of a positive obligation, combined with the breadth of permitted purposes in Part 11, creates a risk that agencies will potentially hold, for prolonged periods of time, large volumes of highly sensitive personal data (namely, the content of communications) that is no longer relevant to their functions.to conduct periodic reviews of holdings.

210. The Law Council recommends that Clause 140 of proposed Schedule 1 to the TIA Act is amended to require agencies to undertake periodic reviews of the information they have obtained under the IPO regime, to assess whether it is likely to remain relevant to a permitted purpose under Part 11, and therefore whether the obligation to destroy irrelevant information is enlivened.

Recommendation

- **Clause 140 of proposed Schedule 1 to the TIA Act should be amended to require agencies to undertake periodic reviews of information obtained under interception and stored communications IPOs to assess whether the obligation to destroy irrelevant information under Clause 140 is enlivened.**

Telecommunications data

Absence of periodic review and deletion obligations

211. The limited deletion obligations in Clause 140 are limited expressly to communications content, and do not cover telecommunications data obtained under an IPO. The Explanatory Memorandum states that this exclusion replicates the current approach taken in the domestic access arrangements in the TIA Act in relation to telecommunications data.[116]

212. In support of extending this approach to telecommunications data obtained under IPOs, the Explanatory Memorandum refers to an undated internal review undertaken by the Attorney-General's Department, in response to recommendation 28 of the PJCIS's advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. The PJCIS recommended that the Department oversee a review of the adequacy of the existing destruction requirements that apply to documents or information disclosed pursuant to an authorisation made under Chapter 4 of the TIA Act and held by law enforcement agencies and ASIO.[117]

213. The Explanatory Memorandum indicates that this review found, among other matters, that: keeping such data for extended periods of time can be beneficial to law enforcement agencies; a destruction requirement may have little privacy benefit and could create a further burden on the telecommunications industry; and it will be administratively challenging to destroy copies of telecommunications data, given its need to be stored on numerous information management systems.[118]

[116] Explanatory Memorandum, [62] and [456]
[117] Ibid.
[118] Ibid.

214. The Law Council is concerned that the report of this internal review does not appear to have been released publicly (or is not readily able to be located on the public record) with the result that it has not been possible to examine the reasoning for its conclusions, which are now relied upon to justify the design of aspects of the IPO scheme. Given the reliance placed on the conclusions of this internal review for the omission of destruction obligations on telecommunications data obtained under IPOs, the Law Council considers it important that these findings are released and examined carefully as part of the Committee's review of the present Bill.

215. By way of general remarks, the Law Council is concerned by the apparent adoption of a position in relation to the **prospective** collection of telecommunications data under an entirely new scheme, which appears to be based heavily on administrative difficulties identified in reviewing and deleting large volumes of 'legacy data' already within agencies' holdings (namely, large volumes of telecommunications data obtained under the domestic arrangements in Chapter 4 of the TIA Act). The Law Council considers that any difficulties in managing deletion of data that is **already** held by agencies does not, and should not, preclude the development and implementation of better practices in relation to data that is **proposed** to be obtained under an entirely new authorisation framework.

216. The extrinsic materials to the Bill do not explain why improved systems and processes for holding and managing telecommunications data obtained under an IPO could not be implemented for telecommunications data obtained under the new scheme, to enable agencies to review their data holdings efficiently, and consider whether that data remains relevant, and to delete it if is no longer relevant. The development of better practices of prospective application for the IPO scheme may also make it easier to apply them to telecommunications data obtained under the domestic regime, at least from a prospective date in future, even if the deletion of 'legacy data' already within agencies' holdings would be impracticable.

217. In addition, the Law Council queries whether the review undertaken by the Attorney-General's Department, and cited in support of the exclusion of IPO telecommunications data from a destruction requirement in Clause 140 of the Bill, specifically considered the practices of ASIO. The portions of that review's findings referred to in the Explanatory Memorandum refer only to the circumstances of law enforcement agencies, yet the proposed exclusion of telecommunications data from the destruction requirement in Clause 140 applies equally to law enforcement agencies and ASIO. The Law Council notes that the submission of the Inspector-General of Intelligence and Security to this Committee's present Review of the Mandatory Data Retention Regime made the following comment, which suggests that the matter of ASIO's retention of telecommunications data remains unresolved:

> *The Committee may recall that, in its Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014, the Committee recommended the Government initiate a review of the ASIO Guidelines, including 'examining requirements to govern ASIO's management and destruction of information obtained on persons who are not relevant, or no longer relevant, to security matters'. Further, in its Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, the Committee recommended that the Attorney-General's Department oversee a review of the adequacy of existing destruction requirements that apply to documents or information disclosed pursuant to an authorisation under Chapter 4 of the TIA Act and held by enforcement agencies and ASIO. Both recommendations were accepted by the Government … [T]he ASIO Guidelines have not*

been updated since 2007, and there have been no changes to ASIO's legislation or policies that would require data that is not relevant, or no longer relevant, to security to be destroyed. As such, IGIS considers this matter remains unresolved.[119]

218. Accordingly, the Law Council considers that the justification given for excluding telecommunications data from the deletion obligations in proposed Clause 140 requires further analysis. In the absence of compelling evidence to substantiate a claim that it would be impractical to impose a **prospective** requirement on law enforcement agencies and ASIO in relation to the review and deletion of irrelevant telecommunications data obtained under an IPO, the Law Council considers that Clause 140 should be amended to cover that data.

Recommendation

- **In the absence of compelling evidence to support a claim that it would be impracticable to do so, the obligations imposed on agency heads under Clause 140 of proposed Schedule 1 to delete irrelevant information from their holdings should be amended to apply to telecommunications data obtained under an IPO.**

Guidance, evidentiary issues and enforcement

Administrative guidance on the operation of the scheme

219. The IPO scheme will need to be supported with administrative guidelines and other supporting materials for participating agencies and the communications industry about the requirements of the scheme. The Law Council considers that it is important that such materials are finalised promptly and are released publicly to ensure appropriate transparency about the operation of the scheme. The Law Council would be pleased to participate in consultations on exposure drafts of those materials.

220. The Law Council considers it particularly important that the Minister's Guidelines to ASIO (made under section 8A of the ASIO Act) are updated to take account of requirements in the present Bill, and to implement repeated recommendations of the PJCIS since 2014 for the guidelines to be updated to provide explicit guidance on the exercise of significant new and expanded powers. [120]

221. The Law Council notes that the introduction and intended urgent passage of the present Bill, together with the operation of the assistance and access regime in Part 15 of the Telecommunications Act, makes it critical that these guidelines are updated and released as a matter of priority. The Law Council also supports consultation with civil society on draft revised guidelines before they are finalised and issued, and would be pleased to participate in any such consultations.

[119] Inspector-General of Intelligence and Security, Submission No 36 to Parliamentary Joint Committee on Intelligence and Security, Review of the Mandatory Data Retention Regime (2 August 2019), 14.
[120] See, eg, Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014* (Report, September 2014), Recommendations 3 & 4.

Recommendation

- **The Government should, as a matter of priority, develop administrative guidance on the application of the IPO scheme and release these materials publicly for consultations before they are finalised and published, prior to the commencement of the amendments. This should include completion of a review of the Minister's Guidelines to ASIO, and the issuing of new guidelines under section 8A of the ASIO Act, as a matter of urgency.**

Evidentiary certificates in relation to compliance with IPOs

222. Part 12 of proposed Schedule 1 to the TIA Act empowers IPO agencies, foreign DCPs and the ADA to issue evidentiary certificates in relation to specified acts or things done under, or in relation to, an IPO. All certificates are of a prima facie character, except certificates issued by DCPs setting out the acts and things done to comply with an IPO, which are deemed to be conclusive evidence of those matters.[121]

Use of conclusive certificates

223. No specific explanation is provided for the conclusive, rather than prima facie, nature of certificates issued by DCPs. The Explanatory Memorandum simply refers to the potential for practical difficulties that may be incurred by a foreign DCP in giving evidence in Australian proceedings, and points to potential limitations in the compellability of their officers.[122]

224. The Explanatory Memorandum does not address how the removal of a person's right to challenge the matters listed in a conclusive evidentiary certificate is compatible with their right to a fair trial or hearing. (For example, in the case of a defendant in criminal proceedings who challenges the admissibility of evidence obtained under an IPO, on the basis that the DCP did acts or things contrary to those specified in the evidentiary certificate and those activities breached conditions or limitations in the IPO.)

225. Further, the Explanatory Memorandum does not address the apparent anomaly in the designation of certificates issued under Subclause 161(3) as conclusive, and the prima facie nature of evidentiary certificates that may be issued by DCPs about the acts and things done to obtain information that they may choose to provide **voluntarily**, in addition to providing the information sought in an IPO.[123]

226. The Law Council acknowledges that existing provisions of the TIA Act, such as subsection 18(2), make provision for telecommunications carriers to issue conclusive evidentiary certificates in relation to acts or things done to give effect to a domestic interception or stored communications warrant. However, the Law Council considers that this provision is not suitable for reproduction in the IPO regime, which covers a considerably broader range of electronic communications technologies than telecommunications (including technologies that may not yet exist). This means that there is likely to be extensive variation in the specific acts or things that DCPs may undertake to give effect to an IPO, and therefore greater scope for a party to legal proceedings to seek to challenge the evidence of a DCP about the specific acts or things they did to give effect to the IPO, including on the basis that they exceeded what was necessary to give effect to that IPO (for example, by contravening any

[121] Ibid cl 161(3)(b)
[122] Explanatory Memorandum, [540].
[123] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, Clause 162.

applicable conditions or limitations). There is also an open question as to whether subsection 18(2) itself remains appropriate in contemporary circumstances.

227. In the absence of a compelling justification for the use of conclusive evidentiary certificates, the Law Council recommends that **all** evidentiary certificates under Part 12 of proposed Schedule 1 to the TIA Act should be of a prima facie nature.[124]

Recommendation

- **Subclause 161(3) of proposed Schedule 1 to the TIA Act should be amended to provide that evidentiary certificates able to be issued by a DCP in relation to acts and things done to comply with an IPOs are of a prima facie nature.**

Enforcement of civil penalty provisions against DCPs

228. Part 8 of proposed Schedule 1 to the TIA Act contains a civil penalty provision for DCPs who do not comply with an IPO that is given to them, provided that they meet a minimum threshold with respect to their connection with Australia. Part 8 enlivens the standard enforcement provisions of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth),[125] and proposes to appoint the Communications Access Co-Ordinator (**CAC**) as the 'authorised applicant' who may commence enforcement proceedings.[126]

Appointment of 'authorised applicant' in civil enforcement proceedings

229. The Explanatory Memorandum describes the CAC as an 'independent officer within the Department of Home Affairs', although it does not explain the reasons the CAC is thought to be independent, or from whom it is thought to be independent, including in the specific context of enforcing IPOs.[127] The Law Council is of the view that the CAC lacks the necessary independence to perform the enforcement functions of 'authorised applicant'. The TIA Act provides that the CAC is the Secretary of the Department of Home Affairs, or a person or body appointed by the Minister for Home Affairs by legislative instrument, with no limitations by reference to their qualifications or seniority.[128] Currently, a number of staff of the Department of Home Affairs are appointed as CAC, including staff at the EL1 and EL2 classifications.[129]

230. The Department of Home Affairs is among the agencies that can obtain IPOs,[130] and is the portfolio department for most of the other Commonwealth agencies that can obtain IPOs. These circumstances may raise doubts about the independence of the CAC as the authorised applicant in making enforcement decisions in relation to those IPOs, since it has an evident interest in securing compliance for the benefit of its own investigations, or those of portfolio agencies.

231. The Law Council considers that the entity responsible for the civil enforcement of IPOs against foreign DCPs should be demonstrably independent from the agencies that may obtain those IPOs. The Law Council recommends that the Secretary of the

[124] See also: Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5* (2020), 32.
[125] Ibid cl 126(1).
[126] Ibid cl 126(2).
[127] Explanatory Memorandum [418].
[128] *Telecommunications (Interception and Access) Act 1979* (Cth), s 6R.
[129] *Telecommunications (Interception and Access) (Communications Access Co-ordinator) Instrument 2018*, cl 6.
[130] As a 'criminal-law enforcement agency' within the meaning of s 110A of the TIA Act, as applied by paragraph (b) of the definition of 'relevant agency' in proposed Schedule 1 to the TIA Act.

Attorney-General's Department would be suitably independent for the purpose of decision-making about the commencement and conduct of civil enforcement actions.

232. In addition, given the significant maximum civil penalty of nearly $10 million for DCPs that are bodies corporate,[131] the Law Council considers that the class of persons to whom the 'appropriate authority' may delegate their functions should be limited to officers with appropriate seniority – namely, an employee of the Department who holds a position that is classified as Senior Executive Service Band 1 or higher.

Recommendation

- **Clause 126 of proposed Schedule 1 to the TIA Act should be amended to provide that the Secretary of the Attorney-General's Department, and not the Communications Access Co-Ordinator, is the 'authorised applicant' for the purpose of the enforcement provisions in Part 8.**

[131] Bill, Schedule 1, item 43, inserting proposed Schedule 1 to the TIA Act, cl 124 and 126(4).