Law Council
OF AUSTRALIA

Office of the President

21 May 2020

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6100
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Chair

Inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

1. Thank you again for inviting the Law Council of Australia to appear at the Parliamentary Joint Committee on Intelligence and Security (**Committee**) public hearing on 12 May 2020. My colleagues and I took two matters on notice during questioning from the Shadow Attorney-General, Hon Mark Dreyfus QC MP, and Mr Julian Leeser MP. I have provided the Law Council's responses to these questions below.

2. To further assist the Committee's deliberations, I have provided some additional information to supplement the Law Council's responses to questions from Mr Leeser about the legal effect of our recommended safeguards in relation to the death penalty at pp. 19-21 of our initial written submission to the Committee of 5 May 2020.

Questions from Mr Dreyfus: matters that should be addressed in the Bill

Question and background

3. Mr Dreyfus asked the Law Council to outline the key matters that the Law Council considers should be regulated directly in primary legislation, rather than being left to individual agreements. One of the four key areas[1] identified was the inclusion of an analogous provision to that in §2523(b)(1)(B)(iii) of the US Stored Communications Act, as inserted by the CLOUD Act.[2] This would require the Attorney-General to certify that an international agreement is compatible with all of Australia's human rights obligations. It would include a requirement to specifically certify compatibility with several enumerated rights, including: rights to privacy, freedom of expression, association,

[1] These four areas (with references to relevant pages of the Law Council's submission) are:
(1) Minimum human rights safeguards that must be included in every agreement (pp. 17-24).
(2) A process for the independent review of decisions to issue IPOs (pp. 37-40).
(3) Arrangements for Australia to monitor the use of 'incoming' IPOs issued by foreign countries (pp. 47-49).
(4) Statutory requirements for the independent and parliamentary review of the IPO scheme (pp. 49-51).

[2] Codified as 18 USC 121 ('Stored Wire and Electronic Communications and Transactional Records Access').

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

peaceful assembly and fair trial; the rights of the child; and the prohibitions on torture, cruel, inhuman or degrading treatment or punishment, and arbitrary arrest and detention.

4. This certification requirement would be a statutory pre-condition to the exercise of the power in proposed Clause 3 to make regulations prescribing an agreement as a Designated International Agreement (**DIA**) and therefore enlivening the legislative framework governing the issuing of International Production Orders (**IPOs**) to Designated Communications Providers (**DCPs**) located in the relevant foreign country party to the agreement, and the requirement for Australian communications providers to comply with to 'incoming' orders received from authorities of that foreign country.[3]

5. The Law Council noted that this provision would require the Attorney-General to certify, among other matters, that the agreement contained adequate protections for human rights in relation to categories of particularly sensitive information that could potentially be within the scope of a production order. Namely, the Law Council identified journalistic information including source identities (to ensure that the agreement is compatible with rights to privacy and freedom of expression); and information that is subject to client legal privilege (to ensure that the agreement is compatible with rights to privacy and a fair trial or hearing).

Matter taken on notice

6. Law Council witnesses indicated an intention to provide the Committee with supplementary information about possible additional statutory protections for these specific categories of particularly sensitive information, in relation to both Australia's outgoing IPOs, and incoming IPOs received from foreign authorities. It was noted that, in the case of Australia's outgoing IPOs issued to foreign communications providers, specific statutory protections could apply in addition to the overarching Attorney-General's certification requirement outlined above. This could facilitate both the human rights compatibility of individual agreements, and the consistency of treatment of such information across all agreements. It was noted that specific protections may be particularly important in relation to journalistic and legally privileged information because, once disclosed, its confidential character is lost. It may therefore be impossible to remediate the ensuing harm to data subjects and others.

Response

<u>The need for additional statutory protections for types of particularly sensitive information</u>

7. The Law Council is supportive of additional, specific statutory protections for categories of information that are fairly characterised as particularly sensitive, in a manner similar to the protections provided in the *Crime (Overseas Production Orders) Act 2019* (UK) (**COPOA**) or the journalist information warrant provision in the domestic telecommunications data access regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**).

8. The relevant categories of particularly sensitive information should include, as a minimum, journalistic information and information that is subject to client legal privilege.

[3] Law Council of Australia, *Submission to the Parliamentary Joint Committee on Intelligence and Security, Review of the Telecommunications Amendment (International Production Orders Bill) 2020*, May 2020, 22-24.

9. The Committee may also wish to consider whether there should be further categories of particularly sensitive information that should attract specific, additional statutory protections under the IPO regime. For example, in the UK, the COPOA excludes 'confidential personal information' from the scope of Overseas Production Orders. This comprises health records and records of personal spiritual or welfare-related counselling that were created in circumstances giving rise to an obligation of confidence that is still in existence, or is held subject to statutory non-disclosure obligations.[4]

Protections in 'outgoing' IPOs issued by Australia to foreign DCPs

10. The Law Council supports some specific statutory protections to the issuing criteria for all forms of IPOs, in addition to the overarching Attorney-General's certification requirement about the compliance of international agreements with all of Australian's human rights obligations. Specific protections for legally privileged information and journalistic information are outlined below.

Protection of legally privileged information

11. The Law Council would support the adoption of similar requirements to those in the UK's COPOA with respect to legally privileged information. Under the COPOA, Overseas Production Orders cannot be issued in relation to legally privileged information, and the authorised officer of a UK law enforcement agency who is applying for an order must not seek in an application any information to the extent that they have reasonable grounds for believing that this information consists of, or is, legally privileged information.[5] The basis for the applicant's belief can then be tested by the issuing authority.

12. The Law Council considers that the Australian adoption of equivalent provisions to the UK orders should include an criterion that specifically requires the issuing authority to review the applicant's claim that there are no reasonable grounds on which to believe that an order is, or consists of, legally privileged information. This should be in the form of a prohibition on issuing an order unless the issuing authority is satisfied that there are reasonable grounds on which to believe that the information sought in the IPO does not consist of, or is not, legally privileged information. The adoption of a statutory issuing criterion will ensure that the matter is identified and assessed consistently in all IPO applications.

13. The Law Council also considers that provision should be made in the Bill to require a foreign communications provider to notify a data subject of the existence of an IPO seeking the production of their data, to enable that data subject to determine whether to bring proceedings in an Australian court, or via the independent review process for resolving objections to the issuing of IPOs (as recommended at pp. 39-40 of the Law Council's submission). This safeguard would ensure that the person in whom legal privilege vests would have an opportunity to make that claim and collaterally challenge the issuing of the IPO in respect of its application to privileged information. It would bring the Australian IPO regime into line with that of the UK. Under the COPOA, the

[4] COPOA (UK), s 3 (definition of 'excluded information' which includes 'confidential personal information' as well as 'legally privileged information') and s 1(3) (applications for orders must not seek information that the applicant has reasonable grounds to believe is or includes 'excluded information').

[5] COPOA, ss 1(3) and 3. The term 'legally privileged information' is defined by reference to the meaning of that term in s 10 of the *Police and Criminal Evidence Act 1984* (UK). It covers lawyer-client communications in connection with the provision of legal advice; or the contemplation or conduct of legal proceedings. This is provided that the relevant information is in the possession of a person who is entitled to possess it; and that the relevant information is not held with the intention of furthering a criminal purpose.

default position appears to be that a foreign communications provider (such as an Australian DCP) is able to notify data subjects of UK-issued Overseas Production Orders which require the provider to disclose the data subject's information. This default right of disclosure is subject to the UK judicial issuing authority specifically making a non-disclosure order, which must specify an expiry date.[6] The ability to delay notification via a specific order for non-disclosure would make appropriate provision for disclosures that would be reasonably likely to prejudice extant law enforcement investigations. In the case of ASIO's national security IPOs, consideration may need to be given to a longer non-disclosure period if a case for secrecy can be established, on the basis of demonstrable prejudice to Australia's national security, in respect of individual IPOs.

Protection of journalistic information

14. As Mr Dreyfus noted at the public hearings, the IPO regime does not include equivalent provisions to those in Division 4C of Chapter 4 of the TIA Act, in relation to journalist information warrants to authorise access to telecommunications data.

15. The Law Council is concerned that this differential treatment would produce an inequity in the degree of protection given to journalistic information based solely on the location of the relevant data, and not its sensitivity or the purpose to which it will be put. As the Law Council commented at pp. 34-35 of its submission, efforts should be made to prevent the IPO regime from entrenching such arbitrary differences between the international and domestic interception and access regimes.

16. The Law Council notes that the IPO regime applies an external authorisation model to telecommunications data access, in contrast to the model of internal authorisation under the domestic access regime in Chapter 4 of the TIA Act. However, this difference does not dispense with the need for the IPO regime to match the specific issuing process (including a role for an independent Public Interest Advocate appointed by the Prime Minister under section 180X of the TIA Act) and specific issuing criteria available under the domestic journalist information warrant provisions.

17. For example, under sections 180L and 180T of the TIA Act, the issuing authority for a journalist information warrant may only issue a warrant if they are satisfied that the public interest in doing so outweighs the public interest in protecting the confidentiality of a journalistic source. The issuing authority must consider a number of prescribed factors in making this assessment, including: the likely interference with privacy; the gravity of the matter in respect of which a warrant is sought; the utility of the information to the investigation; whether reasonable attempts have been made to obtain the information by other means; any submissions made by the Public Interest Advocate; and any other relevant matter.

18. The Law Council considers that the adoption in the IPO regime of these elements of the domestic journalist information warrant regime is essential to ensuring that journalistic information is protected consistently, irrespective of whether a journalist's data is physically stored in Australia or in a foreign country. It would not be acceptable to leave the specialised public interest consideration associated with journalistic data to the more general issuing criteria for IPOs in the Bill as drafted, as this is unlikely to facilitate comprehensive and consistent consideration in all applications.

[6] COPOA (UK), s 8 (inclusion of non-disclosure requirement in an overseas production order).

Protection of other confidential personal information

19. The exclusion in the COPOA outlined above also applies to 'confidential personal information' which covers the matters summarised at paragraph 9 above.[7] The Committee may wish to consider whether a similar exclusion should also apply to confidential personal information in the Australian IPO regime; or whether it could be dealt with acceptably via the overarching Attorney-General's certification requirement recommended by the Law Council; and in the privacy-related issuing criteria for individual IPOs (provided that the relevant issuing criteria for ASIO is amended as recommended at pp. 33-34 of the Law Council's submission).

Protections in 'incoming' IPOs issued to Australian DCPs by authorities of foreign countries

20. As noted at pp. 47-49 of the Law Council's submission, the Law Council is concerned that the Bill makes no provision to ensure that the Australian Designated Authority (**ADA**) or other persons whose data is held in Australia ('data subjects') have awareness of the circumstances in which the significant immunities from Australian law in Part 13 of the Bill are enlivened, when Australian DCPs comply with orders issued by foreign authorities. (Part 13 provides that disclosure offences in relation to telecommunications content and data under the TIA Act and *Telecommunications Act 1997* (Cth) do not apply in these circumstances. It also provides that compliance with an 'incoming IPO' is taken to be authorised by the TIA Act, for the purpose of provisions of the *Privacy Act 1988* (Cth) that prevent disclosures of personal information unless authorised under another law.)

21. In addition to the concerns raised in the Law Council's submission, this absence of visibility also means that there is limited ability for Australia to ensure that data subjects whose Australian-held data is the subject of an incoming IPO issued by a foreign authority are notified of the IPO and have an opportunity to challenge it in an Australian court or the foreign jurisdiction, if desired, for example because the order seeks to compel the production of privileged information. A data subject may, for example, wish initiate a challenge on the grounds that some or all of the information sought under the order is subject to client legal privilege, such as correspondence held in cloud storage between the person and their lawyer, for the purpose of obtaining legal advice or in relation to the conduct of legal proceedings.

22. In practice, the absence of wholesale secrecy provisions in the corresponding laws of other countries, such as the US and the UK, may mean that Australian DCPs would be able to notify data subjects of such requests under the laws of the foreign country, and either the individual data subject or the DCP, or both parties, may initiate a challenge – for example, an action by the provider under §103 of the CLOUD Act in the case of a US-issued warrant, or an action at common law by the data subject.

23. However, the Law Council suggests that Australian law should provide further protective mechanisms, given that it is the enlivenment of immunities under Australian law that would enable privilege to be compromised in these circumstances. To aid the timely resolution of such claims, the Law Council considers that Australian law could usefully make provision for their resolution in an Australian court exercising federal jurisdiction.

24. Further, the Law Council considers that the Bill and Australia's bilateral agreements with foreign countries should be premised on a 'presumption of notification' of data

[7] Ibid, ss 1(3) and 3 ('excluded information' that cannot be sought in overseas production orders).

subjects of IPOs pertaining to their information, unless an issuing authority is reasonably satisfied that real-time notification would cause significant prejudice to an extent law enforcement operation, or would otherwise endanger the lives or safety of other persons.

25. Accordingly, the Law Council further considers that the Bill and Australia's bilateral agreements with foreign countries should also make provision for those cases in which a foreign production order is issued to an Australian DCP subject to a non-disclosure order, which would prevent the DCP from notifying a data subject of an order that may potentially seek privileged information. In such cases, the Law Council considers that there should also be a mechanism to enable the review of the underlying secrecy order by an Australian or foreign court, especially in light of the risk that the secrecy order would deprive the data holder of the opportunity to protect legally privileged communications. In view of the widespread use of cloud platforms to store and manage all of the data subject's information, including highly sensitive and confidential information such as legally privileged communications, this is a substantial concern.

26. To ensure that a DCP has an incentive to consult with the data subject as to whether privilege may exist in information that is the subject of an incoming IPO, and to take other reasonable steps to identify whether privilege may vest in information sought under that order, the Law Council considers it would be appropriate for the Bill to be further amended to apply a pre-condition to the lifting of the 'blocking provisions' applying to DCPs in Part 13 of the Bill (that is, secrecy offences and provisions of the Privacy Act limiting secondary disclosure of personal information). In particular, the Law Council considers it would be appropriate for the Bill to provide that the 'blocking provisions' under Part 13 **will not** be lifted in certain circumstances, so as to place an onus on DCP to take reasonable steps to consider the existence or likely existence of privilege, and consult with the data subject.

27. Part 13 should provide that the blocking provisions will not be lifted if the DCP is aware of a claim of legal professional privilege in relation to information that is the subject of a foreign production order; or if there are reasonable grounds for believing that the information requested under the order is, or includes, information that could be subject to a claim for legal professional privilege (for example, correspondence between a data subject and their lawyer held in a cloud storage service would give rise to a reasonable belief that privilege may exist without a requirement for any third party to read the substantive contents of those documents). The 'blocking provisions' under Australian law should remain in force in relation to the DCP until the privilege claim is disposed of, and the DCP is informed that privilege does not apply or has been voluntarily waived.

28. While the Law Council acknowledges that the UK and US framework legislation does not contain equivalent protections to those proposed above, it is important to note those jurisdictions have judicial review rights under their respective human rights frameworks that would have application in these circumstances. For example, review rights would be available under the *Human Rights Act 1998* (UK). These far exceed the more limited judicial review rights available in Australia arising from section 75 of the Constitution.

Questions from Mr Leeser: statutory death penalty protections

Question

29. Mr Leeser asked representatives of the Law Council questions about the potential application of its recommended amendments to Clause 3 of the Bill at pp. 19-21 of its submission to strengthen death penalty safeguards. Mr Leeser was interested in how these safeguards would operate in relation to a bilateral agreement with the US. Law Council witnesses took on notice a question as to whether offences under US law for espionage, foreign interference and terrorism carried the death penalty.

Response

30. Federal offences in relation to espionage and certain terrorism-related activities are punishable by a maximum penalty of death under US federal laws.[8] The Federal Attorney-General has executive discretion as to whether this penalty is sought or carried out.[9] The Law Council understands that death penalty sentences are relatively rare in federal jurisdiction. A US non-profit organisation, the Death Penalty Information Centre, has reported that 'between reinstatement of the federal death penalty in 1988 and 2019, 79 defendants have been sentenced to death, of whom 3 have been executed'.[10]

Additional information: recommendations to strengthen death penalty protections

Background

31. Mr Leeser also asked representatives of the Law Council about the effect of the two recommended options at p. 21 of its submission to strengthen the death penalty safeguards in Clause 3 of the Bill. He inquired whether option 2 would have a broader application than the existing provisions of Subclauses 3(2) and 3(5).

32. Law Council witnesses indicated that option 1 would provide the stronger protection of the right to life by effectively precluding the implementation of an international agreement unless the foreign country party provided an undertaking not to use Australian-sourced information in the prosecution of an offence punishable by death.

33. It was noted that option 2 would provide for very limited use of Australian-sourced information by countries that have the death penalty, strictly in line with the circumstances currently identified in the Australian Government's administrative guidance on the interpretation of 'special circumstances' provisions in the *Mutual Assistance in Criminal Matters Act 1987* (Cth). Namely, Australian-sourced

[8] 18 USC § 794 (espionage); 18 USC § 2332 (terrorist murder of a US national in a foreign country). Various murder offences are also punishable by death (for example, murder of certain US and foreign officials, and the murder of a US national in a foreign country) as is the offence of treason. For a collation of all federal offences subject to the death penalty, see: Death Penalty Information Centre, United States, *Federal Laws Providing for the Death Penalty*, <https://deathpenaltyinfo.org>.

[9] Federal executive policy requires all federal prosecutors to submit all potential federal capital punishment cases to the Department of Justice for review, and a decision by the Attorney-General regarding whether to see the death penalty: Department of Justice, United States, *United States Justice Manual*, §§ 9-10.010 – 9-10.200, <https://www.justice.gov/jm/justice-manual>.

[10] Death Penalty Information Centre, United States, *Background on the Federal Death Penalty,* <https://deathpenaltyinfo.org>.

information could only be used if the death penalty is not sought or carried out; or only for exculpatory purposes (that is, as evidence in support of a defence).

34. The Law Council noted that this would address the overbreadth in subclauses 3(2) and 3(5) under which the Minister for Home Affairs must obtain an assurance from the relevant foreign government 'relating to **the use** or non-use' of Australian-sourced information in death penalty proceedings. There is no requirement that any undertaking about 'the use' of information (as opposed to an undertaking providing for its non-use) must be consistent with the right to life and Australia's opposition to the death penalty in all countries.

35. It was also noted that option 2 in the Law Council's recommendation was provided in the interests of pragmatism. That is, the Law Council recognises that a wholesale statutory prohibition may preclude the finalisation of an agreement with the US, given that the death penalty exists under the laws of some US states. This may create significant practical difficulties for Australian law enforcement agencies, given that many major electronic communications providers are located and store relevant data in that country.

Additional information

36. To avoid doubt, the second option in the Law Council's recommendation at p. 21 of its submission is **narrower** than subclauses 3(2) and 3(5) of the Bill as presently drafted.

37. This is because option 2 would only allow the use of Australian-sourced information in countries that have the death penalty in very limited circumstances, which do not expose an individual to the imposition of the death penalty. That is, use of Australian-sourced information would be restricted to proceedings in which the death penalty is the maximum penalty but is not sought or carried out; or for the sole purpose of being used in evidence by a defendant in death penalty proceedings.

38. In contrast, as noted at pp. 19-20 of the Law Council's submission, the exceptionally broad language in subclauses 3(2) and 3(5) appears to make it possible for the requirement to be satisfied by the receipt of an undertaking that Australian sourced information **will or may** be used to i**nculpate** a person in death penalty proceedings (for example, admitted in evidence by the prosecution in a case in which the maximum penalty is death, and that penalty is sought by the prosecution). While such an application would be in clear violation of the right to life and Australia's longstanding bipartisan opposition to the death penalty, there is nothing in the ordinary meaning of the broad words used in the provision – which refers to an undertaking 'relating to the use or non-use' of Australian-sourced information – that would provide an unequivocal legal prohibition, and explicitly communicate this to relevant decision-makers.

39. While the Law Council acknowledges that the Australian Government may not intend to utilise subclauses 3(2) and 3(5) in this way, the underlying problem is that the provisions provide no definitive legal safeguard against their aberrant use or misuse in the future. Accordingly, the Law Council shares the concern of the Parliamentary Joint Committee on Human Rights that this makes it impossible to conclude that the proposed IPO regime is compatible with the right to life.[11] This overbreadth should be removed.

[11] Parliament of Australia, Parliamentary Joint Committee on Human Rights, *Scrutiny Report 4* (2020), 22-23.

40. Thank you again for the opportunity to participate in this inquiry. I hope that this information is of assistance to the Committee. Should you require any further information or wish to discuss, please contact the Law Council's Director of Policy, [redacted]

Yours sincerely

[redacted]

Pauline Wright
President