PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Advisory Report on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

ISBN 978-1-76092-128-6 (Printed Version)

ISBN 978-1-76092-129-3 (HTML Version)

Contents

Abbreviations v

Membership of the Committee vii

Terms of Reference ix

List of Recommendations xi

The Report

1 Background 1

The Bill and its referral 1

Conduct of the inquiry 2

Report structure 2

Summary of the Bill 3

The Committee's review of telecommunications legislation 4

Committee comment 6

2 Designated International Agreements 9

Mutual Legal Assistance 9

Enabling provisions of the CLOUD Act 15

Incoming international production orders 16

Designated international agreements 17

International comparisons 21

Committee comment 22

Human rights obligations 29

The right to life 30

Protection against arbitrary or unlawful interference with privacy 32

The protection of the right to freedom of expression 37

Committee comment 40

3 Outgoing International Production Orders 45

Definitional terms 45

Seeking an International Production Order 47

Enforcement of the criminal law 48

Monitoring of a person subject to a control order 54

The Administrative Appeals Tribunal as an issuing authority 60

Committee comment 63

For the purposes of upholding Australia's national security 66

Committee comment 77

4 Approval, Compliance and Oversight 81

The role of the Australian Designated Authority 81

Compliance with IPO requests 86

Evidentiary certificates to demonstrate compliance with IPO requests 87

Oversight by the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security 91

Reporting and record-keeping requirements 97

Notice to the subject of an IPO 100

Record-keeping requirements and retention of data 102

Review of the overall IPO regime 105

Committee comment 107

Appendix A. List of submissions 113

Appendix B. Witnesses appearing at public hearings 115

Abbreviations

AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACLEI	Australian Commission for Law Enforcement Integrity
ADA	Australian Designated Authority
AFP	Australian Federal Police
ANU LRSJ	Australian National University Law Reform and Social Justice Research Hub
ASIO	Australian Security Intelligence Organisation
AVO	Apprehended Violence Order
CDPP	Commonwealth Director of Public Prosecutions
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act*
CSP	Communications service providers
DIA	Designated international agreement
DIGI	Digital Industry Group Incorporated
ICCPR	*International Covenant on Civil and Political Rights*
IGIS	Inspector-General of Intelligence and Security
INSLM	Independent National Security Legislation Monitor
IP	Internet Protocol
IPO	International production order
JSCOT	Parliamentary Joint Standing Committee on Treaties
MAR	Mutual assistance requests

MLAT	Mutual Legal Assistance Treaty
NSW	New South Wales
TIA Act	*Telecommunications (Interception and Access) Act 1979*
TOLA Act	*Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018*
TOLA Bill	Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018
UK	United Kingdom
USA/US	United States of America
WA	Western Australia

Membership of the Committee

Chair

Mr Andrew Hastie MP (until 22/12/2020)

Senator James Paterson (from 04/02/2021)

Deputy Chair

Hon Anthony Byrne MP

Members

Hon Mark Dreyfus QC MP

Hon Dr Mike Kelly AM MP (until 30/04/2020)

Mr Julian Leeser MP

Mr Tim Wilson MP

Ms Celia Hammond MP (from 03/02/2021)

Dr Anne Aly MP (from 03/09/2020)

Senator Amanda Stoker (until 22/12/2020)

Senator the Hon Eric Abetz

Senator Jenny McAllister

Senator the Hon David Fawcett

Senator the Hon Kristina Keneally

Terms of Reference

On 9 March 2020, the Minister for Home Affairs, the Hon Peter Dutton MP, wrote to the Committee to refer the Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020 to the Committee for inquiry and report.

List of Recommendations

Recommendation 1

1.33 In accordance with the Committee's recommendations from previous reports, which the Government has agreed to, the Committee recommends that the Government ensure that the Office of the Commonwealth Ombudsman's has sufficient resources to enable effective oversight of powers under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

Recommendation 2

2.53 The Committee recommends that a new subclause be added to the proposed Clause 182 of Schedule 1 to the Telecommunications (Interception and Access) Act 1979 to provide that designated international agreements must be published and tabled in the regulations, subject to parliamentary scrutiny, and subject to a period of disallowance.

For the commencement of the regulations, proposed Schedule 1 should be amended to provide that regulations made under clause 3 (i.e. listing an agreement as a designated international agreement) cannot commence until no earlier than the expiry of the standard period for disallowance (i.e. 15 sitting days) under the Legislation Act 2003, or until the commencement of the other party's agreement, whichever is the longer.

For the period for disallowance, the bill should be amended to provide that the statutory disallowance period for regulations made under proposed clause 3 of Schedule 1 is the longer of:

- the standard period for disallowance under the Legislation Act 2003; or
- the period for disallowance that applies in the parliament of the foreign country (i.e. the other party to the relevant international agreement).

Recommendation 3

2.58 The Committee recommends that an additional subclause be added to the proposed Clause 182 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that a designated international agreement may be renewed or extended for a period of three years without completing the parliamentary treaty process, if such a renewal or extension is proposed without amendment to the agreement.

However, the Committee recommends that the clause also provide that, following the term of the initial agreement and any additional three year period, any further renewal or extension should be subject to parliamentary scrutiny and disallowance even where no amendment is proposed.

Finally, the same clause should also be amended to provide that, whenever an amendment to a designated international agreement is made or proposed, the amended agreement must be specified as a new agreement in the regulations and thus subject to the usual parliamentary treaty process and be subject to disallowance.

Recommendation 4

2.64 The Committee recommends that a new subclause be included in proposed Clause 3 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that – in order to qualify as a designated international agreement – the agreement must:

- prohibit the foreign government from intentionally targeting an Australian citizen or permanent resident; or
- prohibit the foreign government from intentionally targeting a non-Australian person located outside of Australia if the purpose is to obtain information about an Australian citizen or permanent resident;
- in relation to production orders for the interception of communications, require that the interception activities of the foreign government only be carried out for the purpose of obtaining information about communications of an individual who is outside of Australia;
- provide that all production orders must comply with the minimum requirements for foreign orders specified in paragraph 2.61;
- include safeguards for the use, handling and disclosure of information, as set out in paragraph 2.62;
- provide that all production orders must comply with the domestic law of the relevant foreign country;
- provide that production orders must not last longer than is reasonably necessary to accomplish the approved purposes of the order;
- provide that no production order may relate to the prevention, detection, investigation or prosecution of a political offence or an offence that is not recognised in the ordinary criminal law of Australia; and
- provide that a production order may only be issued if the same information could not reasonably be obtained by another less intrusive method.

Recommendation 5

2.66 The Committee recommends a subclause be included in proposed Clause 3 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that a designated international agreement shall not permit a foreign government to:

- issue an order at the request of or to obtain information to provide to the Australian government or a third-party government, nor shall the foreign government be required to share any information produced with the Australian government or a third-party government.

- such a prohibition will not preclude a foreign government seeking authorisation to share information as set out by Recommendation 4.

Recommendation 6

2.68 The Committee recommends a subclause be included in proposed Clause 3 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that incoming international production orders under a designated international agreement must only be issued for the purpose of obtaining information relating to the prevention, detection, investigation or prosecution of serious crime, including terrorism.

Recommendation 7

2.70 The Committee recommends that proposed Clause 182 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to provide that, for the purposes of the Act, an agreement – and a foreign government – will be considered to satisfy the statutory requirements (including the requirements set out in Recommendation 4 and Recommendation 8 of this report) if the Attorney-General, with the concurrence of the Minister for Home Affairs:

- determines that the agreement and the foreign government satisfy the statutory requirement; and

- submits a written certification, including a detailed explanation, of such a determination to the Joint Standing Committee on Treaties. That certification should be provided at the same time that the regulations are tabled.

Recommendation 8

2.110 The Committee recommends that the proposed Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* be amended to state that a country seeking a designated international agreement with Australia must meet the following criteria:

- Demonstrates respect for the rule of law and the principles of equality and non-discrimination, as set out in paragraph 2.103;
- Demonstrates respect for applicable international human rights obligations and commitments, as set out in paragraph 2.104;
- Clear legal procedures and restrictions governing the use of electronic surveillance investigatory powers, as set out in paragraph 2.105; and
- If:
  - There is an agreement between Australia and a foreign country; and
  - If the agreement deals with (among others things) the issue of orders (however described) by a competent authority (however described) of the foreign country; and
  - One or more offences against the law of the foreign country are punishable by death

The name of the agreement must not be specified under paragraph (1)(b) unless the Minister has received a written assurance from the government of the foreign country relating to the non-use of Australian-sourced information obtained by virtue of the agreement in connection with any proceeding for a death penalty offence in the country or territory.

Recommendation 9

2.117 The Committee recommends that, where relevant, the Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020 be amended to implement the recommendations set out in the Committee's report of its *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press*, including recommendation 2 (i.e. that the current role of the Public Interest Advocate, as provided for under the *Telecommunications (Interception and Access) Act 1979* be amended in line with the terms of that recommendation and expanded to apply to applications for international production orders.

Recommendation 10

3.64 The Committee recommends that proposed Clause 2 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to include a definition of 'urgent circumstances' which provides that in circumstances where:

- there is an imminent risk of serious harm to a person or substantial damage to property exists or, in the case of a national security IPO application, there is an imminent risk of loss of significant intelligence; and

- the production order is necessary for the purpose of dealing with that risk; and

- it is not practicable in the circumstances to submit an application in writing;

such circumstances would constitute 'urgent circumstances' for the purposes of making an oral or telephone application.

Recommendation 11

3.70 The Committee recommends that proposed Clauses 22(3), 33(3)(a), 52(3)(a) and 63(3)(a) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended in a manner that is consistent with Recommendation 11 of the of the Committee's *Review of the Mandatory Data Retention Regime*. That is, these provisions should be amended so that:

- only officers or officials who are designated as authorised officers by the head of an enforcement agency may apply for IPOs;

- only officers or officials who hold a supervisory role in the functional command chain should normally be capable of being designated as 'authorised officers' (although other individuals who hold specific appointments – rather than entire classes of officers or officials – may also be capable of being designated as 'authorised officers')

- in order to authorise an individual to be an authorised officer, the head of an enforcement agency must be satisfied that it is necessary for an individual to be an 'authorised officer' in order for the individual to carry out his or her normal duties;

- prior to the head of an enforcement agency authorising an individual to be an 'authorised officer':

  – the relevant senior officer or official must complete a compulsory training program in relation to proposed new Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*; and

  – the head of the enforcement agency must be satisfied that the senior officer or official has the requisite experience, knowledge and skills to exercise the powers under proposed Schedule 1 to the *Telecommunications (Interception and Access) Act 1979.*

Recommendation 12

3.100 The Committee recommends that proposed Clause 2 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* amended to insert a definition of senior position holder that is consistent with the provisions of the *Australian Security Intelligence Organisation Act 1979*

Recommendation 13

3.101 The Committee recommends that proposed Clauses 83 (3)–(4) and 92(3)–(4) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended so that the Director-General of Security may only delegate powers to a senior position holder

Recommendation 14

3.104 The Committee recommends that proposed Clauses 101(3)–(4) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to provide that the Director-General of Security can only authorise Australian Security Intelligence Organisation employees, or classes of Australian Security Intelligence Organisation employees, at the Executive Level 2 (or equivalent) and above to make applications on the Australian Security Intelligence Organisation's behalf.

Recommendation 15

3.108 The Committee recommends that proposed Clause 83(9) and 92(8) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to require the Australian Security Intelligence Organisation to provide the Attorney-General with:

- the particulars of the urgent circumstances because of which the person making the request considers it necessary to obtain oral agreement
- the matters that ASIO would have been required to set out in a written application to the Attorney-General.

Recommendation 16

4.69 The Committee recommends that the Australian Government ensure that the Commonwealth Ombudsman has sufficient resources to enable effective oversight of the proposed powers granted by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

Recommendation 17

4.71 The Committee recommends that the Australian Government continue to ensure that the Inspector-General of Intelligence and Security is given appropriate resources to enable effective oversight of the proposed powers granted by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

Recommendation 18

4.74 The Committee recommends that the proposed Schedule 1, Division 4 be amended to include an express provision for the Inspector-General of Intelligence and Security, or an official of the Inspector-General of Intelligence and Security, to access the register of international production orders in connection with its oversight responsibilities.

Recommendation 19

4.75 The Committee recommends that proposed Schedule 1, Clause 153 be amended to allow international production order information to be used, recorded or disclosed for the purposes of an official of the Inspector-General of Intelligence and Security exercising their duty as an official.

Recommendation 20

4.76 The Committee recommends that the *Inspector-General of Intelligence and Security Act 1986* be amended to allow for officials of the Inspector-General of Intelligence and Security to share information relating to the international production orders regime with members of the Office of the Commonwealth Ombudsman and members of the Attorney-General's Department where sharing such information is connected to the roles and duties of the member of the organisation.

Recommendation 21

4.79 The Committee recommends that:

- the *Australian Security Intelligence Organisation Act 1979* be amended to provide that a report made under proposed subsection 94(2BBA) should form part of the Australian Security Intelligence Organisation's unclassified annual report; and

- the proposed subsection provide that the recommended statistics would not be provided where the Director-General of Security considers that providing such statistics would prejudice Australia's national security, or prejudice a national security investigation.

Recommendation 22

4.85 The Committee recommends that proposed Schedule 1, Clause 135 and 136 be amended to require the Australian Security Intelligence Organisation to:

- retain a copy of a particular document for three years, or for as long as any of the data obtained under an international production order is retained, whichever is the longer; and

- retain all relevant materials supporting an application for international production order for this period.

Recommendation 23

4.88 The Committee recommends that the Bill be amended to require the Parliamentary Joint Committee on Intelligence and Security to commence a review on the effectiveness and continuing need for an international production orders regime on the earlier of the date that is:

- three years after the date on which the first designated international agreement comes into force; or

- five years after the commencement of the proposed Schedule 1 of the *Telecommunications (Interception and Access) Act 1979*.

Recommendation 24

4.90 The Committee recommends that, following implementation of the recommendations in this report, the Bill be passed by Parliament.

1. Background

1.1 This chapter sets out an overview of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('the Bill'), the context of the Bill's introduction, and the conduct of the Committee's inquiry.

The Bill and its referral

1.2 On 5 March 2020 the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 was introduced to Parliament.

1.3 The Bill complements Australia's domestic powers under the *Telecommunications (Interception and Access) Act* 1979, as enabled by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, and the ability to cooperate with trusted international partners under the *Mutual Assistance in Criminal Matters Act 1987.*

1.4 The Bill seeks to address Australia's evolving technological landscape where data previously held in Australia is now stored overseas. The Explanatory Memorandum states:

> The extensive use of foreign telecommunications and online platforms by both criminals and terrorists has made accessing this data increasingly valuable. Australian law enforcement and national security agencies require timely access to electronic information and communications data from foreign communications providers for criminal investigations and prosecutions, as well as other law enforcement and national security purposes. To collect this data, Australia has relied heavily on mutual legal assistance from overseas jurisdictions, particularly the United States, where many communications providers of interest are located. Accessing communications data through the mutual legal assistance regime is a lengthy process, which cannot keep pace

with the fast moving requirements of the investigation and prosecution of serious crime.[1]

1.5 On 9 March 2020 the Minister for Home Affairs, the Hon. Peter Dutton MP, wrote to the Parliamentary Joint Committee on Intelligence and Security ('the Committee') to inquire into the effectiveness of the Bill.

1.6 The Minister for Home Affairs asked the Committee to table its report by 26 June 2020, and that as far as possible, the Committee should conduct its inquiry in public.

Conduct of the inquiry

1.7 The Committee announced its inquiry on Friday, 13 March 2020 and invited submissions from interested members of the public by Thursday, 30 April 2020.

1.8 The Committee received 32 submissions and 12 supplementary submissions from industry, government and academia. A list of submissions received by the Committee is provided at **Appendix A**.

1.9 Submitters expressed concern about the timeframe for submissions to the inquiry,[2] noting the impact of the COVID-19 pandemic at the time submissions were opened.

1.10 The Committee held three public hearings between Tuesday, 12 May 2020 and Thursday, 14 May 2020. A list of hearings and witnesses who appeared before the Committee is included at **Appendix B**.

1.11 Copies of the submissions, the transcripts from the public hearings and links to the Bill and Explanatory Memorandum can be accessed at the Committee's website.[3]

Report structure

1.12 This report comprises four chapters:

---

1 Explanatory Memorandum, p. [2].

2 Australian Privacy Foundation, *Submission 1*, p. 3; DIGI, *Submission 23*, p. 1; The Allens Hub for Technology, Law & Innovation, *Submission 15*, p. 3.

3 www.aph.gov.au/pjcis

- The remainder of Chapter 1 provides a summary of the Bill, and how the current inquiry fits into the framework of telecommunications related inquiries of the Committee.
- Chapter 2 outlines the proposed overarching enabling instrument of the international production orders regime, designated international agreements, and discusses the interplay of the proposed regime with existing conditions. The Chapter closes with an analysis of the various human rights considerations invoked by the Bill.
- Chapter 3 details the proposed provisions governing outgoing international production orders, discussing the process outlined in the Bill to the point of approval by the relevant decision-maker.
- Chapter 4 outlines the proposed process of international production orders once agreement has been provided by the decision-maker, discussing the role of the Australian Designated Authority and other oversight bodies. This Chapter contains discussion of record-keeping processes and notice requirements as well.

Summary of the Bill

1.13 Primarily, the Bill seeks to append a new Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* which will establish a framework to allow for Australia to negotiate agreements with like-minded foreign governments for reciprocal cross-border access to communications data.[4]

1.14 An agreement made under the provisions of the Bill would allow law enforcement and national security agencies of participating countries to issue orders, through a designated authority, for the production of data directed to communications and technology companies in the other country's jurisdiction.[5]

1.15 From a domestic standpoint, the Bill provides for relevant agencies to seek orders for domestic interception or stored communications or authorisations for access to telecommunications data (referred to as 'outgoing' production orders).[6]

---

4 Explanatory Memorandum, p. [2].

5 Explanatory Memorandum, p. [2].

6 Explanatory Memorandum, p. [3].

1.16 An order may be sought by relevant agencies for the purposes of enforcing the criminal law, to monitor a person subject to a control order, or for the purposes of upholding Australia's national security.[7]

1.17 For requests received from foreign governments with a designated international agreement in place (referred to as 'incoming' production orders), the Bill removes the blocking provisions that prevent domestic communications providers and technology companies from cooperating with a request from a foreign government, when the request complies with the conditions of the designated international agreement.[8]

1.18 The Bill establishes an Australian Designated Authority to review 'outgoing' international production orders to ensure compliance with the terms of designated international agreements and to act as a first point of contact for communications providers and technology companies.[9]

1.19 The Bill provides for the Office of the Commonwealth Ombudsman to have oversight of enforcement agencies' access to the regime,[10] and the Inspector-General of Intelligence and Security (IGIS) to oversee the Australian Security Intelligence Organisation's (ASIO) access to the regime.[11]

1.20 Additional consequential amendments to the *Freedom of Information Act 1982*, *International Criminal Court Act 2002*, *Law Enforcement Integrity Commissioner Act 2006* and *Mutual Assistance in Criminal Matters Act 1987* are included in the Bill to enable the international production order regime to operate, and to incorporate relevant changes following the commencement of the *Federal Circuit and Family Court of Australia Act 2020*.

The Committee's review of telecommunications legislation

1.21 In 2018, the Committee conducted an inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ('TOLA

---

7 Explanatory Memorandum, p. [3].

8 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 167–169.

9 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 110–112.

10 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 142–150.

11 Explanatory Memorandum, p. [84].

Bill'). The TOLA Bill sought to deal with the challenges of encryption by enabling law enforcement and intelligence agencies to compel telecommunications providers to assist with encrypted communications.[12]

1.22 The TOLA Bill also made provisions for ASIO to apply for computer access warrants.[13]

1.23 The Committee's report made 17 recommendations, largely directed at the efficacy and oversight of the industry assistance measures in Schedule 1 of the Bill. In addition to a number of drafting recommendations, the Committee recommended that the IGIS and the Commonwealth Ombudsman be adequately resourced to undertake their respective oversight responsibilities.[14]

1.24 The Committee concluded its review into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ('TOLA Act') in April of 2019 to clarify the intent of its recommendations in the 2018 inquiry and provide advice to Parliament on the extent to which its recommendations were addressed.[15]

1.25 The inquiry report made three recommendations; a further statutory review, the Independent National Security Legislation Monitor to provide a report on the TOLA Act, and to ensure that the IGIS as well as the Commonwealth Ombudsman were adequately resourced to undertake their oversight functions.[16]

1.26 In its response to the review of the TOLA Act, the Government indicated its support of all three recommendations, noting in relation to resourcing:

> The Government supports this recommendation. The Government will monitor the resource impacts on the Inspector General of Intelligence and

---

12 As described in Senator the Hon. Simon Birmingham, Minister for Trade, Tourism and Investment and Deputy Leader of the Government in the Senate, *Senate Hansard*, 6 December 2018, p. 9766.

13 See Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, pp. 110–194.

14 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, December 2018, p. xiii.

15 Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, April 2019, p. 2.

16 Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, April 2019, pp. 6–7.

> Security and the Commonwealth Ombudsman and consider additional resourcing where necessary.[17]

1.27 Noting the Committee's recommendations in these inquiries, the Office of the Commonwealth Ombudsman said that funding has not yet been provided in relation to its oversight functions in the TOLA Act:

> The Office has also requested funding, which has not yet been provided, for two additional functions:
>
> - Overseeing agency compliance with the computer access and industry assistance provisions of the Surveillance Devices Act 2004 and the Telecommunications Act 1997, as introduced by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.
> - Overseeing agency compliance with the international production order scheme, introduced in the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.
>
> We are in ongoing discussion with government on these two measures.[18]

1.28 The Committee has commenced its statutory review into the TOLA Act and was due to conclude the review in September 2020.

Committee comment

1.29 The Committee acknowledges the contributions of industry, government and academia occurred during the COVID-19 pandemic, and expresses its gratitude to those who provided submissions and appeared via telepresence at its public hearings during a challenging and unprecedented time.

1.30 The Committee acknowledges that the Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020 forms one part of a suite of telecommunications and technology related legislative amendments in recent years, and further, that some of these amendments are currently being considered in other inquiries of the Committee.

1.31 The Committee considers that robust oversight arrangements provide assurance to the Australian community that these necessarily intrusive powers are used proportionately and appropriately to investigate and

---

17 *Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report: Review of the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, p. 3.

18 Office of the Commonwealth Ombudsman, *Supplementary Submission 3.1*, p. [2].

prosecute the commission of serious crimes and uphold Australia's national security.

1.32 The Committee, therefore, reiterates that an essential component of a robust oversight regime is adequate resourcing, and recommends that the Government ensure the Commonwealth Ombudsman has sufficient resources to oversee telecommunications powers.

Recommendation 1

1.33 In accordance with the Committee's recommendations from previous reports, which the Government has agreed to, the Committee recommends that the Government ensure that the Office of the Commonwealth Ombudsman's has sufficient resources to enable effective oversight of powers under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

1.34 The Committee anticipates that this issue will receive further attention in its review of the TOLA Act, and welcomes further engagement with the Commonwealth Ombudsman and the IGIS on this topic.

1.35 The Committee notes the additional consequential amendments provided by the Bill enable Schedule 1 of the Bill to function. The Committee notes that submitters have not raised concerns regarding these consequential provisions, and the Committee has not identified any concerns with these provisions. The Committee has therefore contained its discussion to the provisions of proposed Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*.

2. Designated International Agreements

2.1 This chapter provides a summary of the existing international cooperation framework, how the existing framework led to the establishment of the US *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) legislation and discusses the proposed designated international agreement provisions of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('the Bill').

Mutual Legal Assistance

2.2 As a signatory to the United Nations transnational organised crime convention,[1] Australia has the ability to request government-to-government assistance in criminal matters. The ability to request such information assists in obtaining evidence for the investigation and prosecution of drug trafficking, fraud, money laundering, child pornography and other child exploitation offences, as well as terrorism offences.[2]

2.3 These requests take the form of mutual assistance requests (MARs) which are governed by the *Mutual Assistance in Criminal Matters Act 1987* in Australia. This act governs both current incoming and outgoing requests for assistance in criminal matters.

---

1 *United Nations Convention against Transnational Organised Crime and the Protocols thereto,* opened for signature 12 December 2000, A/RES/55/25 (entered into force 29 September 2003).

2 Attorney-General's Department, *Fact Sheet – Mutual assistance overview*, available at <https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Documents/Mutual-assistance-overview.pdf>

2.4 When an offence occurs against Australian law and the investigatory body considers that information is held overseas, the Attorney-General's Department drafts a MAR, considering Australia's relationship with the foreign country, what the request asks, and relevant domestic and foreign laws.[3] Once the terms are agreed, the Attorney-General of Australia (or delegate) approves the request and it is provided to the Foreign Central Authority, who then processes the request in line with their domestic laws.[4]

2.5 A MAR can be provided for a variety of purposes:

a. Taking evidence or statements from persons;

b. Effecting service of judicial documents;

c. Executing searches and seizures, and freezing;

d. Examining objects and sites;

e. Providing information, evidentiary items and expert evaluations;

f. Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;

g. Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;

h. Facilitating the voluntary appearance of persons in the requesting State Party; and/or

i. Any other type of assistance that is not contrary to the domestic law of the requested State Party.[5]

2.6 An examination of 800 individual MARs by the Attorney-General's Department revealed that 440 applications were made to the United States of America (USA) for assistance between 2014 and 2019.

---

3 Australian Federal Police (AFP), *Submission 31*, p. 5.

4 AFP, *Submission 31*, p. 5.

5 *United Nations Convention against Transnational Organised Crime and the Protocols thereto*, opened for signature 12 December 2000, A/RES/55/25, art. 18.3 (entered into force 29 September 2003)

Table 2.1 Mutual assistance requests to the USA (2014–2019)

Agency	2014	2015	2016	2017	2018	2019
CDPP	21	15	15	12	9	9
AFP (incl. ACT Police)	13	15	19	14	21	20
NSW Police	17	19	12	15	23	27
QLD Police	15	16	13	8	12	8
SA Police	7	4	2	1	4	4
TAS Police	0	0	0	0	1	1
VIC Police	2	6	9	8	7	5
WA Police	1	0	1	4	1	1
NT Police	0	0	0	1	0	1
Total	76	75	71	63	78	76

Source: Department of Home Affairs, Supplementary Submission 10.2, pp. 39-40

2.7 The Australian Federal Police (AFP) said that it has submitted 98 MARs to the USA since 2014 for telecommunications data in relation to the following offences:

- 29 related to drug offences
- 26 related to terrorism offences
- 24 related to child sex offences
- 11 related to money laundering offences
- 4 related to foreign bribery offences
- 3 related to human trafficking offences
- 1 related to a range of serious (unspecified) offences.[6]

2.8 The Commonwealth Director of Public Prosecutions (CDPP) said that the majority of requests for evidence sought through mutual assistance are for stored communications data and telecommunications data:

> It is the latter two – stored communications data and telecommunications data which form the preponderance of evidence sought through mutual assistance,

[6] AFP, *Submission 31*, p. 5.

> predominantly from the major [communications service providers (CSPs)] located in the US, for example Facebook, Microsoft and Google. The range of CSPs in the US is increasing as new applications and products become available.[7]

2.9 The growth in requests for telecommunications data is not unique to Australia. The Synod of Victoria and Tasmania, Uniting Church said that cross-border requests are needed in a significant number of criminal investigations in the European Union:

> The European Commission reported in April 2018 that more than half of all investigations at that time involved a cross-border request to access electronic evidence. Electronic evidence is needed in approximately 85% of criminal investigations. In two-thirds of the investigations, there is a need to request evidence from online service providers based in another jurisdiction. The number of requests to Facebook, Google, Microsoft, Twitter and Apple grew by 70% between 2013 and 2016, from 35,300 requests to 60,200 requests.[8]

2.10 Countries have the ability to negotiate treaties with individual states to expedite or clarify aspects of the process. As at November 2019, Australia had 29 bilateral mutual assistance relationships in place.[9] However, the absence of a treaty does not prevent Australia submitting a Letter of Request through diplomatic channels.[10]

2.11 The Department of Home Affairs suggested that the mutual legal assistance process can no longer keep pace with technological advances:

> International crime cooperation mechanisms (such as mutual legal assistance) remain the principal means to obtain evidence, including electronic data, from foreign jurisdictions for use in criminal investigations and prosecutions. However, the digital world and the rapid increase in digital evidence for all types of criminal offences – not just cyber offences – is fundamentally undermining international crime cooperation. The traditional mechanism of mutual legal assistance has proven to be a slow and cumbersome way of

---

7 Commonwealth Director of Public Prosecutions (CDPP), *Submission 22*, p. 4.

8 Synod of Victoria and Tasmania, Uniting Church, *Submission 24*, p. 2.

9 Attorney-General's Department, *Australia's bilateral mutual assistance relationships*, November 2019, available at <https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/Documents/bilateral-treaties-on-mutual-assistance-in-criminal-matters.pdf>

10 Australia is a party to the *Convention on the taking of evidence abroad in civil or commercial matters*, opened for signature 18 March 1970, 23 UST 255 (entered into force 7 October 1972) which enables the operation of this process.

> working, not responding sufficiently to this fundamental shift in the offshore storage of Australians' data.[11]

2.12 Microsoft also considered the Mutual Legal Assistance Treaty (MLAT) provisions are no longer fit for purpose:

> Microsoft has long recognised that the traditional Mutual Legal Assistance Treaty (MLAT) processes for enabling governments' access to data held in foreign jurisdictions is no longer fit for purpose and hinder the ability of law enforcement to effectively investigate crimes and ensure public safety. This is a valid frustration shared by many nations, including Australia.[12]

2.13 The CDPP indicated that some MARs can take between 10–12 months[13] and the Committee received evidence that in some cases the timeframe can be significantly longer[14] – for example, the AFP said that it took nearly four and a half years to receive formally sealed MAR material in a child exploitation case.[15]

2.14 The NSW Police provided that the timeframe for response to a MAR prevented a full range of charges being brought against an offender using Facebook to threaten to kill and intimidate a victim, as provided in the following case study.

---

11 Department of Home Affairs, *Submission 10*, p. 3.

12 Microsoft, *Submission 29*, p. [1].

13 CDPP, *Submission 22*, p. 3.

14 See Australian Commission for Law Enforcement Integrity, *Submission 2*, p. 3; New South Wales Police Force (NSW Police), *Supplementary Submission 12.1*; Department of Home Affairs, *Submission 10*, p. 3.

15 AFP, *Submission 31*, p. 6.

Box 2.1 NSW Police Case Study – Use of carriage service to threaten to kill – withdrawal of prosecution on 16 counts

Between 2013 and 2015, the alleged offender used the on-line social media platform Facebook to threaten to kill and intimidate a victim. The offender created multiple Facebook accounts in false names and sent the victim threats and pictures of the victim's deceased relatives. The offender also created a Facebook account in the victim's own name and sent themselves harassing messages purporting to be the victim. The offender applied for an Apprehended Violence Order (AVO) against the victim, causing the victim considerable expense and hardship. The offender also used Facebook to invite persons to the victim's residence for sexual activity.

Facebook provided Internet Protocol (IP) address details that investigators used to identify the offender by linking Facebook accounts to his computer. However, the addresses were provided as 'Intelligence only' and did not provide a statement/evidentiary certificate for production at court.

The accused was charged with 22 offences in 2015. The IP logs provided by Facebook linking the offender to the accounts could not be produced in the court proceedings. Investigators submitted an MLAT request for all accounts created by the offender in 2015 and to Google to link the email address used in the creation of the accounts to the offender. The prosecution sought an estimated completion date for the request. A completion date could not be provided.

The MLAT request was ultimately complied with in 2019. As a result of the delay, 16 charges were dropped. The offender was convicted of six out of the 22 offences.[16]

2.15 Similarly, the AFP has provided several case studies showing that delays in the MAR process can result in the continuation of criminal activity, affecting additional victims and prolonging trauma.[17]

2.16 The difficulty of the mutual legal assistance process in enabling evidence gathering in the USA led to the passage of the USA's CLOUD Act.[18]

16 NSW Police, *Supplementary Submission 12.1*, p. 1.

17 AFP, *Submission 31*, pp. 6–10.

Enabling provisions of the CLOUD Act

2.17 The catalyst for the introduction of the CLOUD Act was a 2013 civil court case where Microsoft challenged a US warrant for data held on an overseas server:

> … the CLOUD Act resolved a case that Microsoft brought in 2013 and ended at the US Supreme Court—the Microsoft Ireland case—in which we challenged a US government warrant for data held in our Irish data centre. We didn't bring our case out of a desire to frustrate law enforcement; we brought that case to derive the systemic changes necessary to advance public safety and security while at the same time ensuring adequate protections for privacy, human rights and digital sovereignty.[19]

2.18 Prior to the introduction of the CLOUD Act, a warrant was issued under the US *Stored Communications Act* which could be served on a telecommunications organisation under USA jurisdiction.[20]

2.19 However, the CLOUD Act dictates that warrants issued to a provider in the US under the *Stored Communications Act* apply regardless of where the data is held. The CLOUD Act also enables the US government to enter into bilateral agreements with foreign countries. The International Civil Liberties and Technology Coalition summarised the provisions as follows:

> The first part of the CLOUD Act now clarifies that US government requests under the Stored Communications Act of companies that are under US jurisdiction apply, regardless of whether the data is located within or outside of the United States. The second part of the US CLOUD Act is directly relevant to the international production orders bill. It sets up a process through which countries like Australia can enter into a bilateral agreement with the United States that will enable each country to bypass the time-consuming traditional mutual legal assistance treaty, or MLAT, process for gaining access to electronic communications information. This will allow law enforcement

---

18 US Department of Justice, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, April 2019, available at <https://www.justice.gov/opa/press-release/file/1153446/download>, p. 3.

19 Mr Norman Barbosa, Assistant General Counsel, Law Enforcement and National Security, Microsoft Australia, *Committee Hansard*, Canberra (evidence taken via teleconference), 13 May 2020, p. 1.

20 Ms Sharon Bradford Franklin, International Civil Liberties and Technology Coalition, *Committee Hansard,* Canberra (evidence taken via teleconference), 13 May 2020, p. 11.

> officials in each country to make direct requests to be considered in the other country in order to obtain communications information like emails.[21]

2.20 The Department of Home Affairs has indicated that Australia is seeking to enter into a bilateral agreement with the US.

> Australia is likely to be the next qualifying foreign government to enter into an agreement with the United States (after the United Kingdom, who finalised an agreement with the United States in October 2019). On 7 October 2019, Australia and the United States announced the commencement of formal negotiations for a bilateral agreement pursuant to the CLOUD Act.[22]

2.21 The authorisation process and its compatibility with the requirements of the CLOUD Act are discussed further in Chapter 3.

Incoming international production orders

2.22 The Bill makes general provisions for incoming orders and requests.[23] The incoming international production orders (IPO) clauses operate to remove barriers to Australian communications providers cooperating with requests:

> The removal of blocking provisions is reasonable and necessary in the circumstances, as it ensures Australian communications service providers are not be prevented from responding to requests for communications data by foreign governments with which Australia has a designated international agreement, and which are expected to operate under the principle of reciprocity. These measures are permissive in nature, and place no obligations under Australian law on Australian communications service providers to provide data in response to an incoming request.[24]

2.23 The Department of Home Affairs said that a successful cross-border access to data agreement requires blocking statutes to be lifted:

---

21 Ms Sharon Bradford Franklin, International Civil Liberties and Technology Coalition, *Committee Hansard*, Canberra (evidence taken via teleconference), 13 May 2020, p. 11.

22 Department of Home Affairs, *Submission 10*, p. 5.

23 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 167–169.

24 Explanatory Memorandum, p. [13].

> Cross-border access to data agreements are expected to be reciprocal and to require that Australia remove blocking statutes to ensure that Australian industry can disclose electronic data to a foreign authority.[25]

2.24 The substance of conditions relating to the treatment of incoming IPOs are expected to be covered in designated international agreements, rather than in the proposed Act itself.

Designated international agreements

2.25 The Bill provides for a bilateral or multilateral designated international agreement (DIA) to be made between Australia and a foreign country.[26]

2.26 The Explanatory Memorandum defines the intent of clause 3 of the Bill for designated international agreements to be specified in the regulations and subject to disallowance:

> Subclause 3(1) provides, for a bilateral agreement to be a designated international agreement, it must be an agreement that is between Australia and a foreign country, that is specified in the regulations and has come into force. Any regulations made under subclause 3(1) will be legislative instruments and subject to disallowance.[27]

2.27 The Inspector-General of Intelligence and Security (IGIS) suggested the Bill may not provide sufficient certainty that DIAs will be tabled in Parliament and published publicly:

> IGIS assumes that subclause 3(7) of proposed Schedule 1 will mean that any designated international agreement that is entered into for the purposes of the IPO framework will be tabled in the Parliament and made public. However, the Committee may wish to seek assurances that this will be the case, as this provision could be interpreted differently. IGIS would be concerned to be in a position where agencies are held accountable to standards that have not been made public. This would be likely to affect IGIS's statutory responsibility to assure the Parliament and the public that intelligence and security matters are open to scrutiny.[28]

---

25 Department of Home Affairs, *Submission 10*, p. 9.

26 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, sch. 1, cl. 3(1) and 3(3).

27 Explanatory Memorandum, p. [29].

28 Inspector-General of Intelligence and Security (IGIS), *Submission 27*, p. 16. See also Communications Alliance, *Submission 14*, p. 3.

2.28 In response, the Department of Home Affairs said that designated international agreements would be made available through parliamentary processes and by publication in treaties databases:

> … designated international agreements, including any amendments to these agreements, would be made publically available through the usual parliamentary processes and publication in treaty databases. It is normal practice that bilateral treaties are confidential between the parties until the treaty has been signed, unless both parties agree to earlier disclosure. After signing, all treaties must be tabled in Parliament to facilitate public consultation and parliamentary scrutiny.
>
> Under Article 102 of the Charter of the UN, any Treaty that comes into force must be registered with and published by the UN. Additionally, the designated international agreements as treaties will also be published in the Australian Treaties Database and Australian Treaties Library.[29]

2.29 The Australian National University Law Reform and Social Justice (ANU LRSJ) Research Hub also suggested that the Committee and the Office of the Australian Information Commissioner should scrutinise proposed DIAs in addition to the Parliamentary Joint Standing Committee on Treaties (JSCOT) against several criteria:

> In addition to review by the Parliamentary Joint Standing Committee on Treaties (PJSCT), we recommend that any entry into a designated international agreement is carefully scrutinised and assessed by the PJCIS and the Office of the Australian Information Commissioner (OAIC) and that such reviews consider (among other things):
>
> - The domestic privacy protections available in the other jurisdiction, and whether they are equivalent to the protections afforded under Australian law;
> - Whether the agreement allows for requests or orders to be issued in circumstances that afford lower protections than those under the current Australian framework;
> - The circumstances under which Australian companies would be required to comply with the order and whether there is appropriate scope for Australian companies not to comply if they fear the information may be used to harm an individual or in a manner not commensurate to the security value of the information;

[29] Department of Home Affairs, *Supplementary Submission 10.2*, p. 15.

- The likely use of information by the foreign jurisdiction, especially whether surveillance measures have been deployed to prevent dissidents from raising valid concerns with the government;
- The adherence of the foreign jurisdiction to the rule of law and whether appropriate oversight mechanisms are in place;
- Whether the agreement provides for domestic reporting of requests made and granted similar to the reporting required under the IPO framework.[30]

2.30 The Bill provides that where there is an agreement in place between Australia and one or more foreign countries, the regulations will continue to recognise the DIA as an agreement when amended.[31] The Law Council said that this provision would displace the provisions of the *Legislation Act 2003* that ensures that other legislative instruments include the conditions in force at the time the regulation was made:

> 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.[32]

2.31 The Department of Home Affairs responded that it is the intention that 'all amendments to designated international agreements will be subject to Australia's treaty-making requirements, including tabling in Parliament and consideration by the Joint Standing Committee on Treaties'[33] and that amendment of the clause could cause uncertainty about the status of IPOs:

> If the reference to agreements as 'amended and in force from time to time' in clause 182 were removed, this would mean an agreement would need to be specified as a new agreement in the regulations each time it is amended, extended or renewed for a further period.

---

30 Australian National University Law Reform and Social Justice Research Hub, *Submission 17*, p. 7.

31 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1, cl. 182.

32 Law Council of Australia, *Submission 28*, p. 16.

33 Department of Home Affairs, *Supplementary Submission 10.2*, p. 23.

> This could lead to uncertainty about the status and/or operation of international production orders that have already been issued or are in force when a new agreement is entered into and comes into force.[34]

2.32 While the Bill would allow for Australia to negotiate DIAs with foreign governments for reciprocal arrangements, the Department of Home Affairs said that the main priority is the negotiation of an agreement with the US:

> There's no priority list at this stage. The US is the No. 1 priority, for obvious reasons, as it is the data storer for a large part of the world when you're talking about Facebook, Google, Apple and others. It is a real priority. It's what Australians are using in their day-to-day communications. They happen to all be in the US, so this is the No. 1 priority.
>
> After that, once we're able to get that agreement in place, we would consider what other ones might be a priority. The reasons for those priorities could include what other countries have significant data holdings in relation to Australian communications, or what other countries have like-minded processes whereby we could make an agreement. But that is not in consultation at the moment. It's the US that we are absolutely focused on for the first bilateral agreement.[35]

2.33 Submitters have suggested that a draft of the DIA should be made available prior to finalising it.[36] However, the Department of Home Affairs has indicated that releasing a draft version is not their intention, and that concerned parties should look to the agreement between the US and the United Kingdom (UK) for broad guidance on expected inclusions in the agreement – discussed further below.[37]

2.34 Once the terms of a designated international agreement has been agreed by representatives of both State parties, the instrument is tabled, subjected to scrutiny processes and subjected to a period of disallowance. In Australia, the standard timeframe for disallowance is 15 sitting days; however, the US Congress has a period of 180 days to disallow the instrument[38]

---

34 Department of Home Affairs, *Supplementary Submission 10.2*, p. 24.

35 Mr Andrew Warnes, Assistant Secretary, National Security Policy Branch, Department of Home Affairs, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 21.

36 See International Civil Liberties and Technology Coalition, *Submission 9*, p. 1; Microsoft, *Submission 29*, p. [4].

37 Mr Warnes, Department of Home Affairs, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 22.

38 Law Council of Australia, *Submission 28*, p. 13.

International comparisons

2.35 As the only country that has finalised negotiations with the US on a CLOUD Act agreement,[39] the agreement between the US and the UK signed on 3 October 2019 is a reference to compare to the provisions of the Bill.

2.36 The agreement provides that subject to judicial review or oversight, the US or the UK may approach a provider to seek stored or live communications through each party's Designated Authority.[40] An issuing country may approach a receiving country's communications provider directly for subscriber information without submitting through the relevant Designated Authority.[41]

2.37 The issue of such orders are restricted, in broad terms, to those who are not citizens, residents, or organisations of the country receiving the request.[42]

2.38 The agreement expressly provides that the issuing country's Designated Authority shall review the orders to ensure compliance with the agreement and provide a written certification that the order is lawful and complies with the agreement. A provider in receipt of an order may raise objections with the issuing Designated Authority in the first instance, and the issuing Designated Authority must respond.[43]

2.39 Where an agreement cannot be reached, the agreement states that a communications provider may approach the Designated Authority of the receiving country. Upon consideration, the receiving country's Designated Authority may determine that the agreement does not apply to the order.[44]

---

39 Department of Home Affairs, *Submission 10*, p. 5.

40 *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* ('Data Sharing Bilateral Agreement'), United Kingdom-United States of America, signed 3 October 2019, art. 5.

41 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 10.

42 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 1.

43 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 5.

44 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 5.

2.40 The agreement states that an issuing country must seek permission from the receiving country's Designated Authority if an order would seek information in a way that could be used in the prosecution of a death penalty case – as in the US – or in a way that would infringe upon freedom of speech – as in the UK. A receiving country may impose restrictions on how the information can be used, or may decline the information being used entirely.[45]

2.41 The agreement provides that parties shall engage in a review of compliance with the terms of the agreement, and that each party shall provide an annual report detailing aggregated data concerning the use of the provisions of the agreement.[46]

2.42 Finally, the agreement is in force for a five year period, but may be extended for an additional five year period through an exchange of diplomatic notes – or any other period as agreed.[47]

2.43 Following the required period of notice, the agreement came into effect on 8 July 2020.[48]

Committee comment

2.44 The Committee notes the evidence received from submitters in relation to the challenges posed by the mutual legal assistance process, and that the regulatory requirements of MARs create inefficiency for the investigation and prosecution of serious offences.

2.45 The Committee thanks the Australian Commission for Law Enforcement Integrity, the Corruption and Crime Commission (WA), the Australian Federal Police and NSW Police for providing case studies to enhance its understanding of the operational consequences of delays with the mutual legal assistance process.

2.46 On its face, the CLOUD Act will provide opportunities to streamline requests for information, and the Committee supports this intent, and

---

45 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 8.

46 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 12.

47 Data Sharing Bilateral Agreement, United Kingdom-United States of America, signed 3 October 2019, art. 17.

48 Law Council of Australia, *Submission 28*, p. 9.

Australia's desire to negotiate a designated international agreement with the USA in the first instance.

2.47 The Committee notes that the provisions of the Bill are designed to be non-prescriptive to allow for details to be decided between parties in consideration of the laws of the country with which Australia is seeking to make a designated international agreement.

2.48 While the Committee generally supports this principle, the Committee supports the concerns raised by the Law Council of Australia and the Inspector-General of Intelligence and Security that certain core aspects related to designated international agreements are not sufficiently explicit.

2.49 The Committee welcomes the advice of the Department of Home Affairs that the Parliamentary Joint Standing Committee on Treaties will have the opportunity to scrutinise proposed designated international agreements as part of the treaty-making process.

2.50 The Committee also welcomes the advice of the Department of Home Affairs that it will adhere to the practice of advising foreign countries that Australia has taken all appropriate steps to enter the agreement into force only after the period of disallowance has expired.

2.51 The Committee considers that while a designated international agreement should come into force at the expiry of the disallowance period provided by the *Legislation Act 2003* (i.e. 15 sitting days) the bill should be amended to allow for the statutory disallowance period to align with foreign country Australia is seeking to make an agreement with.

2.52 The Committee recommends that the bill be amended to provide that a designated international agreement must be published and tabled in the regulations, subject to parliamentary scrutiny and subject to a period of disallowance. The Committee also recommends that the bill be amended to provide that the statutory disallowance period should reflect the longer of the standard 15 sitting days disallowance period, or the disallowance period that applies in the foreign country.

Recommendation 2

2.53 The Committee recommends that a new subclause be added to the proposed Clause 182 of Schedule 1 to the Telecommunications (Interception and Access) Act 1979 to provide that designated international agreements must be published and tabled in the regulations, subject to parliamentary scrutiny, and subject to a period of disallowance.

For the commencement of the regulations, proposed Schedule 1 should be amended to provide that regulations made under clause 3 (i.e. listing an agreement as a designated international agreement) cannot commence until no earlier than the expiry of the standard period for disallowance (i.e. 15 sitting days) under the Legislation Act 2003, or until the commencement of the other party's agreement, whichever is the longer.

For the period for disallowance, the bill should be amended to provide that the statutory disallowance period for regulations made under proposed clause 3 of Schedule 1 is the longer of:

- **the standard period for disallowance under the Legislation Act 2003; or**
- **the period for disallowance that applies in the parliament of the foreign country (i.e. the other party to the relevant international agreement).**

2.54 The Committee notes that the Department of Home Affairs suggested that amendments to designated international agreements would be made publicly available through parliamentary processes and published in treaties databases.

2.55 The Committee also notes the advice of the Department that uncertainty regarding the authority of designated international agreements could have an adverse impact on the outcome of IPO processes.

2.56 The agreement between the USA and the UK allows for the agreement to be extended for an additional period following the initial term. The Committee notes that there is a potential benefit to being able to extend an agreement with a foreign government without amendment when the agreement is working effectively.

2.57 However, the Committee also considers that periodic scrutiny of agreements will provide Australians with assurance that the provisions of the agreement

are being used effectively and appropriately. Therefore, the Committee recommends that a designated international agreement should be authorised to be extended for a period of three years following commencement, but that a parliamentary scrutiny process should apply a further extension. For the avoidance of doubt, the Committee also recommends that where an amendment is made, the amended designated international agreement should be specified as a new agreement and subject to appropriate parliamentary processes.

Recommendation 3

2.58 The Committee recommends that an additional subclause be added to the proposed Clause 182 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that a designated international agreement may be renewed or extended for a period of three years without completing the parliamentary treaty process, if such a renewal or extension is proposed without amendment to the agreement.

However, the Committee recommends that the clause also provide that, following the term of the initial agreement and any additional three year period, any further renewal or extension should be subject to parliamentary scrutiny and disallowance even where no amendment is proposed.

Finally, the same clause should also be amended to provide that, whenever an amendment to a designated international agreement is made or proposed, the amended agreement must be specified as a new agreement in the regulations and thus subject to the usual parliamentary treaty process and be subject to disallowance.

2.59 The Committee notes that the agreement between the United States and the United Kingdom provides protections for issue of orders against its citizens and addresses specific human rights issues impinging on sharing of information, and that the Bill is intended to be a framework to allow for negotiation.

2.60 However, the CLOUD Act also requires several conditions to be contained in an executive agreement, which includes matters addressed by the Bill, such as appropriate external authorisation, robust oversight, consideration of human rights matters, prevention of third-party requests and ensuring that requests relate to the prevention, detection, investigation or prosecution of serious crime, including terrorism.

2.61 Where a designated international agreement permits a foreign country to issue orders or requests directly to Australian communications provisions, the Committee considers that it would be appropriate for the designated international agreement to contain minimum requirements for orders, including that:

- it be appropriately targeted towards specific accounts, persons, other specific identifiers (clearly excluding indiscriminate or bulk data collection);
- subject to a specified period of time and subject to reauthorisation if required; and
- issued pursuant to domestic legal criteria designed to ensure they are reasonable, proportionate and necessary or other equivalent thresholds. This requirement would not require the same Australian particularly exacting standard (e.g. reasonable grounds of criminal suspicion), but achieve similar objectives (e.g. probable cause in the United States).

2.62 The Committee considers that it would be appropriate for a country seeking a designated international agreement to have sufficient safeguards in place to detail how Australian-sourced information would be handled, used and disclosed. In the Committee's view, this requirement should allow for a foreign country with a designated international agreement to seek permission to share information on a case-by-case basis or through a standing permission – for instance, allowing consideration of legitimate information sharing with INTERPOL, EUROPOL, war tribunals or the International Criminal Court.

2.63 The Committee considers that there is an opportunity for the Bill to be more prescriptive in relation to incoming international production orders on issues that will not preclude the successful negotiation of agreements with like-minded countries on issues such as protection of information, respect of law, and proportionality, and recommends that the Bill be amended to explicitly outline these principles.

Recommendation 4

2.64 The Committee recommends that a new subclause be included in proposed Clause 3 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that – in order to qualify as a designated international agreement – the agreement must:

- **prohibit the foreign government from intentionally targeting an Australian citizen or permanent resident; or**
- **prohibit the foreign government from intentionally targeting a non-Australian person located outside of Australia if the purpose is to obtain information about an Australian citizen or permanent resident;**
- **in relation to production orders for the interception of communications, require that the interception activities of the foreign government only be carried out for the purpose of obtaining information about communications of an individual who is outside of Australia;**
- **provide that all production orders must comply with the minimum requirements for foreign orders specified in paragraph 2.61;**
- **include safeguards for the use, handling and disclosure of information, as set out in paragraph 2.62;**
- **provide that all production orders must comply with the domestic law of the relevant foreign country;**
- **provide that production orders must not last longer than is reasonably necessary to accomplish the approved purposes of the order;**
- **provide that no production order may relate to the prevention, detection, investigation or prosecution of a political offence or an offence that is not recognised in the ordinary criminal law of Australia; and**
- **provide that a production order may only be issued if the same information could not reasonably be obtained by another less intrusive method.**

2.65 In addition, the Committee considers that a provision should be inserted to prevent a foreign government from seeking information on behalf of a third-party government. However, the Committee also notes that there may be some benefit in allowing cooperation with international bodies when mutually beneficial – see paragraph 2.62 – and the Committee therefore recommends that such a prohibition not preclude a country with a designated international agreement from seeking authority to share Australian-sourced information as set out in Recommendation 4.

Recommendation 5

2.66 The Committee recommends a subclause be included in proposed Clause 3 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that a designated international agreement shall not permit a foreign government to:

- **issue an order at the request of or to obtain information to provide to the Australian government or a third-party government, nor shall the foreign government be required to share any information produced with the Australian government or a third-party government.**

- **such a prohibition will not preclude a foreign government seeking authorisation to share information as set out by Recommendation 4.**

2.67 Noting that the intention of the Bill is to allow for information to be sought in relation to serious offences and issues related to terrorism and Australia's national security, the Committee considers that it would be appropriate to articulate this purpose in the Bill.

Recommendation 6

2.68 The Committee recommends a subclause be included in proposed Clause 3 of Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* to provide that incoming international production orders under a designated international agreement must only be issued for the purpose of obtaining information relating to the prevention, detection, investigation or prosecution of serious crime, including terrorism.

2.69 The Committee notes that if its recommendations are accepted, it would be appropriate for the Attorney-General, with the concurrence of the Minister for Home Affairs to provide assurance that the conditions for a designated

international agreement have been met – such as those set out at Recommendation 4 and Recommendation 8 of this report. The Committee therefore recommends that the Bill be amended to require the Attorney-General with the concurrence of the Minister for Home Affairs to submit a written certification, including a detailed explanation, where it has determined the agreement has met the statutory requirements.

Recommendation 7

2.70 The Committee recommends that proposed Clause 182 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to provide that, for the purposes of the Act, an agreement – and a foreign government – will be considered to satisfy the statutory requirements (including the requirements set out in Recommendation 4 and Recommendation 8 of this report) if the Attorney-General, with the concurrence of the Minister for Home Affairs:

- **determines that the agreement and the foreign government satisfy the statutory requirement; and**
- **submits a written certification, including a detailed explanation, of such a determination to the Joint Standing Committee on Treaties. That certification should be provided at the same time that the regulations are tabled.**

Human rights obligations

2.71 Australia is a party to the *International Covenant on Civil and Political Rights* (ICCPR) which provides for the right to life (art. 6), the protection against arbitrary or unlawful interference with privacy (art. 17), and the protection of the right to freedom of expression (art. 19) and these matters are engaged by the provisions of the Bill.[49]

2.72 Several submitters to the inquiry commented that a precondition to entering into a bilateral agreement with the US is the adherence to applicable international human rights obligations.[50] The Attorney-General's

---

49 Explanatory Memorandum, p. [5].

50 See Synod of Victoria and Tasmania, Uniting Church, *Submission 24*, p. 4; Mr Eric Wilson, *Submission 7*, p. 1; Mr Thomas McBride, *Submission 19*, pp. [8]–[9]; International Civil Liberties and Technology Coalition, *Submission 9*, p. 2; The Allen's Hub for Technology, Law and Innovation, *Submission 15*, p. 3.

Department said that matters concerning incompatibility under international law will be considered as part of the parliamentary scrutiny process:

> There are various safeguards in section 8 of the [*Mutual Assistance in Criminal Matters Act 1987*] relating to the Attorney-General's grounds of refusal of assistance. For example, there are mandatory and/or discretionary protections relating to the death penalty, torture, military offences, political offences, dual criminality, double jeopardy, national security and national or State/Territory interests. AGD understands that the inclusion of appropriate safeguards in a DIA that Australia seeks to implement under the Bill framework will be negotiated on a case-by-case basis with the particular country or countries and subject to Parliamentary scrutiny. That is, before Australia's ability to issue IPOs pursuant to a DIA is given effect in Australian domestic law by way of regulations under the Bill, those agreements must be laid before Parliament and are subject to scrutiny by the Joint Standing Committee on Treaties, parliament and the public.[51]

2.73 However, in its submission to the inquiry the Law Council of Australia considers that the Bill has inadequate human rights protections:

> It seems to us that there are no legal safeguards in the bill that would prohibit Australia from giving domestic legal effect to an agreement that could be used to disclose information that could in turn be used to inculpate a person in foreign death penalty proceedings; to prosecute a child as an adult; to prosecute a person for a political offence that, in substance, targets peaceful dissent, advocacy or discussion; to violate rights to freedom of expression, such as targeting a journalist's source or telling a journalist to disclose their sources; and to prejudice a person's right to a fair hearing by targeting and using information that's subject to client legal privilege.[52]

The right to life

2.74 The Bill does not refer to human rights obligations aside from the right to life, where the Minister must seek written assurance about the use or non-use of Australian-sourced information in the prosecution of a case that could attract the death penalty.[53]

---

51 Attorney-General's Department, *Submission 16*, p. 11.

52 Dr Sarah Pritchard SC, Chair, National Human Rights Committee, Law Council of Australia, *Committee Hansard*, Canberra (evidence taken via teleconference), 12 May 2020, p. 11.

53 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 3.

2.75 The Capital Punishment Justice Project suggested that the wording of Clause 3 provides ambiguity in how Australian-sourced information could be used in death penalty cases in the US:

> Clause 3 of proposed Schedule 1 does not, for example, impose an obligation on the Minister to obtain in writing an absolute assurance from the foreign government in question that information provided from Australian sources will not, in any circumstances, be used in death penalty proceedings, or in investigations of crimes that may attract the death penalty in their jurisdiction. There is also no requirement that the Australian sourced information in such instances will only be used for exculpatory purposes. As such, these proposed provisions are in practice capable of permitting actions which are incompatible with Australia's stated foreign policy position, of being against the death penalty in all circumstances.[54]

2.76 The Law Council of Australia echoed the concerns of the Capital Punishment Justice Project, and noted that the intention of the relevant clause outlined in the Explanatory Memorandum does not accord with the proposed statutory provision:

> 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.[55]

2.77 The Attorney-General's Department said that the relevant intent of the clause is to prevent the Minister from specifying a DIA without written assurance restricting or excluding information from death penalty cases:

> … the Bill provides that the Minister cannot specify a DIA without a written assurance from the relevant partner country regarding restricting or excluding the use of Australian-sourced information in a proceeding relating to a foreign offence that is punishable by death.[56]

2.78 In addition, the Attorney-General's Department said that seeking assurances as part of the treaty negotiating process can take a variety of forms:

---

54 Capital Punishment Justice Project, *Submission 30*, p. 2.

55 Law Council of Australia, *Submission 28*, p. 19.

56 Attorney-General's Department, *Submission 16*, p. 10.

> The Australian Government has previously received written assurances regarding the death penalty in a range of forms. For example, a written assurance may be contained in a single document, or across a number of documents, such as the text of the agreement, a letter or exchange of letters, or a record of understanding or memorandum of understanding. The written assurances may deal with how Australian-sourced information may be used by the foreign country in proceedings in connection with prosecutions for death penalty offences, including for exculpatory purposes, and subject to any restrictions or conditions. They may also specify that Australian-sourced information is not to be used in prosecutions of offences that attract the death penalty. This approach to death penalty risks is broadly comparable with Australia's existing MLA arrangements concerning the death penalty at the prosecution stage.[57]

2.79 Mr Andrew Warnes, Assistant Secretary, National Security Policy Branch, Department of Home Affairs said that protections surrounding right to life will be at the centre of negotiations for designated international agreements:

> Further, I would like to note a core protection in the bill concerning the death penalty. The bill provides that a country that has the death penalty must provide a written assurance about the use of information obtained from Australian service providers in death penalty prosecutions before an agreement can be designated. This will ensure that the death penalty is of paramount consideration from the outset in negotiating and settling international agreements and that Australia's longstanding opposition to the death penalty can be reflected. The use of assurances to protect Australia's death penalty interests is a longstanding practice in related mutual assistance regimes.
>
> The framework set out in the bill will be supplemented by additional safeguards and protections within designated international agreements. Agreements will set requirements for foreign countries that reflect Australian values such as respect, the rule of law, privacy and civil liberties.[58]

Protection against arbitrary or unlawful interference with privacy

2.80 The ICCPR provides that 'no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to

---

57 Attorney-General's Department, *Submission 16*, p. 10.

58 Mr Warnes, Department of Home Affairs, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 16.

unlawful attacks on his or her honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks.'[59]

2.81 The Attorney General's Department said that not all interferences with privacy are unlawful under international human rights law:

> Not all interferences with privacy are unlawful. To be permissible as a matter of international human rights law, interferences with privacy must be according to the law and not arbitrary. In order not to be arbitrary, any such interference must be reasonable and necessary in the particular circumstances, as well as proportionate to the objectives it seeks to achieve.[60]

2.82 The Explanatory Memorandum states that the provisions of the Bill necessarily intrude on individual privacy for a permitted purpose:

> The purpose of the Bill, and the associated limitations on the protection against arbitrary or unlawful interference with privacy, are to protect national security, public safety, and address crime and terrorism. The Bill aims to protect the rights and freedoms of individuals by providing law enforcement and national security agencies with the tools they need to keep Australians safe.[61]

2.83 The Bill proposes a number of measures designed to ensure that an individual's privacy is weighed against the overarching obligation to ensure the overall safety of Australians. There are specific measures included as part of the authorisation process that are discussed in Chapter 3. However, several submitters raised concerns about the implications of the Bill on privacy outside of the authorisation process.

2.84 The Australian Privacy Foundation said that the Bill is 'a manifestation of a drip by drip erosion of privacy protection in the absence of a justiciable constitutionally-enshrined right to privacy in accord with international human rights frameworks'[62] and further that:

> … the Bill seeks to enable "the exemption from Commonwealth laws restricting interception or disclosure" on the basis of a designated international agreement: a low threshold at odds with the Minister's reference to "robust privacy and civil liberty protections".

---

59 Explanatory Memorandum, p. [6].

60 Attorney-General's Department, *Submission 16*, p. 11.

61 Explanatory Memorandum, p. [7].

62 Australian Privacy Foundation, *Submission 1*, p. [1].

> That threshold should be contextualised through reference to ongoing 'privacy creep' (ie drip by drip year by year erosion of privacy protection) and the regulatory incapacity of watchdogs such as the Commonwealth Ombudsman and Office of the Australian Information Commissioner.[63]

2.85 The ANU LSRJ Research Hub said that access to digital surveillance by law enforcement agencies has increased through relatively recent passage of laws:

> In Australia, powers of law enforcement agencies have increased through the passage of laws, granting:
>
> - Access to metadata, that must be held by telecommunications providers for two years;
> - Extended warrant schemes under the TIA Act and the Crimes Act allowing for greater access to information stored digitally (see especially s. 3F Crimes Act); and
> - Greater powers to compel assistance from technology companies (in regard to accessing information) through the use of TARs, TANs and TCNs under the TIA Act, following amendments made at the end of 2018.[64]

2.86 The increase in global connectivity provides an ongoing exercise in balance between individual privacy and the investigation or prosecution of serious crimes and national security. The Explanatory Memorandum discusses serious crimes and their online elements:

> Almost every crime type and national security concern has an online element— agencies require electronic information and communications data not only for cyber investigations but also for investigations and prosecutions regarding violent crimes, human trafficking and people smuggling, drug trafficking, financial crimes, terrorism and child sexual abuse.[65]

2.87 In its case study below, the AFP said that delays in the outcome of investigations puts a victim at risk of continued offending, and creates potential new victims.[66]

---

63 Australian Privacy Foundation, *Submission 1*, p. [4].

64 Australian National University Law Reform and Social Justice Research Hub, *Submission 17*, p. 2.

65 Explanatory Memorandum, p. [2].

66 See generally Synod of Victoria and Tasmania, Uniting Church, *Submission 24*.

Box 2.2 AFP Case Study – Child exploitation investigation – delays on behalf of overseas jurisdiction

Investigation Summary

The AFP was investigating an individual who was blackmailing a juvenile to produce child abuse material (CAM). The AFP identified content held by a carriage service provider located in a foreign country, which was crucial to prove elements of the offence. Accordingly, the AFP initiated an MAR with the Australian Central Authority.

MAR Challenges

In this case, there were significant delays with the foreign Central Authority progressing the MAR and seeking the material from the provider.

The AFP received the material 9 months after initiating the MAR process. In the meantime, the offender continued to produce CAM and was distributing it to contacts, resulting in ongoing offending and harm to the victim.

The material obtained via MAR was fundamental for investigators to be able to link the offender to the production of the CAM.

As a consequence of this delay over a 9 month period, the offender was also able to actively use another online forum, potentially to groom further victims.

Alternative Impact if an IPO was available

An IPO would have allowed the request to be quickly directed to the relevant foreign provider, who would then be in a position to provide the content or data directly back to Australian authorities, likely within much shorter timeframes.

Any reduction in timeframes in this matter would have significantly hindered the offender in being able to continue using forums to identify and target other victims, while reducing the overall length of the investigation (including reducing strain on AFP resources) and initiation of a more timely justice process.[67]

[67] AFP, *Submission 31*, p. 7.

2.88 The Explanatory Memorandum says that 'it is expected that consideration of protections and safeguards related to privacy will also be a consideration when developing international agreements'[68] and this principle is also stated in submissions by the Department of Home Affairs[69] and the Attorney-General's Department.[70]

2.89 The Independent National Security Legislation Monitor (INSLM) recently outlined the importance of independence, and the appearance of independence, in the inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act):

> This independence engenders the necessary trust in the minds of members of the public that the powers are being exercised in a manner that is no more than is necessary. A proper appreciation of the impact of an intrusive TOLA power depends upon the issuer being independent of the agency concerned and, importantly, having technical knowledge. The powers under TOLA cannot be exercised, let alone their impact understood, in the absence of independent technical expertise.[71]

2.90 The Law Council of Australia said that access to technical expertise – in addition to special advocates – to provide advice on the potential impacts of the use of technology on an individual's privacy, and how intrusive such technical measures are would be a useful tool to support independent decision-makers in supporting applications for IPOs.[72]

2.91 BSA | The Software Alliance said that IPO applications should be made in consultation with technological providers who are most qualified to provide weight to technical capabilities.[73]

2.92 The INSLM proposed the introduction of an investigatory powers division to be established within the Administrative Appeals Tribunal. The proposed division would have the ability to consider applications for access to intrusive telecommunications powers under the TOLA Act and appoint a

---

68 Explanatory Memorandum, p. [98].

69 See Department of Home Affairs, *Submission 10*, p. 4.

70 See Attorney-General's Department, *Submission 16*, p. 10.

71 Independent National Security Legislation Monitor, *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, 2020, pp. 36-37.

72 Law Council of Australia, *Submission 28*, p. 36.

73 BSA | The Software Alliance, *Submission 20*, p. 4.

panel of technical and legal advisers to the division in carrying out its functions.[74]

2.93 The INSLM said that such a mechanism would be valuable in the establishment of the IPO framework:

> The desirability of a decision-maker independent of the executive and its agencies is recognised in the Government's Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill), which is a critical step that enables Australia to seek a bilateral agreement with the US under their Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act). The IPO Bill would enable Australia to give effect to such a bilateral agreement by creating a new international production order framework that allows Australian law enforcement and intelligence/security agencies to issue or obtain extraterritorial orders for electronic data on foreign DCPs (where there is an agreement in place).[75]

2.94 The CLOUD Act provides additional protections for the privacy of its citizens, stating that an agreement requires:

> (A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;
>
> (B) the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;
>
> (C) the foreign government may not issue an order at the request of or to obtain information to provide to the United States Government or a third-party government, nor shall the foreign government be required to share any information produced with the United States Government or a third-party government…[76]

---

74 Independent National Security Legislation Monitor, *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters*, 2020, pp. 37–38.

75 Independent National Security Legislation Monitor, *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters*, 2020, p. 37.

76 CLOUD Act, 18 USC §2523(b)(3)

The protection of the right to freedom of expression

2.95 In 2015, the Committee's advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 ('Data Retention Bill') noted the importance of the principle of press freedom and the protection of journalists' sources[77] and subsequently conducted an additional inquiry into how to protect those principles under the data retention regime.[78]

2.96 While the second inquiry was underway the Bill was amended to include journalist information warrants, a process that ascribes a higher degree of consideration to applications by law enforcement or the Australian Security Intelligence Organisation (ASIO) when seeking access to the data of a journalist in order to identify their source.

2.97 In 2019, the Committee was asked to review the impact of national security legislation on the freedom of the press by the Attorney-General. The Committee tabled its report in August 2020 and made a series of recommendations to address the freedom of the press in Australia.

2.98 The IGIS said that journalist protections provided under domestic legislation were not replicated in the Bill:

> The Bill proposes to establish a new authority for agencies to be able to obtain the content of communications and telecommunications data of certain persons, in parallel with existing domestic regimes. However, some of safeguards that are afforded under Australia's existing domestic scheme for the same type of information do not appear in the Bill. For example, the domestic regime provides additional protections where ASIO or law enforcement agencies are seeking to access the telecommunications data of a journalist for the purpose of identifying another person whom is reasonably believed to be that journalist's source.[79]

2.99 In response, the Department of Home Affairs said that independent authorisation in addition to governance and accountability mechanisms would be sufficient to ensure protection of journalistic privilege:

---

77 Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014, February 2015, pp. 257–258.

78 Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the authorisation of access to telecommunications data to identify a journalist's source*, April 2015.

79 IGIS, *Submission 27*, p. 11.

The journalist information warrants under the TIA Act provide an additional layer of protection telecommunications data relating to journalists' sources. An independent authorisation by a decision-maker outside of the agency will issue the warrant, rather than the typical process of internal authorisation by agencies for telecommunications data.

However, our domestic interception and stored communications warrants do not include these particular carve-outs as they are already subject to independent authorisation. Exemptions may also raise issues associated with the application of investigatory powers on the basis of profession-based carve-outs and present challenges for agencies in investigating matters relating to crime or national security.

In addition to legislative safeguards, there will be governance and accountability mechanisms, such as ministerial directions under subsection 37(2) of the *Australian Federal Police Act 1979*. In August 2019, the Minister for Home Affairs issued a Ministerial Direction outlining the Government's expectations for the AFP in relation to investigative action involving a professional journalist or news media organisation in the context of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer.[80]

2.100 Mr Karl Kent, Deputy Commissioner of Specialist and Support Operations, said that the AFP would comply with its processes for IPOs related to journalists:

In terms of the AFP's response to that, we would still apply our processes that are put in place in relation to journalists internally in the organisation that reflect the legislative environment in Australia and our changed approach as a result of recent matters in order to strengthen our approach and where we also need to comply with a ministerial direction in relation to journalists and those processes.[81]

[80] Department of Home Affairs, *Supplementary submission 10.2*, pp. 11–12.

[81] Mr Karl Kent, Deputy Commissioner of Specialist and Support Operations, AFP, *Committee Hansard*, Canberra (evidence taken by teleconference), 14 May 2020, p. 14.

2.101 In addition, ASIO restated their concern with having provisions specifically designed for members of the community:

> I would say in relation to journalism or, indeed, any profession, that ASIO's point of view is that we have potential concerns if carve-outs are made in relation to a particular class of persons based purely on their profession.[82]

2.102 Mr Michael Fitzgerald, Assistant Commissioner and Commander, Forensic Evidence and Technical Services Command, said that NSW Police would expect to go before a public interest monitor for an application related to a journalist:

> What we do support is the current regime under the telecommunications interception act. It's a fairly strict regime and, if we ever did attempt to seek information in regard to a journalist, it would have to go before a public interest monitor. I would assume that it would be the same process that we'd find. I would certainly believe that if we ever did seek this information then it would come across my desk, and then I would seek fairly high-level legal advice and corporate advice in regard to proceeding.[83]

2.103 The Bill provides that for applications made in Victoria and Queensland in relation to interception of data, a Public Interest Monitor will assess the application against the same criteria as the designated decision-maker, in accordance with the statutory requirements of those jurisdictions. The decision-maker must then consider the assessment of the Public Interest Monitor in deciding whether to grant the order.[84] No such provision is made for stored communications data and telecommunications data.[85]

Committee comment

2.104 The Committee notes the concerns raised by submitters in relation to human rights considerations in the Bill. Given the Department of Home Affairs' advice that designated international agreements will be subject to scrutiny by the Joint Standing Committee on Treaties, the Committee is assured that

---

82 Mr Peter Vickery, Deputy Director-General, Enterprise Service Delivery, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 3.

83 Mr Michael Fitzgerald, Assistant Commissioner and Commander, Forensic Evidence and Technical Services Command, NSW Police Force, *Committee Hansard*, Canberra (evidence taken via teleconference), 13 May 2020, p. 23.

84 Explanatory Memorandum, p. [9].

85 Law Council of Australia, *Submission 28*, p. 35.

Australia's human rights obligations will be given appropriate weight when designated international agreements are considered.

2.105 In relation to submitters' concerns regarding the right to life, the Committee notes that the Bill requires written assurances from the Designated Authority of the country that has a designated international agreement with Australia regarding any potential use of information sourced from Australia in a death penalty proceeding – the practice that occurs under the current Mutual Legal Assistance Treaty process, which allows cooperation in death penalty cases with appropriate assurances. However, the Committee recommends that additional safeguards in relation to the death penalty and broader human rights considerations be included in the proposed Schedule 1 of the *Telecommunications (Interception and Access) Act* 1979 to articulate the appropriate thresholds that a country must meet to have a designated international agreement with Australia.

2.106 The Committee considers that requiring a country seeking a designated international agreement to demonstrate respect for the rule of law would provide that Australia may enter into cross-border access to data agreements to be designated under the international production order framework only with countries that that abide by the rule of law and provide equal treatment of an individual or group irrespective of particular characteristics.

2.107 The Committee also considers that requiring a country seeking a designated international agreement to demonstrate respect for international laws, and international human rights recognised as international laws where applicable, would provide assurance that human rights are given adequate weight in designated international agreements. This would include human rights recognised in international treaties, for example the ICCPR, such as:

- protection from arbitrary and unlawful interference with privacy;
- procedural fairness in law, in the form of rights of due process, and a fair and impartial trial;
- freedom of expression, association, and peaceful assembly;
- prohibitions on arbitrary arrest and detention; and
- prohibitions against torture and cruel, inhuman, or degrading treatment or punishment.

2.108 In addition, the Committee considers that it would be appropriate to require a country seeking a designated international agreement to demonstrate clear legal procedures and restrictions in terms of how government entities, such as law enforcement and national security agencies use electronic surveillance investigatory powers for the purposes of investigating serious

crime. The Committee considers that this should include clear legal mandates and procedures that govern the collection, retention, use and sharing of information collected using those powers. In the Committee's view, such a core principle also recognises the importance the Australian community places on mechanisms that go to accountability, transparency and oversight. The Committee also considers that this requirement would be in addition to the existing requirements in relation to seeking assurances on the use or non-use of Australian-sourced information in connection with prosecutions for an offence that is punishable by death.

2.109 In relation to prosecutions offences punishable by death, the Committee notes that Australia has a long standing commitment to the right to life and the Committee considers that the Bill should more explicitly state Australia's expectations in relation to use of Australian-sourced material in investigations where death is a sentencing option.

Recommendation 8

2.110 The Committee recommends that the proposed Schedule 1 of the *Telecommunications (Interception and Access) Act 1979* be amended to state that a country seeking a designated international agreement with Australia must meet the following criteria:

- **Demonstrates respect for the rule of law and the principles of equality and non-discrimination, as set out in paragraph 2.103;**
- **Demonstrates respect for applicable international human rights obligations and commitments, as set out in paragraph 2.104;**
- **Clear legal procedures and restrictions governing the use of electronic surveillance investigatory powers, as set out in paragraph 2.105; and**
- **If:**
  - **There is an agreement between Australia and a foreign country; and**
  - **If the agreement deals with (among others things) the issue of orders (however described) by a competent authority (however described) of the foreign country; and**
  - **One or more offences against the law of the foreign country are punishable by death**

The name of the agreement must not be specified under paragraph (1)(b) unless the Minister has received a written assurance from the government of the foreign country relating to the non-use of Australian-sourced information obtained by virtue of the agreement in connection with any proceeding for a death penalty offence in the country or territory.

2.111 The Committee notes the Independent National Security Legislation Monitor's recommendation that an investigatory powers division be established within the Administrative Appeals Tribunal to have oversight of the powers provided by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

2.112 The Committee supports the evidence provided by the Independent National Security Legislation Monitor and notes that the proposed

investigatory powers division could have a role in considering international production order requests.

2.113 The Committee considers that strengthening the independence of the authorisation process will provide valuable assurance to foreign governments that requests are appropriate and proportionate to the threat and is broadly supportive of such a model.

2.114 The Committee acknowledges the evidence from the Department of Home Affairs that the authorisation process for international production orders are higher than under the current domestic provisions, and that the Department considers that this process will ameliorate concerns regarding access to journalist information, including sources.

2.115 The Committee will consider the recommendations of the Independent National Security Legislation Monitor in the Committee's inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

2.116 However, in line with the recommendations made by the Committee in its recent inquiry into the impact of law enforcement and intelligence powers on the freedom of the press, the Committee considers that its recommendations – such as those related to Public Interest Advocates – be incorporated into the relevant provisions of the Bill.

Recommendation 9

2.117 The Committee recommends that, where relevant, the Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020 be amended to implement the recommendations set out in the Committee's report of its *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press*, including recommendation 2 (i.e. that the current role of the Public Interest Advocate, as provided for under the *Telecommunications (Interception and Access) Act 1979* be amended in line with the terms of that recommendation and expanded to apply to applications for international production orders.

3. Outgoing International Production Orders

3.1 This Chapter discusses the proposed powers provided in the Telecommunications Legislation Amendment (International Production Orders) Bill ('the Bill') for designated agencies to seek an international production order for interception of data, stored communications and telecommunications data.

Definitional terms

3.2 While the Bill provides key terms that broadly reflect domestic provisions, there are some variances in the definitions contained in the proposed Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

3.3 Though the TIA Act contains a definition of communications providers, the Bill suggests a more expansive definition. The Department of Home Affairs said that this is because the communications landscape has evolved significantly:

> As noted above, the communications landscape and the types of communications service providers have evolved significantly in recent decades. Accordingly, and in recognition of the kinds of international services likely to hold electronic data relevant to Australian criminal matters (such as over-the-top application services like Facebook, Instagram, Skype and Discord), the IPO framework reflects communications technologies in a broad sense. This differs from the current domestic warrant and authorisation

regimes for interception, stored communications and telecommunications data access, which are more limited in definition or scope.[1]

3.4 As set out by the Department of Home Affairs, this change would allow an international production order to be directed to the following types of communications services providers:

- Carriers and carriage service providers (e.g. internet service providers and telephone carriers)
- Message, voice and video call application service providers (e.g. Facebook Messenger, Skype, WhatsApp)
- Storage backup providers (e.g. cloud storage providers)
- General electronic content providers (e.g. chat forums, social media platforms and other website providers).[2]

3.5 The definitions of intercept and telecommunications data broadly replicate those contained in Chapter 2 and Chapter 4 of the current TIA Act, however, while the TIA Act defines stored communication as:

> …a communication that:
>
> - is not passing over a telecommunications system; and
> - is held on equipment that is operated by, and is in the possession of, a carrier; and
> - cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.[3]

the definition of stored communications has been broadened to include 'material that is uploaded for storage/back-up or posted'.[4]

3.6 Mr Thomas McBride said that the expansion of the definition of stored communications to include uploaded material captures information that would not be available under domestic provisions, and notes that the process of uploading information is often automatic and completed without the users' express consent.[5]

---

1 Department of Home Affairs, *Submission 10*, p. 6.

2 Department of Home Affairs, *Submission 10*, p. 6.

3 *Telecommunications (Interception and Access) Act 1979*, s 5.

4 Explanatory Memorandum, p. [29].

5 Mr Thomas McBride, *Submission 19*, p. [14].

3.7 The Explanatory Memorandum says that this expanded definition is designed to provide a clear distinction between the definition of interception and the definition for access to stored communications.[6]

3.8 The current TIA Act contains a definition of serious offence in section 5D to include offences that incur a maximum term of 7 years or life in most cases.[7]

3.9 Section 5E of the TIA Act includes an offence punishable by a maximum term of imprisonment of at least 3 years, offences carrying certain pecuniary penalties, or a serious offence as defined above.[8]

3.10 These definitions are largely replicated in the Bill to provide a serious category 1 offence and a serious category 2 offence.[9]

Seeking an International Production Order

3.11 The Bill proposes three different types of international production orders that can be sought for three purposes. The types of production orders include interception of data, access to stored communications, and access to telecommunications data.[10] Such an order may be sought for the following purposes:

- the investigation of an offence of a serious nature; or
- the monitoring of a person subject to a control order, so as to protect the public from terrorist acts, prevent support for terrorist acts and hostile acts overseas and detect breaches of the control order; or
- the carrying out by the Australian Security Intelligence Organisation (ASIO) of its functions.[11]

3.12 The process for seeking an international production order varies depending on the type of production order and the purpose for which it is sought. The differences in each of these processes is set out below.

---

6 Explanatory Memorandum, p. [28].

7 Department of Home Affairs, *Supplementary Submission 10.1*, p. 7.

8 Department of Home Affairs, *Supplementary Submission 10.1*, p. 7.

9 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1, cl. 1.

10 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1, cl. 1.

11 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1, cl. 1.

Enforcement of the criminal law

3.13 The Bill proposes to allow law enforcement agencies to seek an international production order to assist in the investigation or prosecution of serious crimes.

Interception of data

3.14 The ability to request interception of data is covered under current domestic provisions but is not a power available under the mutual legal assistance process.

3.15 An 'interception agency' may make an application to an eligible judge or nominated AAT member. As set out by the Bill, an interception agency includes the:

- Australian Federal Police
- Australian Commission for Law Enforcement Integrity
- Australian Criminal Intelligence Commission
- Law Enforcement Conduct Commission
- State Police Forces
- State-based Integrity and Corruption bodies.[12]

3.16 Other than in urgent circumstances, an application must be in writing and conform to the form and requirements set out by the Bill.[13] A written application must contain an affidavit to set out the facts and grounds on which the application is based.[14] An application may also take the form of a telephone application in urgent circumstances.[15] A definition of urgent circumstances is not provided in the Bill, and the Inspector-General of Intelligence and Security said:

> The Bill does not set out what may constitute an urgent circumstance, and the Explanatory Memorandum does not provide guidance on this matter. The Committee may wish to consider whether the types of circumstances that would amount to 'urgent circumstances' should be set out in legislation—

12 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 22(3).

13 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 23–24.

14 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 25.

15 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 26.

perhaps adopting the approach taken in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, where a specific harm threshold was inserted for urgent requests or notices. That Act provides that technical assistance requests and technical assistance notices must not be issued orally unless:

a. an imminent risk of serious harm to a person or substantial damage to property exists; and

b. the request or notice is necessary for the purpose of dealing with that risk; and

c. it is not practicable in the circumstances to give the request or notice in writing.

A similar statutory definition of 'urgent circumstances' could have several benefits: it would clearly articulate the Parliament's expectations about when 'urgent circumstances' are considered to arise, provide legislative guidance to nominated members of the Security Division of the AAT when considering IPO applications, and promote consistent decision-making within ASIO when applying for IPOs.[16]

3.17 In response, the Department of Home Affairs said that a statutory definition may limit the operational effectiveness of the telephone application provisions:

> … the Department notes that as currently drafted it relies on its ordinary meaning and is intended to cover circumstances which because of their urgency, mean that it is not possible to make an application in writing in the normal way following normal processes.
>
> While this power is unlikely to be used often, it is important that the legislation does not seek to anticipate every potential scenario where it may be needed because of 'urgent circumstances'. To do so may limit the operational utility of the regime.[17]

3.18 NSW Police outlined the internal processes associated with the domestic regime, for interception and stored communications requests, prior to being presented to the issuing authority:

> Requests for assistance drafted by applicants are reviewed and scrutinised by a specialist 'Assessment Committee' at the Telecommunications Interception Branch. This committee is comprised of specialist officers led by a

---

16 Inspector-General of Intelligence and Security, *Submission 27*, p. 13.

17 Department of Home Affairs, *Supplementary Submission 10.1*, p. 14.

> Superintendent of Police, who to date, has been a qualified lawyer. The committee assesses the application for compliance with the Act, ensuring reasonable grounds for suspicion that a requisite 'serious offence' for interception or 'serious contravention' for stored communications, has been committed or is likely to be committed and the person for whose service the matter applies can be adequately connected to use of that service.
>
> If the application is approved, the proposed deponent drafts an affidavit, which is quality reviewed by a Detective Inspector of Police. The reviewing officer completes a 'checklist' and acknowledges they have reviewed relevant aspects of the application for accuracy and compliance with legislative and organisational requirements.
>
> The affidavit is then forwarded to the NSWPF Covert Applications Unit, a specialist unit comprised of Legal Consultants and Solicitors, who review the affidavit for legal compliance, assess its appropriateness to be submitted to an issuing authority, and work with the applicant to ensure all legal considerations are adequately addressed. In circumstances were the Covert Applications Unit determines an individual's privacy is unjustifiably breached, or alternate, less intrusive means have not been exhausted, the investigator is informed and requested to address any of these concerns.
>
> Once an affidavit has been settled by a legal consultant at the Covert Applications Unit, it is reviewed by a supervisor or senior legal officer at the Covert Applications Unit. The senior legal officer again ensures compliance with each clause within the legislation and must sign off on the application for it to proceed to the issuing authority.[18]

3.19 Noting the intrusive nature of the interception powers, the Bill allows Public Interest Monitors in Queensland and Victoria to make submissions and question certain persons in the process of making submissions, in accordance with the statutory requirements of those jurisdictions.[19] The authorising authority in the state where the application is made must give weight to these submissions in deciding whether to grant the order.[20]

---

18 NSW Police, *Supplementary Submission 12.2*, p. 1.

19 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 28–29.

20 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 30(5).

3.20 Other matters that the eligible Judge or nominated AAT member must have regard to includes:

- interference with the privacy of an individual;
- the gravity of the conduct constituting a serious category 2 offence.
- the ability of the information sought to assist in a law enforcement investigation; and
- the extent to which other methods of investigation have been exhausted, and the likely assistance or prejudice such methods would cause.[21]

3.21 Where the eligible Judge or nominated AAT member is satisfied, on the basis of the information given, they may issue the IPO on the basis that the application requirements have been complied with, that there are reasonable grounds to suspect that the application relates to an appropriate designated communications provider, and that the information being sought would be likely to assist in connection with the investigation of a serious category 2 offence for the enforcement of criminal law.[22]

3.22 An order may require a carriage provider to intercept communications or an individual message/call application service to intercept messages sent or received, voice calls made or received, use of the service within a specified period and to make relevant material as disclosures as required under the Bill.[23] An order may not be made for a period in excess of 90 days.[24]

3.23 The Bill allows for interception of a communications service of a person who is not a person involved in an investigation of a relevant offence, referred to as a B-Party.[25] When considering a B-Party application, the eligible issuing authority must give consideration to matters of privacy, the availability and use of other means to achieve objectives, and the impact of the use of other means on the objectives of the investigation.[26]

---

21 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 30(5).

22 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 30(2).

23 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 30(2).

24 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 30(4).

25 Explanatory Memorandum, p. [9].

26 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 30(6–7).

3.24 Finally, the Bill sets out the contents of an IPO,[27] and provides that an eligible Judge or AAT member may make further IPOs in respect of a service to a provider, but only where the period specified in the new order commences after the end of the period in the original order.[28]

Stored communications

3.25 Law enforcement agencies have the ability to access stored communications under existing domestic provisions and under the mutual legal assistance process discussed in Chapter 2.

3.26 The Bill allows a criminal law enforcement agency to make an application for an IPO to an eligible magistrate, judge or member of the AAT ('issuing authority').[29] In the case of a written application, it must include an affidavit that sets out the facts and other grounds on which the application is based.[30] Where a criminal law enforcement agency considers that the circumstances are urgent enough to warrant a telephone application, the circumstances contributing to the urgency must be provided to the issuing authority.[31]

3.27 An issuing authority must have regard to the:

- interference with the privacy of an individual;
- the gravity of the conduct constituting a serious category 1 offence;
- the ability of the information sought to assist in a law enforcement investigation;
- the extent to which other methods of investigation have been exhausted, and the likely assistance or prejudice such methods would cause; and
- any other relevant matters.[32]

---

27 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 31.

28 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 32.

29 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 16.

30 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 33–36.

31 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 37.

32 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 39(3).

3.28 Where the issuing authority is satisfied on reasonable grounds that conditions related to the stored communications are met, they may issue an IPO requiring a designated communications provider to copy and disclose relevant communications to the criminal law enforcement agency.[33] An order may require that the stored communications are made available to a law enforcement agency in a specified way.[34]

Telecommunications data

3.29 Similar to stored communications data, law enforcement agencies have the ability to access telecommunications data under existing domestic provisions and under the mutual legal assistance process.

3.30 In contrast to existing domestic provisions, which allow internal staff members to approve an application to access telecommunications data, an application to access telecommunications data through an IPO must be made to an eligible magistrate, judge or member of the AAT.[35] An application may be written or by telephone in urgent circumstances.[36] In the case of a telephone application, the issuing authority must be satisfied that the matter was urgent.[37]

3.31 The issuing authority must have regard to the following matters:

- interference with the privacy of an individual;
- the gravity of the conduct constituting a serious category 1 offence.
- the ability of the information sought to assist in a law enforcement investigation;
- the extent to which other methods of investigation have been exhausted, and the likely assistance or prejudice such methods would cause; and
- any other relevant matters.[38]

---

33 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 39.

34 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 40.

35 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 48.

36 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 48.

37 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 48.

38 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 48.

3.32 Where the issuing authority is satisfied of these matters an IPO may be issued for a period commencing not before the time the order is provided to a designated communications provider, and for no longer than a period of 90 days.[39] The issuing authority may also direct that the information is disclosed to the enforcement agency through the Australian Designated Authority.[40]

Monitoring of a person subject to a control order

3.33 In March 2018, the Committee tabled its report on the control order regime in Australia.[41] A control order may impose obligations, prohibitions and restrictions on the subject of a control order, on the balance of probabilities that such an order is reasonably necessary. For a person over the age of 18, an order may remain in place for a period of 12 months, but for a person between the ages of 14 and 18 a control order may remain in place for no more than 3 months.[42]

3.34 Under the current provisions of the TIA Act, a warrant may be sought to obtain evidence of compliance or non-compliance with a control order.[43] The Bill seeks to allow relevant authorities to apply for information to support the monitoring of control orders to designated communications providers where that information is held overseas.[44]

3.35 In relation to control orders, the Law Council of Australia said that it is opposed to the inclusion of monitoring a person who is subject to a control order as a circumstance where it would be appropriate to seek an IPO:

> 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*

---

39 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 48.

40 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 49.

41 Parliamentary Joint Committee on Intelligence and Security, *Review of Police Stop, Search and Seizure Powers, The Control Order Regime and the Preventative Detention Order Regime*, March 2018

42 Parliamentary Joint Committee on Intelligence and Security, *Review of Police Stop, Search and Seizure Powers, The Control Order Regime and the Preventative Detention Order Regime*, March 2018, p. 37.

43 *Telecommunications (Interception and Access) Act 1979*, s. 46.

44 Explanatory Memorandum, p. [3].

1995 (Cth). This implements an equivalent international power to the domestic control order monitoring warrants presently available under the TIA Act.

The Law Council maintains its longstanding view that the control order scheme is neither necessary nor appropriate and, as such, should be repealed. 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.[45]

3.36 The Department of Home Affairs indicated that the increasing use of online communications platforms means that data that would assist law enforcement to monitor compliance with an order is increasingly located outside of Australia and 'outside of Australian agencies' reach'[46] and the Department said the ability to seek evidence will bolster Australia's ability to respond to terrorism threats.

In 2020, the AFP applied for and was granted control orders against convicted terrorist offenders upon release from prison after completing their head sentence. These orders have controls that limit their ability to use social media and communication based platforms. The use of social media platforms by a person on a Control Order constitutes a criminal offence that is punishable by a term of imprisonment. Timely access to evidence of these breaches through an IPO would be critical to the AFP's ability to respond rapidly, prosecute and enforce the breaches of control orders and ultimately assist in preventing an unacceptable escalation of risk to the Australian community. As such, IPOs for the purpose of monitoring and enforcing Control Orders would be an appropriate and proportionate law enforcement capability in the current threat environment.

It is well understood that terrorist threats can evolve rapidly, and the time between attack planning and execution can be very short. While the AFP can conduct monitoring warrants under section 3ZZOA of the *Crimes Act 1914* (Cth) and obtain Telecommunication Intercept and Surveillance Device warrants in relation to control order subjects, these have limitations.

- For example, if a control order subject was using an associate's device to access a social media account to contact prohibited associates.

45 Law Council of Australia, *Submission 28*, p. 35.

46 Department of Home Affairs, *Supplementary Submission 10.1*, p. 29.

- The ability to obtain an IPO in such circumstances would allow the AFP to access critical information stored offshore that may otherwise be unobtainable, at least in time to prevent possible imminent threat.[47]

3.37 The Committee commenced its latest statutory review of control order powers provided to the Australian Federal Police (AFP) under Division 104 of the *Criminal Code Act 1995* on 18 June 2020, and therefore while this report does not make comment on the effectiveness or appropriateness of these provisions, the Committee will have the opportunity to provide commentary as part of that inquiry in due course.

3.38 The Bill allows a control order IPO agency to make an application for an IPO in support of monitoring compliance with a control order. The definition is drawn from the current provisions of the *Telecommunications (Interception and Access) Act 1979*, which provides that a control order warrant agency includes a Commonwealth agency[48] or an eligible authority of a State that a declaration in force under the TIA Act authorises to apply for a control order warrant.[49]

Interception of data

3.39 A 'control order IPO agency' may make an application to an eligible judge or nominated AAT member either in writing – accompanied by a written affidavit[50] – or by telephone in urgent circumstances. A control order IPO agency includes:

- Australian Federal Police;
- Australian Commission for Law Enforcement Integrity;
- Australian Criminal Intelligence Commission; and
- Designated state authority declared under section 34 of the *Telecommunications (Interception and Access) Act 1979.*[51]

3.40 As above, the Bill allows Public Interest Monitors in Queensland and Victoria to make submissions and question certain persons in the process of

---

47 Department of Home Affairs, *Supplementary Submission 10.1*, p. 30.

48 Explanatory Memorandum, p. [6].

49 *Telecommunications (Interception and Access) Act 1979*, s. 5.

50 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 55.

51 Explanatory Memorandum, p. [6].

making submissions.[52] The authorising authority in those states where the application is made must give weight to these submissions in deciding whether to grant the order.[53]

3.41 In addition, an eligible judge or nominated AAT member must have consideration of the following matters:

- interference with the privacy of an individual;
- the ability of the information sought to assist in the protection of the public from a terrorist acts, the ability to prevent support for terrorist activities, or the ability to determine the success of the operation of the control order;
- the extent to which other methods that do not involve interception have been exhausted, and the likely assistance or prejudice such methods would cause; and
- whether the interception of activities would constitute the least interference with a person's privacy;
- the likelihood that a person has engaged in activities that would contravene a control order; and
- any other relevant matters.[54]

3.42 The inclusion of additional considerations for eligible judges and AAT members in issuing an IPO for monitoring compliance with a control order acknowledges that an IPO can be issued for a purpose that does not involve the investigation or prosecution of a serious offence:

> For IPOs relating to control orders, the decision maker must consider whether intercepting communications would be the method that is likely to have the least interference with any person's privacy. This additional requirement was inserted into the Bill (and forms part of the current domestic control order warrant regime) on the basis that additional protection is considered appropriate noting the IPO can be issued for purposes in connection with the monitoring of a person subject to a control order rather than in connection with an investigation into a specific serious offence.[55]

---

52 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 58–59.

53 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 60(5).

54 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 60(5).

55 Explanatory Memorandum, p. [7].

3.43 When the eligible judge or AAT member is satisfied on reasonable grounds of the conditions pertaining to the issue of an international production order, an order may be issued for no longer than 45 days if the order is sought in relation to a party that is not subject to a control order, or for 90 days when the application relates to the subject of a control order.[56]

3.44 When considering a B-Party application, the eligible judge or AAT member is restricted from issuing an order unless they are satisfied that the control order IPO agency has exhausted all other practicable methods of identifying the carriage service and that the interception of communications would not otherwise be possible.[57]

Stored communications

3.45 A control order IPO agency may make an application for access to stored communications to an eligible magistrate, judge or member of the AAT ('issuing authority').[58] An application may be written – accompanied by an affidavit[59] – or by telephone where a control order IPO agency considers that the circumstances are urgent enough to warrant a telephone application.[60]

3.46 An issuing authority must have regard to the:

- interference with the privacy of an individual;
- the ability of the information sought to assist in the protection of the public from a terrorist acts, the ability to prevent support for terrorist activities, or the ability to determine the success of the operation of the control order;
- the extent to which other methods that do not involve interception have been used by or are available to the control order IPO agency, and the likely assistance or prejudice such methods would cause; and

---

56 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 60(3–4).

57 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 60(7).

58 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 69.

59 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 66.

60 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 69.

- any other relevant matters.[61]

3.47 Where the issuing authority is satisfied on reasonable grounds that conditions related to the stored communications are met, they may issue an IPO requiring a designated communications provider to copy and disclose relevant communications to the control order IPO agency.[62] An order may require that the stored communications are made available to a control order IPO agency in a specified way.[63]

Telecommunications data

3.48 A control order IPO agency may make an application to access telecommunications data to an eligible magistrate, judge or member of the AAT. An application may be written – accompanied by an affidavit[64] – or by telephone in urgent circumstances.[65] In the case of a telephone application, the issuing authority must be satisfied that the matter was urgent.

3.49 An issuing authority must consider the following matters prior to deciding whether to issue an IPO for telecommunications data:

- interference with the privacy of an individual;
- the ability of the information sought to assist in connection with the protection of the public from a terrorist acts, the ability to prevent support for terrorist activities, or the ability to determine the success of the operation of the control order;
- the extent to which other methods that do not involve interception have been used by or are available to the control order IPO agency, and the likely assistance or prejudice such methods would cause; and
- any other relevant matters.[66]

---

61 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 69(3).

62 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 70.

63 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 70.

64 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 75.

65 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 73.

66 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 78.

3.50 Where the issuing authority is satisfied of these matters an IPO may be issued for a period commencing not before the time the order is provided to a designated communications provider, and for no longer than a period of 90 days.[67] The issuing authority may also direct that the information is disclosed to the enforcement agency through the Australian Designated Authority.[68]

The Administrative Appeals Tribunal as an issuing authority

3.51 The Bill allows the Attorney-General to, by writing, nominate the Deputy President, senior member, or member of the Administrative Appeals Tribunal (AAT) to issue international production orders where the conditions of the relevant clause are met.[69]

3.52 The application of such powers to members of the AAT is currently provided for under the domestic provisions of the *Telecommunications (Interception and Access) Act 1979*.

3.53 When performing these functions, a judge, magistrate or member of the AAT is acting in their personal capacity (*persona designata)*. The Attorney-General's Department describes *persona designata* functions:

> A judge, magistrate or AAT member exercises a function in their personal capacity as a way to ensure accountability in the course of a sensitive investigation or law enforcement procedure. Requiring an executive action to be approved by a decision-maker who is independent of government and outside of the investigation process can provide an important safeguard and promote public confidence that law enforcement agencies are operating with appropriate oversight.
>
> …
>
> *Persona designata* functions may only be conferred on a judge where the function is not incompatible with their role as a judicial officer. The independence of judicial officers from executive government is guaranteed by Chapter III of the Australian Constitution. The conferral of powers on federal judicial officers in their personal capacity must reflect the independence of

---

67 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 79.

68 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 79(5).

69 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 15.

> these officers, and meet the 'incompatibility principle'. This principle ensures that the functions do not undermine the judiciary's institutional integrity and its independence from the executive and legislative arms of government.[70]

3.54 Further, the Attorney-General's Department said that the consent component to the appointment of judges, magistrates and eligible AAT members enshrines the principle of *persona designata*, and allows for independent operation of powers:

> The Bill provides that judges of federal courts (excluding the High Court) may consent to being nominated as an eligible judge or issuing authority by the Attorney-General. The Attorney-General may then, by written declaration, confer on the judge a power to issue an IPO.
>
> Importantly, the consent process ensures that the functions conferred under Schedule 1 of the Bill are powers conferred on judges in their personal capacity, and not powers to be exercised by the court to which they are appointed. This arrangement, in which consent may be withdrawn at any time, also ensures that judges are not compelled to exercise the power to issue an IPO. This process is similarly replicated for magistrates.
>
> Similarly, as a matter of practice, AAT members provide written consents prior to being authorised to perform *persona designata* functions, and will do so for functions under the Bill. These are important features of a properly conferred *persona designata* power, enshrining the authoriser's independence and autonomy to decide whether or not to exercise powers vested.[71]

3.55 The Law Council said that while acting *persona designata*, a judicial officer must act consistently with the essential requirements of the judicial process:

> … 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.[72]

3.56 The Attorney-General's Department said that even though the AAT does not have its independence enshrined by the Australian Constitution, it has sufficient independence to appropriately authorise IPO applications:

---

70 Attorney-General's Department, *Submission 16*, p. 6.

71 Attorney-General's Department, *Submission 16*, p. 7.

72 Law Council of Australia, *Submission 28*, p. 29.

> While an AAT member is not independent of government in the same way as a judge (although some members of the AAT are also judges), the AAT is similarly seen to require a high degree of independence from government in its decision-making. AAT members are afforded similar protections to judges. For example, termination of the appointment of an AAT member is only possible if determined by the Governor-General following prayer for the termination by both Houses of Parliament on specific grounds and, in exercising *persona designata* functions, AAT members have the same protection and immunity as a Justice of the High Court of Australia. As such, similar principles which apply to judges also guide provisions relating to AAT members.[73]

3.57 As outlined in Chapter 2, the Independent National Security Legislation Monitor (INSLM) has proposed that an investigatory powers division be established within the AAT with certain controls to provide an additional degree of certainty in the independence of the authorisation process. The INSLM suggests that such a division not exercise their powers as *persona designata*.[74]

3.58 The INSLM suggested that an investigatory powers division should be equipped with technical and legal advisors that the division can draw upon in considering IPO applications.[75]

3.59 In order to make an executive agreement with a foreign party, the US CLOUD Act requires oversight by a court, judge, magistrate or other independent authority as a pre-condition to an agreement.[76] Some submitters suggested that the AAT may not be sufficiently independent and suggested that the judiciary should be given responsibility for authorising IPOs.[77]

---

73 Attorney-General's Department, *Submission 16*, p. 6.

74 Independent National Security Legislation Monitor, *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters*, Summary of recommendations, 2020, p. 21.

75 Independent National Security Legislation Monitor, *Trust but verify: A report concerning the* Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 *and related matters*, Summary of recommendations, 2020, p. 16.

76 US CLOUD Act §2523(b)(3)(D)(v)

77 See Law Council of Australia, *Submission 28*, pp. 29–30; BSA | The Software Alliance, *Submission 20*, p. 3; DIGI, *Submission 23*, p. 3; Australian Privacy Foundation, *Submission 1*, p. 5; Communications Alliance, *Submission 14*, p. 2; International Civil Liberties and Technology Coalition, *Submission 9*, p. 2.

3.60 The Committee notes that the Australian Government has received advice from US House Judiciary Committee indicating concerns with authorisation processes.[78] The Department of Home Affairs responded that these concerns have been taken into account when developing the IPO framework:

> The proposed differences between the pre-existing persons who can authorise warrants and authorisations, and the IPO framework, acknowledges the requirement to adopt a model that best accommodates different legal systems working alongside each other. This generally requires the identification and utilisation of similar decision-makers in approving investigatory powers (such as judicial authorities). Relevantly, the US CLOUD Act requires authorisation of orders by persons characterised as a '… court, judge, magistrate, or other independent authority'. The IPO framework facilitates this requirement.[79]

Committee comment

3.61 The Committee notes that the evolving nature of telecommunications services requires definitional updates that will enable the efforts of enforcement agencies to investigate and prosecute serious crimes and prevent terrorist acts. The Committee notes the concerns of submitters in relation to definitional amendments, but considers that these concerns can be appropriately managed through the application process.

3.62 The Committee considers that, overall, the provisions related to the application process for IPOs related to the enforcement of the criminal law and monitoring control orders give appropriate weight to the privacy of individuals and the necessary intrusion on privacy in certain circumstances to protect Australians from serious crime and terrorism.

3.63 However, the Committee considers that, in order to provide certainty to law enforcement dealing with IPO requests in urgent circumstances, the Bill should provide a definition of urgent circumstances that accords with the definition contained within the *Telecommunications (Interception and Access) Act 1979*.

---

78 DIGI, *Submission 23*, p. 3.

79 Department of Home Affairs, *Submission 10*, p. 7.

Recommendation 10

3.64 The Committee recommends that proposed Clause 2 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to include a definition of 'urgent circumstances' which provides that in circumstances where:

- **there is an imminent risk of serious harm to a person or substantial damage to property exists or, in the case of a national security IPO application, there is an imminent risk of loss of significant intelligence; and**
- **the production order is necessary for the purpose of dealing with that risk; and**
- **it is not practicable in the circumstances to submit an application in writing;**

such circumstances would constitute 'urgent circumstances' for the purposes of making an oral or telephone application.

3.65 The Committee considers that such a definition could apply to a broad range of scenarios that would necessitate the use of a telephone application.

3.66 The amount of information of assistance to an investigation that can be obtained through telecommunications data is not insignificant, and the Committee supports the mechanisms in place to ensure that applications for telecommunications data are appropriate and proportionate.

3.67 As discussed in Chapter 2, the Committee notes the INSLM recommended the establishment of an investigatory powers division with the Administrative Appeals Tribunal which would operate as an independent body and have access to technical and legal expertise in considering IPO applications. The Committee refers the Australian Government to the recommendation as a concept to consider as consideration on the IPO framework progresses.

3.68 The Committee notes the evidence from the Attorney-General's Department that the *persona designata* function ascribed to members of the AAT provides broad protection to make judgments independently. The Committee supports the qualification requirements set out in clause 16 of the Bill.

3.69 The Committee also notes the range of bodies authorised by the provisions of the Bill to make applications for international production orders. As set out in its *Review of the Mandatory Data Retention Regime*, the Committee considers that those accessing information under the relevant provisions of the Bill should meet certain standards in order to access telecommunications data. The Committee therefore recommends that the Bill be amended to incorporate an appropriate standard for access.

Recommendation 11

3.70 The Committee recommends that proposed Clauses 22(3), 33(3)(a), 52(3)(a) and 63(3)(a) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended in a manner that is consistent with Recommendation 11 of the of the Committee's *Review of the Mandatory Data Retention Regime*. That is, these provisions should be amended so that:

- **only officers or officials who are designated as authorised officers by the head of an enforcement agency may apply for IPOs;**
- **only officers or officials who hold a supervisory role in the functional command chain should normally be capable of being designated as 'authorised officers' (although other individuals who hold specific appointments – rather than entire classes of officers or officials – may also be capable of being designated as 'authorised officers')**
- **in order to authorise an individual to be an authorised officer, the head of an enforcement agency must be satisfied that it is necessary for an individual to be an 'authorised officer' in order for the individual to carry out his or her normal duties;**
- **prior to the head of an enforcement agency authorising an individual to be an 'authorised officer':**
  - **the relevant senior officer or official must complete a compulsory training program in relation to proposed new Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*; and**
  - **the head of the enforcement agency must be satisfied that the senior officer or official has the requisite experience, knowledge and skills to exercise the powers under proposed Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*.**

For the purposes of upholding Australia's national security

3.71 The Bill provides new powers for the ASIO – referred to as the Organisation in the Bill – to obtain assistance from designated communications providers for the purposes of upholding Australia's national security, in addition to

the powers of cooperation provided under section 19 of the *Australian Security Intelligence Organisation Act 1979*.[80]

3.72 Mr Peter Vickery, Deputy Director-General, Enterprise Service Delivery, ASIO said that the Bill will provide the Organisation with the tools it needs to address the ongoing threat of terrorism in Australia:

> ASIO welcomes this bill as an important piece of legislation that will assist ASIO in conducting its critical work in protecting Australia from threats to our security. Threats to Australia and Australians from both terrorism and espionage are at unacceptable levels. The terrorist threat remains at 'probable'—that is, we have credible intelligence that individuals and groups have the capability and intent to conduct terrorism onshore. Right now, terrorists are plotting to harm Australians. ASIO have said on a number of occasions that the level of threat we face from espionage and interference activities is unprecedented. Right now, there are more foreign intelligence officers and their proxies operating in Australia than at the height of the Cold War—many with the capability, the intent and the determination to cause significant harm to Australia's national security.
>
> ASIO support the international production orders bill, as it will assist us to protect Australia from violent, clandestine and deceptive efforts to harm Australians and undermine our sovereignty. ASIO activities in confronting these threats are conducted in an environment where almost all electronic communications of investigative value are encrypted.
>
> Authorised, warranted investigations into terrorist or espionage threats to Australia are increasingly hindered through encryption. ASIO have been engaged with the Department of Home Affairs in the formation of the bill as part of the ongoing collaborative work around a potential agreement with the United States to share information under the auspices of the CLOUD Act. The successful negotiation of an agreement between our two countries under the CLOUD Act will enable more timely access to security-relevant data and content held by US communications providers that is critical to ASIO's investigations but currently inaccessible. This would provide the least intrusive method to access such information, which is currently difficult to access via traditional methods of interception due to encryption.[81]

---

80 Law Council of Australia, *Submission 28*, p. 24.

81 Mr Peter Vickery, Deputy Director-General, Enterprise Service Delivery, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 1.

3.73 The Department of Home Affairs said that access to the IPO scheme provides a legislative pathway to ensure information can be provided to assist in the detection, prevention and investigation of serious crimes, including terrorism:

> ASIO's inclusion in the IPO regime provides a clear legislative pathway to ensure that ASIO is able to benefit from future international agreements for obtaining data directly from foreign communications providers. Many of the national security investigations undertaken by ASIO relate to the detection, prevention and investigation of serious crimes, including terrorism.
>
> The Bill is not intended to replace existing foreign cooperation mechanisms but to complement current processes to ensure our agencies have every avenue available to them to protect public safety and combat serious crime. Existing mechanisms do not enable ASIO to compel production of data from foreign providers.[82]

Interception of data and stored communications

3.74 To make an application for interception of data and stored communications, the Director-General of Security may designate ASIO employees or classes of employees to make an application on ASIO's behalf.[83]

3.75 The Inspector-General of Intelligence and Security said that this clause does not correspond with current provisions of the *Telecommunications (Interception and Access) Act 1979* that require the Director-General of Security to authorise warrants:

> The Bill proposes to provide the Director-General of Security, a Deputy Director-General of Security or an ASIO employee (in relation to whom a specific authorisation is in force) with the right to make an application for an international production order. There is no requirement in the Bill for the ASIO employee, or class of ASIO employees, be of a particular level of seniority or to possess particular qualifications. Nor does the Bill limit the scope of, or otherwise describe, the ASIO employees that could be authorised to apply for an IPO.
>
> More generally, these provisions are a substantial departure from ASIO's existing domestic telecommunications warrant regime. In particular, ASIO's existing warrant framework provides that only the Director-General may apply for a warrant to intercept telecommunications or to access stored

---

82 Department of Home Affairs, *Submission 10.1*, p. 26.

83 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 83 and 92.

communications. This restriction reflects the significant intrusion into a person's privacy (and that of third parties with whom they communicate) that results from interception and access. Similarly, the Director-General's power to apply for warrants under the ASIO Act cannot be delegated.[84]

3.76 Mr Vickery noted that any material provided to the Attorney-General's office is provided to the Director-General:

> From the outset, the underlying philosophy of the organisation in relation to all of the bill is that, where we can and where we should, we have existing protocols and policies and procedures that will continue to apply. So, in relation to IPOs, the underlying philosophy of anything that goes to the Attorney-General, like our current warrant regime, will have to go via the DGs office. There's certainly not an intention from anyone within the organisation—and I know from the director-general—that it will be a carte blanche ability for anyone in the organisation to apply for an IPO. That is certainly not the way that the organisation will operate. So our existing protocols and procedures in terms of authorisation levels or access to information will continue to apply.[85]

3.77 ASIO said that it is developing internal policy requirements to allow the Director-General to personally review applications for IPOs related to interception and stored communications:

- ASIO is developing an internal policy requirement for the Director-General to personally review and approve each application for an IPO for interception or stored communications before it is provided to the Attorney-General, and ahead of consideration by the Administrative Appeals Tribunal (AAT).
- While maintaining his oversight of IPO requests, the Director-General may not necessarily be the ASIO representative signing the IPO request.

> The IPO legislation enables the AAT to require the person who signed the IPO request to appear before them to provide further information. It is not efficient, viable or indeed necessary for the Director-General to personally provide this information on each and every occasion as required by the AAT. As such, ASIO will look to develop a system to accommodate this situation while maintaining appropriate Director-General oversight.[86]

---

84 Inspector-General of Intelligence and Security, *Submission 27*, p. 12.

85 Mr Vickery, ASIO, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 2.

86 ASIO, *Supplementary Submission 26.2*, p. 2.

3.78 ASIO must apply to the Attorney-General of Australia for approval to submit an application for an IPO.[87] The Attorney-General is prevented from consenting to the making of an application unless satisfied that there are reasonable grounds for suspecting that the services are being, or are likely to be, used for purposes prejudicial to Australia's security, or that the information would be likely to assist ASIO in carrying out its functions.[88]

3.79 The Attorney-General's Department said that this threshold is consistent with current domestic provisions:

> This threshold is consistent with the thresholds in sections 9 and 109 of the TIA Act for the Attorney-General to issue domestic warrants for interception and access to stored communications to ASIO.[89]

3.80 The Bill requires that a request to the Attorney-General seeking consent should be made in writing,[90] unless urgent circumstances necessitate seeking agreement orally.[91] Any such request must be followed up with a written report to the Attorney-General and the Inspector-General of Intelligence and Security detailing the particulars of the urgent circumstances.[92]

3.81 The Inspector-General of Intelligence and Security said that the Bill does not require ASIO to provide the circumstances justifying making an urgent application to the Attorney-General, and suggest amending the Bill to provide for this:

> An amendment to provide that the Attorney-General is also advised orally of the particulars of the urgent circumstances which necessitate a telephone application would ensure that the Attorney-General is apprised of the 'full picture' in the same manner and timeframe as the nominated AAT member. The report, proposed in subclauses 83(10) and 92(9), could then formalise the

---

87 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 83 and 92.

88 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 83(6–7) and 92 (6–7).

89 Attorney-General's Department, *Submission 16*, p. 8.

90 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 83(8) and 92(7)

91 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 83(9) and 92(8)

92 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 83(10–11) and 92 (9–10)

> oral advice provided to the Attorney-General, as well as advise the Attorney whether the application was granted, withdrawn or refused.[93]

3.82 Following the Attorney-General's consent, an application may be made to a nominated member of the Security Division within the AAT. The Law Council of Australia said that judicial officers should have the ability to be appointed to consider national security-related IPO applications:

> … 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.[94]

3.83 Mr Vickery said that due to the requirement to store and handle classified material, the Security Division of the AAT is appropriately placed to consider IPO applications made by ASIO:

> I think our view in relation to that is that we are comfortable with the security division of the AAT being the right place. I say that because that particular division has extensive experience in dealing with the organisation and the matters that we are involved in—for instance, in relation to security assessments and so on—so they're well versed in the way that we operate and what we can and cannot do. I would also note that the staff in that particular division have appropriate security clearances, they are well versed in the storage and handling of classified material, which is what we would be dealing with, and so we are very comfortable that that meets our requirements in terms of somebody to deal with to progress an application.[95]

3.84 The nominated AAT Security Division member must have regard to the extent to which other methods that do not involve interception have been used by ASIO, and the likely assistance or prejudice such methods would

---

93 Inspector-General of Intelligence and Security, *Submission 27*, p. 13.

94 Law Council of Australia, *Submission 28*, p. 32.

95 Mr Peter Vickery, ASIO, *Committee Hansard*, Canberra (evidence taken via teleconference), 14 May 2020, p. 8.

cause, as well as any other matters the nominated AAT Security Division member considers relevant.[96]

3.85 The Inspector-General of Intelligence and Security said that unlike law enforcement applications, the nominated AAT Security Division member is not required to consider privacy and proportionality in ASIO IPO applications:

> In particular, the nominated member is not required to have regard to the privacy of any person or the gravity of the conduct being investigated, or the level of assistance that would be likely be provided to ASIO in carrying out its functions. The Explanatory Memorandum does not give reasons for this distinction. IPOs issued to ASIO could potentially be very broad in scope, extending beyond individuals reasonably suspected of being engaged in acts prejudicial to security, to services used for 'purposes prejudicial to security'.
>
> IGIS would expect ASIO to consider privacy and proportionality matters in its applications. The Attorney-General's Guidelines, issued to ASIO under section 8A of the ASIO Act (discussed further below at page 10), require that any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence; and require ASIO to undertake its investigations using as little intrusion into individual privacy as is possible, consistent with the performance of its functions.[97]

3.86 The Inspector-General of Intelligence and Security further noted that 'the Attorney-General's Guidelines do not extend to decisions made by members of the Security Division of the AAT'.[98] The Department of Home Affairs outlined that the matters that must be considered reflect ASIO's anticipatory role:

> The criteria that must be considered by a nominated AAT Security Division member before issuing a national security international production order under Part 4 of the Bill recognises ASIO's role as being anticipatory and protective in nature.
>
> …

---

96 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 89 and 98.

97 Inspector-General of Intelligence and Security, *Submission 27*, p. 8.

98 Inspector-General of Intelligence and Security, *Submission 27*, p. 8.

> The decision-maker is also able to take into consideration any other matters they consider relevant, which may include further privacy or human rights considerations.
>
> These additional criteria ensure that the nominated AAT Security Division member assesses the potential privacy impacts, and that the proposed interference with privacy is proportionate to the national security purpose.[99]

3.87 Further, the Department of Home Affairs said that any requirement for nominated members of the Security Division of the AAT to consider privacy and proportionality would be duplicative, as ASIO makes these considerations prior to seeking the Attorney-General's agreement:

> The Guidelines ensure that privacy, proportionality and human rights are considered in issuing ASIO warrants under the TIA Act, and the Guidelines will also apply to national security international production orders.
>
> The guidelines provide that information to be obtained by ASIO is to be done in a lawful, timely and efficient way and in accordance with the following:
>
> - any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence
> - inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and
> - wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.
>
> These considerations ensure that ASIO conducts a thorough assessment of the potential privacy impacts before seeking to use covert powers such as those under an international production order, and that the use of those powers, including the necessary interference with a person's privacy, are proportionate to the relevant conduct. Noting these requirements it is unnecessary and duplicative to replicate them in the Bill.[100]

3.88 The Law Council of Australia said that administrative obligations do not provide appropriate safeguards for the use of intrusive powers, and that consistency between IPO provisions would be appropriate:

> … the Law Council considers that an administratively binding obligation about the manner in which an intrusive collection power is to be exercised is a

---

99 Department of Home Affairs, *Supplementary Submission 10.1*, pp. 9–10.

100 Department of Home Affairs, *Supplementary Submission 10.1*, p. 10.

> 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.
>
> 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'. However, the Law Council considers that the explicit statutory prescription of third-party privacy impacts as an issuing criterion would ensure that this matter is given a consistent degree of consideration and weight in the determination of all IPO applications.[101]

3.89 Where the member of the Security Division of the AAT is satisfied of the relevant matters, they may issue the IPO, and can incorporate conditions such as the format of the data and that the information be provided to the Australian Designated Authority.[102] For interception of data, this may be for a period of up to three months or up to six months where certain conditions are met.[103]

---

101 Law Council of Australia, *Submission 28*, pp. 33–34.

102 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 89 and 99.

103 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 89.

3.90 For applications related to B-Party interception, the nominated AAT Security Division member must have regard to whether other less intrusive methods of obtaining the information are available and have been used.[104]

Telecommunications data

3.91 Under domestic laws, applications to access telecommunications data by ASIO are approved by the Director-General of Security, Deputy Director-General of Security or an ASIO employee or ASIO affiliate approved by the Director-General of Security.[105] Under the Bill, such applications would be approved by a nominated member of the Security Division of the AAT and would not have to be approved by the Attorney-General.

3.92 The Department of Home Affairs said that this threshold has been put in place to accord with the requirements of making an executive agreement under the US CLOUD Act:

> … all international production orders sought by ASIO must be independently authorised by an Administrative Appeals Tribunal (AAT) Security Division member. This differs from the domestic framework in the TIA Act, under which ASIO warrants for interception or stored communications are authorised by the Attorney-General, ASIO journalist information warrants for telecommunications data are authorised by the Attorney-General, and authorisations for telecommunications data can be internally authorised.
>
> There is a clear policy reasoning for the different authorisation mechanism adopted for ASIO in the Bill, which reflects the unique requirements of the United States CLOUD Act. It is imperative that the framework of international production orders is well-placed to work alongside many different foreign legal systems. For example, the United States CLOUD Act requires that foreign orders under CLOUD Act agreements must be subject to review or oversight by an authority characterised as a "court, judge, magistrate, or other independent authority".[106]

---

104 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 89(6).

105 *Telecommunications (Interception and Access) Act*, s 175.

106 Department of Home Affairs, *Supplementary Submission 10.1*, p. 9.

3.93 An application for telecommunications data should be in writing,[107] and be accompanied by an affidavit,[108] unless urgent circumstances provide that it would be appropriate to make a telephone application.[109]

3.94 In order to issue an IPO for telecommunications data to ASIO, the nominated member of the Security Division of the AAT must be satisfied of several matters, including that the request is made in connection with ASIO's functions.[110] An application need not satisfy the nominated member that the subject of the request is involved in a serious offence.

3.95 The IGIS said that the nature of telecommunications data and the information it can provide has evolved since the existing domestic provisions were introduced in 2007, and that the authorisation threshold was 'low':

> While this is consistent with Chapter 4 of the TIA Act (the equivalent domestic authorisation scheme),
>
> IGIS notes that this domestic authorisation scheme is currently the subject of the Committee's *Review of the mandatory data retention regime*. In a submission to that review, IGIS noted that the threshold for ASIO to access telecommunications data is 'low'. This threshold was introduced more than twelve years ago (in 2007, the same year the iPhone was introduced) when the volume and nature of communications data held by carriers and carriage service providers was quite different. IGIS notes that the informative value and relative privacy intrusion of telecommunications data (including a person's location history, and the details of the persons they contact) to both intelligence agencies and the public, has increased significantly with technological advances. IGIS notes that other countries with similar regimes have set a higher threshold for data access than the Bill. For example, the United States' CLOUD Act limits any disclosure of communications or data to matters involving serious criminal offences and terrorism matters (which are indictable offences in Australian law).[111]

---

107 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 102(1).

108 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 104

109 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 102(2)

110 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl 107.

111 Inspector-General of Intelligence and Security, *Submission 27*, p. 9.

3.96 Where satisfied of the relevant matters, the nominated member of the AAT may issue an IPO that can require data to be disclosed in a certain format, or to the Australian Designated Authority.[112] An IPO cannot be granted for a period of longer than 90 days.[113]

Committee comment

3.97 The Committee notes the evidence from ASIO regarding the current and ongoing threats of terrorism in Australia, and supports the need for ASIO to have the tools available to address this threat.

3.98 However, given the necessarily classified nature of ASIO's role in investigating these threats, the Committee considers that there should be robust safeguards built into the international production orders framework to ensure that the public is assured that intrusions into individual privacy are considered with the necessary degree of proportionality.

3.99 The Committee considers that the Director-General of Security's ability to authorise employees of the Organisation to make applications for interception of data or to access stored communications on its behalf should be restricted to senior position holders of the Organisation as defined in the *Australian Security Intelligence Organisation Act 1979*.

Recommendation 12

3.100 The Committee recommends that proposed Clause 2 of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* amended to insert a definition of senior position holder that is consistent with the provisions of the *Australian Security Intelligence Organisation Act 1979*

112 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 107

113 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 107(4).

Recommendation 13

3.101 The Committee recommends that proposed Clauses 83 (3)–(4) and 92(3)–(4) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended so that the Director-General of Security may only delegate powers to a senior position holder

3.102 In recognition of the current authorisation thresholds for ASIO to access telecommunications data, the Committee does not propose to require a senior positon-holder to approve applications. However, the Committee notes the evidence received from the Inspector-General of Intelligence and Security that the nature of material that can be obtained through access to telecommunications data has evolved since the measures were first introduced.

3.103 The Committee therefore considers that applications by ASIO for telecommunications data should only be delegated to staff members at the Executive Level 2 (or equivalent) or above.

Recommendation 14

3.104 The Committee recommends that proposed Clauses 101(3)–(4) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to provide that the Director-General of Security can only authorise Australian Security Intelligence Organisation employees, or classes of Australian Security Intelligence Organisation employees, at the Executive Level 2 (or equivalent) and above to make applications on the Australian Security Intelligence Organisation's behalf.

3.105 The Committee supports the requirement for ASIO to inform the nominated member of the Security Division of the AAT of the particulars of the urgent circumstances requiring a telephone application, and include the matters that would have been required to be set out in the written application or affidavit in support of the application.

3.106 The Committee notes the evidence from the Inspector-General of Intelligence and Security that ASIO is not required to inform the Attorney-General of the same particulars when seeking oral agreement to make an application.

3.107 The Committee therefore recommends that, in order to provide assurance that the Attorney-General is provided with all relevant information, that the relevant clauses be updated to include the requirement to provide the

Attorney-General with the same information as a telephone application to the AAT.

Recommendation 15

3.108 The Committee recommends that proposed Clause 83(9) and 92(8) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* be amended to require the Australian Security Intelligence Organisation to provide the Attorney-General with:

- **the particulars of the urgent circumstances because of which the person making the request considers it necessary to obtain oral agreement**

- **the matters that ASIO would have been required to set out in a written application to the Attorney-General.**

3.109 The Committee supports the requirement for such an agreement to be followed up with a written report to the Attorney-General and the Inspector-General of Intelligence and Security within three days of the oral application.

4. Approval, Compliance and Oversight

4.1 This chapter discusses the role of the Australian Designated Authority, and other oversight bodies in relation to the provisions of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('the Bill').

The role of the Australian Designated Authority

4.2 Once a request for an international production order (IPO) has been received by an enforcement agency, a control order agency, or the Australian Security Intelligence Organisation (ASIO), it must be provided to the Australian Designated Authority (ADA).[1] As the Attorney-General's Department administers the provisions of the mutual legal assistance process – see Chapter 2 – the Secretary of the Attorney-General's Department is suggested as the appropriate authority.[2]

4.3 The Law Council of Australia said that the role of ADA would be more appropriately fulfilled by an independent statutory office holder:

> 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.

---

1 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1. cl. 111–112.

2 Attorney-General's Department, *Submission 16*, p. 9.

> 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.
>
> …
>
> 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 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.[3]

4.4 The Department of Home Affairs said that establishing the ADA as an independent statutory office holder would 'complicate existing approaches that work well in current international legal cooperation processes.'[4]

4.5 Following receipt, the ADA will assess whether an IPO complies with the provisions of the relevant designated international agreement (DIA).[5] Where it determines that an IPO complies with a DIA, the ADA is required to provide the IPO to the designated communications provider as soon as practicable.[6]

4.6 Where the ADA determines that an IPO does not comply, it has broad authority to cancel an IPO and return the document to the relevant agency along with any details it deems necessary for the reason it has determined that the IPO is incompatible with the conditions of the DIA. A cancellation may be made on the basis of the ADA's own assessment, or following the lodgement of a complaint by a provider. The Attorney-General's Department outlined the proposed process:

> Key functions of the ADA, as set out in Part 5, will be to review IPOs for compliance with the relevant DIA and, if satisfied that the IPO is compliant,

---

3 Law Council of Australia, *Submission 28*, pp. 52–53.

4 Department of Home Affairs, *Supplementary Submission*, p. 35.

5 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1. cl. 111–112.

6 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1. cl. 111–112.

give the IPO to the DCP in the foreign country (subclause 111(1)(c)). The ADA will liaise with the agency that obtained the IPO to obtain further information if necessary to determine the IPOs compliance with the DIA (subclauses 111(7) and 112(7)). If not satisfied that the IPO is compliant with the relevant DIA, the ADA must cancel the IPO and give the relevant agency such advice regarding compliance as may be required (clause 111(1)(d)). Under Part 7, the ADA also has a role in managing and considering objections from DCPs where the DCP has reason to believe that an IPO directed to it does not comply with the relevant DIA.

The ADA has a broad discretion to cancel an IPO, including before or after it has been provided to the DCP (clause 122). In practice, the ADA may decide to cancel an IPO for a range of reasons including, for example, because the ADA receives new information that indicates the IPO does not in fact comply with the DIA, or the ADA considers it in the public interest to do so following dispute resolution with the DCP or the government of a foreign country pursuant to Part 7 or the terms of the DIA.[7]

4.7 The Law Council of Australia said that the powers granted to cancel an IPO under the Bill are not sufficiently prescriptive:

> 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. Subclause 122(1) simply provides that the ADA may cancel an IPO, 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 to exercise its discretionary power to cancel the IPO after giving it to the DCP and considering the DCP's objection.[8]

4.8 In response the Department of Home Affairs said that the discretionary power provides flexibility in dealing with IPOs:

> Clause 122 of the Bill stipulates the Australian Designated Authority may cancel an international production order. The construction gives adequate flexibility for agreed review and dispute resolution processes to operate by

---

7 Attorney-General's Department, *Submission 16*, p. 9.

8 Law Council of Australia, *Submission 28*, pp. 38–39.

> virtue of designated international agreements. For example, a designated international agreement may allow a designated communications provider to raise an objection to the requesting party's authorities on particular grounds and set out a process for that to occur.
>
> Administrative guidance will also set out the procedures and process that the Australian Designated Authority will go through when it receives an objection from a designated communications provider.
>
> If an order is found to be incompatible with the agreement after an objection has been raised by a designated communications provider (in circumstances there was an original assessment that it was compliant), the Australian Designated Authority would be under an obligation under the designated international agreement to ensure that the order is not progressed.[9]

4.9 The Law Council of Australia suggested that the Bill should be amended to require the ADA to cancel an IPO when it determines the conditions are not consistent with an IPO application.[10] The Department of Home Affairs said that this would constrain the ability to remedy issues before seeking cancellation:

> Adopting this recommendation would limit Australia's flexibility – under the proposed model the ultimate outcome if there is non-compliance with the international agreement is the international production order would be cancelled. However, the construction adopted in the Bill provides an ability to remedy issues before this is to occur.[11]

4.10 The ADA is intended to be the first point of contact for designated communications providers who object to provisions of an IPO. Several submitters identified concerns with the lack of judicial review for decision-making.[12] In its submission to the inquiry, Google said that consideration should be given to appeals options in the Bill:

> We respectfully suggest that the appeal options contained within the Bill could be strengthened. Deferring to existing appeal mechanisms is not satisfactory given the lack of appropriate merit based appeal processes in other relevant legislation such as the Telecommunications and Other Legislation (Assistance

---

9 Department of Home Affairs, *Supplementary Submission 10.1*, p. 32

10 Law Council of Australia, *Submission 28*, p. 40.

11 Department of Home Affairs, *Supplementary Submission 10.1*, p. 32

12 See BSA | The Software Alliance, *Submission 20*, pp. 4–5; International Civil Liberties and Technology Coalition, *Submission 9*, p. 6; ACT The App Association, *Submission 25*, pp. [3]–[4]; Mr Eric Wilson, *Submission 7*, p. 14.

> and Access) Act 2019. The reliance on existing law as the primary source for appeal procedures is especially problematic in light of the enforcement provision discussed above. In particular, overseas providers may be subject to other third-country laws, conflicts with which are not and cannot be lifted through the international agreement, yet no option would exist to raise such an impediment to compliance. This would create exactly the type of conflict of laws scenario that the CLOUD Act is designed to prevent.[13]

4.11 However, the Department of Home Affairs said in its supplementary submission that Australian courts would retain jurisdiction for judicial review of a decision to issue an IPO through the original jurisdiction of the High Court of Australia and the Federal Court of Australia:

> The Bill provides for independent authorisation of international production orders. In addition, Australian courts will retain jurisdiction for judicial review of a decision to issue an IPO, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*. This ensures that an affected person or a provider has an avenue to challenge decision-making.
>
> The Australian Designated Authority will perform the role of ensuring that international production orders comply with the terms of the designated international agreements. The Australian Designated Authority will be the key facilitator and single point of contact for Australian agencies and foreign providers with experience, expertise and a broad view across international crime cooperation matters. The Bill contains a specific mechanism for designated communications providers to raise objections with the Australian Designated Authority, and it is anticipated the international agreements themselves will also contain processes for objections and resolution of disputes between governments and between providers and governments. Decisions of the Australian Designated Authority will also be subject to judicial review.[14]

4.12 Outside of the ADA's ability to cancel an IPO, enforcement agencies, control order agencies and ASIO have the ability to revoke IPOs in a variety of circumstances, including revocation of an IPO where the grounds on which the order was issued have ceased to exist.[15]

---

13 Google, *Submission 21*, p. [3].

14 Department of Home Affairs, *Supplementary Submission 10.1*, p. 32.

15 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1, cl. 114–115.

4.13 Similar to the approval powers discussed in Chapter 3, the revocation provisions allow for the Director-General of Security to delegate revocation powers to any ASIO employee.[16]

4.14 As noted in Chapter 3, an issuing authority has the power to subject an IPO to conditions requiring information to be supplied directly to the enforcement agency, control order agency, or ASIO. The issuing authority can also require the information to be supplied through the ADA. Google suggested that designated communications providers should be required to provide all information to the ADA:

> Designated communications providers are instructed under Schedule 1 Part 6 of the Bill to provide any requested communications and data to the requesting agency or the Australian Designated Authority, depending on the directions of the IPO. Respectfully, our experience is that a better approach would be that all communications to and from an Australian law enforcement agency be channelled through the Designated Authority and that this Authority acts as a coordinator across multiple agencies. Putting in place a coordinating body will guard against the risk of duplication and will act as a single point of contact for training, education and access to designated communications providers.[17]

Compliance with IPO requests

4.15 In order to comply with an IPO request, a designated communications provider must provide information within the requested timeframe. Where the conditions of an IPO are not complied with, a civil penalty may apply.

4.16 Ms Lucie Krahulcova of the International Civil Liberties and Technology Coalition said that the civil penalties for non-compliance encroach on the sovereign jurisdiction of a foreign country:

> This is I think less about penalty than an attempt to exert jurisdiction over data that is held in a different country. Although, how far can one country reach into the other where the provider is located to demand the data? To date, that has been only through government-to-government requests under the mutual legal assistance treaty process. The CLOUD Act structure is designed to create a more streamlined process, recognising that in the MLAT process the rights protected are cumbersome, so it's a question of how far one country can reach into the others. I think it's a jurisdictional question separate from how you can

---

16 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1, cl. 119.

17 Google, *Submission 21*, p. [2].

> condition the rights of companies that try to do business within your borders.[18]

4.17 In order for the compliance framework to take effect, there has to be a material link to Australia. The Bill provides that a designated communications provider must supply a service to one or more Australians; must own or operate a telecommunications network that is used to supply a carriage service; or one or more Australians have posted material on an electronic content service provided by a designated communications provider.[19]

4.18 In addition, for the compliance framework to apply, a two-part test must be satisfied. The Explanatory Memorandum sets out the requirements of the test:

> This provision sets out a two-part test for the compliance framework to apply. Firstly, the 'minimum contacts' test that requires there be a minimum of one or more Australians using the service, who are ordinarily resident in Australia. The second part sets out when a designated communications provider does not meet the threshold, on an exception basis. The second part is a 'reasonableness' test that goes to whether the designated communications provider could not reasonably be considered to have offered or provided the service to Australians at the time the order was given. The intention is to permit legal process to be served on a wide array of providers, but to exclude from the compliance framework local services that restrict their services to particular local identifiers for access, or passive services that have no intention that Australians use their services.[20]

4.19 Where the designated communications provider meets the elements of the threshold, the Bill provides for an civil penalty provision that allows the Communications Access Co-ordinator as an independent officer within the Department of Home Affairs to apply for an order – that is enforceable by Part 4 of the *Regulatory Powers (Standard Provision) Act 2014* – to the Federal Court or the Federal Circuit Court.[21]

---

18 Ms Lucie Krahulcova, International Civil Liberties and Technology Coalition, *Committee Hansard*, Canberra (evidence provided via teleconference), 13 May 2020, p. 14

19 Explanatory Memorandum, p. [79].

20 Explanatory Memorandum, p. [79].

21 Explanatory Memorandum, p. [80].

Evidentiary certificates to demonstrate compliance with IPO requests

4.20 The Bill provides for enforcement agencies, control order agencies, ASIO, the ADA, and designated communications providers to make evidentiary certificates to detail their compliance with the requirements of an IPO.

4.21 A designated communications provider may set out an evidentiary certificate in lieu of an affidavit detailing acts or things done by a provider to comply with an IPO:

> Part 12 of the Bill includes provisions for the issuing of evidentiary certificates that set out facts in respect of acts or things done by DCPs in compliance with IPOs. For example, subclauses 161(1) and (2) provide that where an IPO is directed to a DCP such DCPs may issue certificates setting out relevant facts 'with respect to acts or things done to comply with the [IPO]'. Subclause 161(3) goes on to provide that in proceedings in Australia, such certificates are to be received in evidence without further proof and will be deemed conclusive evidence of the matters stated within.[22]

4.22 An evidentiary certificate negates the requirement for a designated communications provider to travel to Australia to provide evidence, and also replicates domestic provisions:

> Current practices within the TIA Act for domestic interception, access to stored communications and telecommunications data allow for evidentiary certificates. The use of evidentiary certificates for IPOs is of significant utility as requiring the appearance of employees of foreign designated communications providers to court proceedings held in Australia will be complex and, at times, impractical. This also recognises the novel fact that whilst it will be easier to obtain information by virtue of the new order framework, Australian prosecutorial and law enforcement bodies will not be able to compel foreign provider employees to attend court to give evidence.[23]

4.23 The Law Council of Australia questioned the appropriateness of conclusive evidentiary certificates for this purpose:

> 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

---

22 Attorney-General's Department, *Submission 16*, p. 14.

23 Explanatory Memorandum, p. [95].

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 applicable conditions or limitations). There is also an open question as to whether subsection 18(2) itself remains appropriate in contemporary circumstances.[24]

4.24 The Attorney-General's Department said that the content of conclusive evidentiary certificates should be limited to matters not generally in contestation:

> The content of conclusive evidentiary certificates should be limited to procedural, formal, technical and non-controversial matters, so that the certificates:
>
> - cover matters sufficiently removed from the main facts in issue
> - would not prevent the admissibility of the content of communications produced under IPOs from being challenged
> - would not prevent the legality of the issuance of IPOs from being challenged.
>
> Clause 161 is consistent with the approach in subsection 18(2) of the TIA Act, which was upheld by the New South Wales Court of Criminal Appeal in *R v Cheikho*. Subsection 18(2) allows certificates to conclusively set out such facts relevant to 'acts or things done by, or in relation to, employees of the carrier in order to enable a warrant to be executed'. As the matters in clause 161 are non-controversial and well removed from the ultimate facts in a case, it is acceptable for clause 161 certificates to be received as conclusive evidence.[25]

4.25 The Department of Home Affairs said that the inclusion of conclusive evidentiary certificates does not prevent the judge from exercising discretion in deciding whether to adduce the evidence:

> Subclause 161(3) of the Bill is consistent with the approach taken for provider evidentiary certificates in the TIA Act. These provisions specify that certificates are conclusive evidence of the matters stated in the certificate

---

24 Law Council of Australia, *Submission 28*, pp. 57–58.

25 Attorney-General's Department, *Submission 16*, pp. 14–15.

> where they cover technical matters that are sufficiently removed from the main facts at issue. This will ensure that Australian courts have complete information before them to assist in the administration of justice.
>
> This provision recognises the difficulties associated with having staff from communications providers attend court to give witness testimony on technical or formal matters undertaken by the provider to comply with an order. These difficulties are expected to be greater under the international production order framework as designated communications providers will be based overseas and would need to travel internationally to attend court in Australia. In addition, it is expected that large global communications providers may receive a high number of international production orders.
>
> This provision does not prevent a defendant from challenging the admissibility of illegally or improperly obtained evidence during proceedings. The presiding judge retains discretion over whether to admit evidence.[26]

4.26 Information related to other matters contained in the Bill may be provided in a *prima facie* evidentiary certificate:

> By contrast, evidentiary certificates issued under clauses 162 to 166 will be considered prima facie evidence of their respective matters. These certificates relate to: voluntary provision of associated information (subclause 30(2)(j)), interception (subclause 163(4)(b)), stored communications (subclause 164(4)(b)), telecommunications data (subclause 165(4)(b)), and the ADA (subclause 166(5)(b)).[27]

4.27 *Prima facie* evidentiary certificates may be challenged by contradictory evidence against the facts, which is in line with the ordinary rules of evidence.[28] The Law Council of Australia said that all evidentiary certificates should be *prima facie*:

> 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.[29]

---

26 Department of Home Affairs, *Supplementary Submission 10.1*, p. 37.

27 Attorney-General's Department, *Submission 16*, p. 14.

28 Attorney-General's Department, *Submission 16*, p. 14.

29 Law Council of Australia, *Submission 28*, p. 58.

Oversight by the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security

4.28 The Commonwealth Ombudsman will have oversight responsibility of the actions of the ADA, law enforcement agencies and control order agencies with access to the IPO regime. In line with its traditional oversight role, the Inspector-General of Intelligence and Security (IGIS) will retain oversight responsibility of ASIO in relation to the IPO regime.

4.29 The functions and powers of the Commonwealth Ombudsman in overseeing the regime is set out in Part 10 of the Bill. The Commonwealth Ombudsman notes that the provisions of the Bill fit with its existing oversight role,[30] and outlines the impact of the Bill on inspection requirements:

> The Bill would provide my Office with responsibility for inspecting and reporting on law enforcement and integrity bodies' use of international production orders (IPOs) to intercept telecommunications provided by organisations overseas, or gain access to stored communications and telecommunications data held by these organisations. While my Office currently inspects those bodies' use of the above powers within Australia,' the Bill would create three new, parallel regimes which would impose an additional set of requirements to access data and content held overseas.[31]

4.30 The Commonwealth Ombudsman said that overseeing compliance with the IPO regime would be resource intensive, despite efforts to ameliorate this:

> My Office would be able to leverage its existing knowledge and expertise from inspecting use of domestic access regimes to develop and implement approaches for inspecting the use of IPOs. Further, we would look to minimise costs by scheduling multiple inspections with a single agency wherever possible.
>
> However, the Bill proposes requirements that my Office inspect and report about the use of IPOs separate from the inspection reporting requirements for the domestic regime. For this reason, my staff would likely need to inspect both a full sample of IPOs and a full sample of domestic authorisations for each type of access and for each agency.
>
> Under the Bill, six Commonwealth agencies and 15 State and Territory agencies could gain access to data and information held overseas under each

---

30 Commonwealth Ombudsman, *Submission 3*, p. 1.

31 Commonwealth Ombudsman, *Submission 3*, p. 1.

of the three IPO regimes. The Office would also have the function of inspecting the records of the Australian Designated Authority. This could result in up to 65 additional inspections each year.[32]

4.31 The Commonwealth Ombudsman said that the primary means of inspection is through the examination of records:

> The primary means through which the Ombudsman will carry out oversight of the IPO scheme is through the inspection of records. To support the Ombudsman's inspection role, the Bill provides the Ombudsman with a range powers, including powers to:
>
> - enter the premises of a relevant agency or the ADA at any reasonable time
> - obtain full and free access to all records of the relevant agency or the ADA which are relevant to the inspection, and the ability to make copies of relevant documents
> - require staff members of a relevant agency or the ADA to provide the Ombudsman with any information in their possession (or which the member has access to) that the Ombudsman considers necessary and relevant for the inspection
> - require staff of a relevant agency and the ADA to provide the Ombudsman any assistance the Ombudsman requires to perform the inspection function
> - require specific staff members of a relevant agency and the ADA to provide information and answer questions relevant to an inspection, with the failure to provide such information or answer such questions subject to a penalty of up to six months' imprisonment.[33]

4.32 The Commonwealth Ombudsman had raised resourcing requirements with Government:

> While I am broadly comfortable with the oversight role the Bill provides my Office, if the Bill is passed without appropriate funding, my Office will not be able to undertake the activities necessary to assure the Parliament these new powers are being used appropriately. I note that my Office is engaged in conversations with the Government, with funding proposed to be determined in an upcoming budget process.[34]

4.33 The Bill provides a positive notification requirement for relevant agency heads to notify the Commonwealth Ombudsman of matters relating to the

---

32 Commonwealth Ombudsman, *Submission 3*, p. 1.

33 Attorney-General's Department, *Submission 16*, p. 16.

34 Commonwealth Ombudsman, *Submission 3*, p. 2.

issue and revocation of IPOs. The Australian National University Law Reform and Social Justice Research Hub suggested that the timeframe for reporting the issue of an IPO should be one month:

> We are also concerned about the timeframe provided to agencies to notify the Ombudsman and provide a copy of the IPO order. Given the general concern regarding the timeliness of the orders (indeed the delay in the present international information access scheme is the primary justification for the Bill), a similar degree of haste in reporting the orders to ensure compliance should be expected.[35]

4.34 Law enforcement and integrity agencies are comfortable with the positive notification and broader oversight requirements:

> ACLEI is also comforted by the clear guidance and safeguards the Bill provides in terms of accessing and handling this information. The requirements on Agency heads to notify the Ombudsman of the issue of an order, and to produce a copy of that order, enable clear oversight of the use of the proposed provisions.[36]

4.35 Every three months, ASIO is required to provide a report to the Attorney-General regarding its use of interception orders under the IPO regime.[37] The IGIS said that this reporting requirement should be extended to IPOs issued for access to stored communications and telecommunications data, and should require reporting on additional matters:

> The Bill provides that the Director-General must give a written report to the Attorney-General in respect of each IPO issued for intercepted communications within three months of its expiry, revocation or cancellation. However, IGIS notes that the Bill currently provides that a report to the Attorney-General is not required for IPOs for access to stored communications or IPOs for telecommunications data. The Explanatory Memorandum does not give any reasons for this difference. To close this lacuna and to ensure consistency and accountability, IGIS suggests that written reports, within three months of expiry, should be provided to the Attorney-General for all IPOs, or at least those IPOs where the Attorney-General's consent is required prior to issue.

---

35 The Australian National University Law Reform and Social Justice Research Hub, *Submission 17*, p. 6.

36 Australian Commission for Law Enforcement Integrity, *Submission 2*, p. 4.

37 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 129

> Further, while clause 129(a) requires ASIO to provide a report to outline how the information collected under an IPO for interception has assisted the Organisation in carrying out its functions, IGIS suggests that these reports should be required by statute to include more comprehensive reporting requirements, such as an explanation of what information or data was obtained (including any information or data relating to persons other than the subject of the IPO), how ASIO has used the information or data (including whether such information or data was shared with other agencies) and whether the data is still being retained (and, if so, why).[38]

4.36 Additionally, ASIO is required to provide notice to the IGIS on matters relating to revocation of IPOs, however the Bill is silent on notifying the IGIS on when an order is sought. The IGIS suggested that a recommendation to this effect should be incorporated:

> As a result [of implementing notice recommendations of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018], that Act requires ASIO to notify IGIS within seven days of issuing an industry assistance request or notice, regardless of the urgency of the assistance sought.
>
> There are no equivalent notification requirements in the IPO Bill for ASIO to notify the IGIS, and the Committee may wish to consider an amendment to the Bill to provide for a statutory notification obligation. Noting that the frequency of ASIO's use of IPOs may be difficult to quantify for some time, it may be sufficient for there to be a statutory obligation to notify IGIS within three months, with the option of other notification periods being agreed to by the Inspector-General and the Director-General. This could allow for bulk or batch-style reporting on a periodic basis, if necessitated by the quantity of orders issued.[39]

4.37 The IGIS is granted broad oversight of ASIO by virtue of its enabling legislation and by the provisions of the Bill:

> IGIS will have oversight of ASIO's use of the IPO framework. This oversight will be supported by existing provisions in the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), which confers broad oversight powers on the IGIS in relation to ASIO activities. In addition, the Bill includes a number of mechanisms designed to ensure that IGIS has access to relevant information to facilitate effective ASIO oversight, including notably:

---

38 IGIS, *Submission 27*, p. 14.

39 Inspector-General of Intelligence and Security, *Submission 27*, p. 17.

> The Bill imposes obligations on ASIO to share certain information with IGIS and keep records of ASIO's use of the IPO framework (clauses 83(11), 92(10), 135 and 136).
>
> The Bill also provides an exemption to the information protection requirements in Part 11 to allow protected information to be disclosed to an IGIS official for the purposes of the performance of a duty, power or function under the IGIS Act (clause 153). In addition to allowing ASIO employees to disclose IPO-related information to IGIS, this exemption also supports IGIS' visibility of ASIO's IPOs as they progress through the assessment phase undertaken by AGD (as the ADA) by permitting AGD employees to share relevant information with IGIS.[40]

4.38 However, the IGIS raised concerns about the wording of the legislation in its potential to constrain its oversight ability. The IGIS notes that the secrecy provisions as worded could limit the extent of cooperation between the Attorney-General's Department as ADA and the IGIS:

> As noted by the Attorney-General's Department in its submission, the exception will permit both ASIO and Attorney-General's Department employees to share relevant information with IGIS, including for the purpose of IGIS's inspections, inquiries or in response to complaints about ASIO's activities under the IPO framework
>
> However, IGIS notes two limitations in the scope of this exception as drafted:
>
> 1 The exception at clause 153(1)(p) only extends to an IGIS official's functions, duties and powers under the IGIS Act. IGIS officials also have functions and duties under other pieces of legislation, including the ASIO Act, the Freedom of Information Act 1982 and the Public Interest Disclosure Act 2013. Unnecessarily limiting the exception to functions and duties under the IGIS Act could limit our ability to respond appropriately to matters arising under each of those Acts in connection with ASIO's activities under the IPO regime. This limitation would be resolved if the exception was amended to enable disclosure for the purpose of 'an IGIS official exercising a power, or performing a function or duty, as an IGIS official'.
>
> 2 The exception at clause 153(1)(p) only extends to information being used, recorded or disclosed (for example, by the Attorney-General's Department) in support of IGIS's functions. Given that IGIS and the Attorney-General's Department will have oversight roles for different parts of the process for ASIO IPOs, IGIS may need to work closely with the Department to ensure that the respective roles are effective. This may, at times, require IGIS to

[40] Attorney-General's Department, *Submission 16*, p. 17.

> share information with the Department in support of its functions. Under the secrecy offence at section 34 of the IGIS Act, however, it is an offence for an IGIS official to divulge to any person information acquired under the IGIS Act by reason of the person being an IGIS official, except in the performance of his or her functions or duties or in the exercise of his or her powers under the IGIS Act (or other named Acts). A broadly drafted amendment to the IGIS Act, providing explicit authority for IGIS officials to share information with the Attorney-General's Department for the purpose of its role as Australian Designated Authority, would achieve the necessary level of certainty for IGIS and the Attorney-General's Department to cooperate in this manner.[41]

4.39 The IGIS suggested that the construction of the relevant clauses of the Bill may unintentionally constrain the sharing of information by the ADA in relation to its functions under the *Australian Security Intelligence Organisation Act 1979*, the *Freedom of Information Act 1982*, and the *Public Interest Disclosure Act 2013*. In addition, the provisions of the secrecy offences in the *Inspector-General of Intelligence and Security Act 1986* may prevent the ADA from sharing information with the IGIS.[42]

4.40 While the Bill allows the Commonwealth Ombudsman to access the mandatory register of IPOs maintained by the ADA, the IGIS is not provided with access to the register. The IGIS noted that it does not have oversight of the ADA, however, the IGIS indicated that access to the register would assist with oversight of ASIO's compliance with the requirements of the regime.[43]

4.41 The Law Council of Australia suggested that the ability of the IGIS to give protected information to the Commonwealth Ombudsman and the ADA should be expanded to enable more efficient oversight:

> 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

---

41 Inspector-General of Intelligence and Security, *Submission 27*, p. 17.

42 IGIS, *Submission 27*, p. 20. See also, the Law Council of Australia, *Submission 28*, p. 44.

43 IGIS, *Submission 27*, p. 18. See also the Law Council of Australia, *Submission 28*, p. 44.

- 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.[44]

Reporting and record-keeping requirements

4.42 The Department of Home Affairs said that there are several components of the Bill that are designed to allow for reporting to occur:

> Comprehensive oversight and reporting is a key objective of the IPO framework. This has been developed to reflect Australian community expectations of appropriate oversight around the interception of communications, and access to stored communications and telecommunications data under the TIA Act. Core aspects of the oversight and reporting under the IPO framework include:
>
> - Comprehensive oversight regime by the Commonwealth Ombudsman of law enforcement agencies' use of the IPO framework, and the Australian Attorney-General's Department insofar as it relates to its duties as the Australian Designated Authority (see below).
> - The Minister, upon receipt of annual inspection reports conducted by the Commonwealth Ombudsman, must cause a copy to be tabled in Parliament.
> - Comprehensive oversight regime by the Inspector-General of Intelligence and Security of ASIO's use of the IPO framework (under its existing powers).
> - Reporting on ASIO's use of the IPO framework as part of ASIO annual reporting requirements under the Australian Security Intelligence Organisation Act 1979
> - Reporting on inspections provided as part of the regular Inspector-General of Intelligence and Security reporting.
>
> Furthermore, agencies will only be able to keep sensitive personal communications where there is a legitimate reason to do so; otherwise, agencies will be required to immediately destroy all records obtained using an IPO.[45]

4.43 The ADA and law enforcement agencies are required to provide information regarding the use of the IPO regime to their Minister each year which will be

---

44 Law Council of Australia, *Submission 27*, p. 47.

45 Department of Home Affairs, *Submission 10*

tabled in Parliament.[46] However, information relating to ASIO's operation will be contained in its classified annual report, and information relating to control orders will be excluded from reporting requirements if it could identify a person subject to a control order.[47]

4.44 The Explanatory Memorandum outlines the reasons that control order information may be excluded from reporting requirements:

> Clause 132 broadly aligns with reporting requirements that are applied to control order information in Australia's current regime. It is intended to recognise that control orders have been sought and made only rarely, with the effect that it is uncommon for there to be more than a limited number of control orders in force at any given time. If the Minister were required to contemporaneously report publicly on control orders, and only a limited number of persons are subject to control orders at that time, annual reporting may effectively reveal that a particular person who is subject to a control order is or is not also subject to covert surveillance.[48]

4.45 The Law Council of Australia said that historically, ASIO has been excluded from reporting requirements for similar reasons and considers that such consideration could apply to ASIO reporting requirements:

> … 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. 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).[49]

4.46 The IGIS invited the PJCIS to consider requiring ASIO to report publicly on its use of the IPO regime, noting that this approach contrasts with international approaches and the reporting requirements of domestic law enforcement agencies:

---

46 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 128, 130 and 131.

47 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, proposed sch. 1 cl. 129 and 132.

48 Explanatory Memorandum, p. [82].

49 Law Council of Australia, *Submission 28*, p. 41.

> The Bill amends the ASIO Act to require that ASIO include a range of statistics on its use of the IPO regime in its annual report. Although unclassified portions of ASIO's annual report are required to be tabled in the Parliament, the Minister, on the Director-General of Security's advice, may make such deletions as he or she considers necessary in order to avoid prejudice to security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs, or the privacy of individuals. Statistics on ASIO's use of warrants and other powers are generally excluded from the public version of the report.
>
> This approach contrasts with provisions for law enforcement agencies, for which the Bill includes a specific provision requiring statistics on each agency's use of the IPO regime to be included in a public annual report that is tabled in the Parliament and a scheme for reconsideration of a decision that it is necessary to exclude some information. If it was considered necessary to allow the exclusion of certain information from ASIO's public reporting, the proposed scheme for reconsideration of such decisions for law enforcement could be extended to ASIO's reporting requirements.
>
> The absence of public statistical reporting for ASIO contrasts with international approaches; for example, in the United Kingdom, where a wide range of statistics on the use of investigatory powers, including by intelligence agencies, is reported in the annual report of the Investigatory Powers Commissioner's Office.[50]

4.47 In response to this suggestion, the Department of Home Affairs said that such an amendment would conflict with the requirements of the current domestic regime[51] and could provide insight on the use of the framework to persons of interest in ASIO investigations:

> The inclusion of statistics in an unclassified annual report would highlight specifically how much ASIO utilises the international production order framework. This may permit inferences to be drawn as to how ASIO utilises the proposed international production order framework, and may assist persons of interest to change their behaviour due to public reporting on the use of investigatory powers.[52]

4.48 As outlined in Chapter 2, the agreement between the United States and the United Kingdom contains a requirement that the issuing country shall

---

50 IGIS, *Submission 27*, p. 15.

51 Department of Home Affairs, *Supplementary Submission 10.1*, p. 14.

52 Department of Home Affairs, *Supplementary Submission 10.1*, p. 33.

provide a report of the requests it has made each year to the receiving country.[53]

4.49 In addition, the Bill requires the Commonwealth Ombudsman to provide a report to the Minister at the end of each financial year detailing inspection outcomes:

> The Ombudsman is required to provide a written report to the Minister for Home Affairs as soon as practicable after the end of each financial year about the inspection of records of relevant agencies and the ADA. The report must then be tabled by the Minister in each House of Parliament. The Ombudsman also has the ability to provide a report to the Minister at any time about the outcomes of an inspection, and must do so if requested by the Minister. The Ombudsman may also include any information in the report regarding contraventions of the IPO scheme by a relevant agency or the ADA (clause 150).[54]

4.50 The IGIS is also required to report publicly each year on the outcome of its inspections:

> Under the IGIS Act, the IGIS is required to report on its inquiries and has the discretion to do so in relation to inspections (see Part II, Division 4 of the IGIS Act). These arrangements will apply to IGIS' oversight of ASIO's use of the IPO framework. AGD considers that these oversight arrangements are appropriate and will keep them under review after the framework is implemented.[55]

Notice to the subject of an IPO

4.51 Several submitters to the inquiry raised the issue of providing notice to a subject that their data has been accessed, even where such notice is delayed to prevent destruction of evidence or prejudice to an investigation.[56] The International Civil Liberties and Technology Coalition said that the Bill does

---

53 *Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland 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), art. 12.

54 Attorney-General's Department, *Submission 16*, p. 16.

55 Attorney-General's Department, *Submission 16*, p. 17

56 Mr Norman Barbosa, Assistant General Counsel, Law Enforcement and National Security, Microsoft Australia, *Committee Hansard,* Canberra (evidence taken via teleconference), 13 May 2020, pp. 2–3. See also DIGI, *Submission 23*, p. 5.

not provide certainty for designated communications providers to notify an individual that their data is being accessed:

> In general, users have a universal right to notice. The International Production Orders Bill does not provide any requirement, or even mechanism, for government officials to notify data subjects of requests. We would note that unlike the U.K.'s Investigatory Powers Act, the International Production Orders Bill does not explicitly prohibit providers from providing notice to their customers.[57]

4.52 The Synod of Victoria and Tasmania, Uniting Church in Australia said that notifying the subject of an investigation that their data is being accessed carries a risk of destruction of evidence:

> The Synod is concerned by the views of the International Civil Liberties and Technology Coalition that suspected offenders of severe crimes should be tipped off they are under investigation. The Coalition provides no consideration of the dangers this poses to victims, witnesses or the likelihood that an offender will be able to destroy evidence as a result. Often offenders will use multiple platforms and communication devices. Law enforcement agents may seek an IPO on over one platform. Even if data on this platform were to be protected from destruction, after being tipped off, the offender might be able to destroy evidence on other platforms. The Coalition makes only a passing reference in their submission to delaying tipping off a suspected offender "where necessary to protect an on-going investigation." However, they do not refer to any concerns for victims or witnesses.
>
> The Sheriff's office in Brevard County in Florida reported they had to force entry into a house to stop an alleged child sex offender from continuing to run CDs through a shedder after they were tipped off by an ICT technology corporation that they were under investigation.
>
> As an example, there is a very real danger that paedophiles will seek to intimidate victims and destroy evidence if tipped off that an IPO has been issued. Paedophiles often operate in large online networks that assist each other. Thus, the Committee should strongly avoid recommending any measures that would allow a suspected paedophile they are under investigation. Any process that would tip off a suspected paedophile may enable them to alert others in their network and possibly seek assistance from others in the network to cover up their activities.[58]

---

57 International Civil Liberties and Technology Coalition, *Submission 9*, p. 3.

58 Synod of Victoria and Tasmania, Uniting Church in Australia, *Submission 24*, p. 10.

4.53 Ms Lucie Krahulcova, International Civil Liberties and Technology Coalition said that notice should occur to allow the subject of an order to advocate for their interests:

> In practice we have to look at what happens here and the sort of interests that are at play— whether it's a law enforcement agency or an intelligence agency almost directly submitting an IPO, for instance for telecommunications data. The discretion doesn't have to be exercised. They can go direct. There's no intervention on behalf of the individual. There should be an interactive notification for individuals. But I think you have to look at the weighing mechanism, when a warrant like that is presented, of who is representing the individual. Often this ends up being companies just because they have the legal team and they are bound by consumer legislation in different jurisdictions to respect individuals' rights. As I flagged, my concern is that this sort of mechanism that the individual has over the company has been removed. I think that's a huge area of concern. I was part of the EU negotiations on very similar mechanisms for several years when I worked in Brussels. From my perspective, companies being in a position to reject requests is not a perfect system, but it is often the last frontier for individuals' rights, because there isn't a human rights body or an independent reviewer who is part of that mechanism. Again, I recognise that there are public interest monitors who would be engaged in several states as a part of that process. However, that sort of neutral or independent reviewer should be part of every evaluation that happens, because there is such a power discrepancy between an agency going directly or an agency with the Attorney-General's signing-off going directly to the company, where the company is not liable to the user. It presents a really tragic power paradigm.[59]

Record-keeping requirements and retention of data

4.54 The Bill requires an agency to destroy records of intercepted and stored communications data when it is no longer required for a legitimate purpose, with an exception for telecommunications data mirroring domestic legislation.[60]

4.55 The Law Council of Australia said that information that is intercepted or stored communications must be deleted where it is determined that the retention of information is no longer required:

---

59 Ms Lucie Krahulcova, International Civil Liberties and Technology Coalition, *Committee Hansard*, Canberra (evidence received via teleconference), 13 May 2020, p. 13.

60 Department of Home Affairs, *Supplementary Submission 10.1*, p. 15.

> 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. The Explanatory Memorandum suggests that Clause 140 'will ensure that records of sensitive, personal communications are not kept by agencies where no longer needed'.[61]

4.56 The Law Council of Australia and the IGIS raised concerns that the requirement to review materials obtained through the IPO regime to ensure its retention is consistent with a legitimate purpose is not adequately provided for in the Bill.[62]

4.57 The Law Council of Australia recommended that a statutory requirement for review be incorporated into the Bill:

> 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.
>
> 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.[63]

4.58 The Law Council said that the evidence does not support the exclusion of telecommunications data from the requirement for review:

---

61 Law Council of Australia, *Submission 28*, p. 53.

62 See Law Council of Australia, *Submission 28*, p. 54; IGIS, *Submission 27*, pp. 18–19.

63 Law Council of Australia, *Submission 28*, p. 54.

> … 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.[64]

4.59 In relation to the requirement to retain records, the IGIS suggested that amending the requirements to retain records would assist the IGIS in its oversight function:

> The record retention requirements for ASIO's domestic telecommunications warrants are regulated by a 2016 determination of the National Archives under the *Archives Act 1983*. The determination specifies that records related to warrants for security intelligence collection may be destroyed from ten to 150 years after last action or must be retained indefinitely (depending on the class of record). IGIS notes that ASIO's recordkeeping in respect of its current warrant framework is of a high standard, and anticipates that similar standards would be maintained in respect of the IPO regime.
>
> Nonetheless, IGIS considers that oversight is greatly assisted by clear legislative requirements for the retention of information. The Bill's requirement that ASIO retain certain records for three years could be enhanced by adding an additional requirement to provide that certain records must be kept for three years, or for as long as any of the data obtained under an IPO is retained, whichever is the longer. This would ensure that there is a clear accountability record for data received under an IPO that is subsequently retained.
>
> However, IGIS also notes that not all documents that must be prepared under the Bill are required by clauses 135 and 136 to be kept. For example, the documentation provided to the Attorney-General seeking consent to an application for an IPO, and a record of whether the Attorney-General consented to that application or refused consent, is not required to be retained.
>
> IGIS considers that legislating a specific list of records that are required to be kept carries a risk that not all records associated with the administration of the IPO regime would be captured. The Committee may therefore consider it preferable that the Bill contain a general record retention obligation that requires ASIO to keep all relevant records for IGIS inspection. IGIS notes that the inspection regime undertaken by IGIS for 'legality and propriety' looks to

64 Law Council of Australia, *Submission 28*, p. 56.

a much wider range of information than the specific regime prescribed for inspections by the Ombudsman.[65]

Review of the overall IPO regime

4.60 The Bill does not presently provide a statutory review mechanism for the Independent National Security Legislation Monitor (INSLM) or the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

4.61 The Law Council recommended that the INSLM's enabling legislation be reviewed to incorporate a statutory review provision:

> 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, or a one-off statutory review, as is the case for other recent amendments including the TOLA Act.
>
> 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 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.
>
> 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. 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.
>
> 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.[66]

---

65 IGIS, *Submission 27*, pp. 18–19.

66 Law Council of Australia, *Submission 28*, pp. 49–50.

4.62 The Law Council of Australia said that the PJCIS's existing oversight functions may not provide for scrutiny of the regime in its entirety:

> 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; 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. 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.
>
> 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); 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).
>
> 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.

4.63 The Department of Home Affairs said that any statutory review undertaken by the INSLM or the PJCIS should occur 'a significant period after the operationalisation of the first designated international agreement.'[67]

---

[67] Department of Home Affairs, *Supplementary Submission 10.1*, p. 35.

4.64 In relation to the oversight responsibilities of the PJCIS, the Department of Home Affairs said that the IPO regime would be subject to extensive oversight arrangements:

> Agencies' use of the international production order framework and the Australian Designated Authority will be subject to comprehensive operational oversight by the Commonwealth Ombudsman and IGIS.
>
> The Department notes that the Committee has existing functions under section 29 of the Intelligence Services Act 2001 to review the administration and expenditure of ASIO and matters relating to ASIO that have been referred to the Committee, and to monitor and review legislation referred to it
>
> Currently the Australian Designated Authority is not required to provide briefings on request to the PJCIS. Pursuant to section 30 of the Intelligence Services Act 2001, it would be open for the PJCIS to request briefings from the Commissioner of the AFP or Director-General of Security on the AFP and ASIO's use of the international production order framework to support their functions in relation to the Australian Intelligence community.[68]

Committee comment

4.65 The Committee notes the role of the ADA is designed to reflect the current authorisation processes associated with the mutual legal assistance regime, and agrees that the Attorney-General's Department has the relevant subject matter knowledge to manage the process.

4.66 The Committee notes the concerns of submitters in relation to potential for civil penalties to apply to instances of non-compliance with the conditions of an international production order. The Committee expects that the Department of Home Affairs will exercise this power judiciously and as a tool of last resort.

4.67 In addition, the Committee notes the views of submitters in relation to the use of evidentiary certificates. Noting that adducing the evidence of compliance with an international production order can be challenged by the defendant in the event of prosecution, and noting that the elements of a conclusive evidentiary certificate should be confined to non-controversial matters, the Committee is not persuaded by the Law Council of Australia that there is no place for a conclusive evidentiary certificate in the international production orders process.

---

68 Department of Home Affairs, *Supplementary Submission 10.1*, p. 35.

4.68 The Committee notes with concern the evidence provided by the Commonwealth Ombudsman regarding resource matters. As articulated in Chapter 1, the Committee considers that robust oversight arrangements are essential when considering intrusive powers, and that resourcing limitations can have a significant impact on this important assurance role. The Committee therefore recommends that the Government should ensure the Commonwealth Ombudsman has sufficient resources to oversee the powers provided by the Bill.

Recommendation 16

4.69 The Committee recommends that the Australian Government ensure that the Commonwealth Ombudsman has sufficient resources to enable effective oversight of the proposed powers granted by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

4.70 Though the Inspector-General of Intelligence and Security has not identified resourcing concerns as a result of its oversight of the international production orders regime, the Committee considers that the Australian Government should continue to ensure that the resourcing levels of the Office of the Inspector-General of Intelligence and Security are appropriate.

Recommendation 17

4.71 The Committee recommends that the Australian Government continue to ensure that the Inspector-General of Intelligence and Security is given appropriate resources to enable effective oversight of the proposed powers granted by the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

4.72 The Committee considers that the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security should have unambiguous access to the information required to oversee access to the regime.

4.73 The Committee therefore supports the recommendations proposed by the IGIS and the Law Council of Australia to allow full and unimpeded cooperation between the ADA, the Commonwealth Ombudsman and the IGIS.

Recommendation 18

4.74 The Committee recommends that the proposed Schedule 1, Division 4 be amended to include an express provision for the Inspector-General of Intelligence and Security, or an official of the Inspector-General of Intelligence and Security, to access the register of international production orders in connection with its oversight responsibilities.

Recommendation 19

4.75 The Committee recommends that proposed Schedule 1, Clause 153 be amended to allow international production order information to be used, recorded or disclosed for the purposes of an official of the Inspector-General of Intelligence and Security exercising their duty as an official.

Recommendation 20

4.76 The Committee recommends that the *Inspector-General of Intelligence and Security Act 1986* be amended to allow for officials of the Inspector-General of Intelligence and Security to share information relating to the international production orders regime with members of the Office of the Commonwealth Ombudsman and members of the Attorney-General's Department where sharing such information is connected to the roles and duties of the member of the organisation.

4.77 The Committee was not convinced that aggregated public reporting from ASIO, with the ability to withhold information should it have the potential to identify a party involved in an international production order, would prejudice an ASIO investigation.

4.78 The Committee therefore considers it would be appropriate to recommend that ASIO provide public statistics on the use of the regime where the data would not inadvertently identify the subject of an investigation.

Recommendation 21

4.79 The Committee recommends that:

- **the *Australian Security Intelligence Organisation Act 1979* be amended to provide that a report made under proposed subsection 94(2BBA) should form part of the Australian Security Intelligence Organisation's unclassified annual report; and**

- **the proposed subsection provide that the recommended statistics would not be provided where the Director-General of Security considers that providing such statistics would prejudice Australia's national security, or prejudice a national security investigation.**

4.80 The Committee notes the conditions of the agreement between the United Kingdom and the United States requiring data to be provided regarding incoming IPOs. The Committee expects that such information will be captured in the designated international agreement and does not propose any additional recommendations in relation to the material.

4.81 The Committee notes the views of submitters in relation to notice provisions. The Committee considers there are significant risks in allowing notice to be given to the subject of an investigation, especially noting the propensity of parties to work in groups.

4.82 However, the Committee acknowledges the evidence from the International Civil Liberties and Technology Coalition that designated communications providers are not always best placed to contest an international production order application from the position of an individual. The Committee considers that the Independent National Security Legislation Monitor's recommendation – as discussed in Chapter 2 and Chapter 3 – regarding the establishment of an investigatory powers division within the Administrative Appeals Tribunal could be an appropriate mechanism to address these concerns.

4.83 The Committee notes the evidence provided by the IGIS relating to document retention. As stated above, the Committee supports the IGIS's ability to have access to relevant records it needs to complete its oversight role.

4.84 Therefore the Committee supports amendments to require ASIO to retain production orders information for the length of time the order is in place,

and to require ASIO to retain extrinsic material to a request that would assist the IGIS in overseeing ASIO's compliance with the regime.

Recommendation 22

4.85 The Committee recommends that proposed Schedule 1, Clause 135 and 136 be amended to require the Australian Security Intelligence Organisation to:

- **retain a copy of a particular document for three years, or for as long as any of the data obtained under an international production order is retained, whichever is the longer; and**

- **retain all relevant materials supporting an application for international production order for this period.**

4.86 As discussed in Chapter 2, the Bill is designed to operate as a framework to allow designated international agreements to prescribe relevant details in line with the laws of like-minded countries that Australia is seeking an agreement with. As a consequence, the Committee considers that it is necessary to provide for a statutory review to evaluate the effectiveness of the regime once a designated international agreement is in place.

4.87 The Committee acknowledges the advice of the Department of Home Affairs, and considers that such a statutory review would need to commence after a designated international agreement had time to operate, and therefore recommends that a statutory review be commenced on the earlier of 3 years after the date of the first designated international agreement coming into effect or 5 years following the commencement of the provisions of the Bill.

Recommendation 23

4.88 The Committee recommends that the Bill be amended to require the Parliamentary Joint Committee on Intelligence and Security to commence a review on the effectiveness and continuing need for an international production orders regime on the earlier of the date that is:

- **three years after the date on which the first designated international agreement comes into force; or**
- **five years after the commencement of the proposed Schedule 1 of the *Telecommunications (Interception and Access) Act 1979*.**

4.89 The Committee acknowledges that the Bill will provide significant assistance to agencies to investigate and prosecute serious crimes, monitor compliance with control orders, and maintain Australia's national security. The Committee supports the passage of the Bill following implementation of these recommendations.

Recommendation 24

4.90 The Committee recommends that, following implementation of the recommendations in this report, the Bill be passed by Parliament.

Senator James Paterson
Chair

A. List of submissions

1 Australian Privacy Foundation

2 Australian Commission for Law Enforcement Integrity

- 2.1 Supplementary to submission 2

3 Commonwealth Ombudsman

- 3.1 Supplementary to submission 3

4 *Name Withheld*

5 Corruption and Crime Commission (WA)

6 Mr Peter Jardine

7 Mr Eric Wilson

- 7.1 Supplementary to submission 7
- 7.2 Supplementary to submission 7

8 Western Australia Police Force

9 International Civil Liberties and Technology Coalition

10 Department of Home Affairs

- 10.1 Supplementary to submission 10

11 Mr. Peter Swire

12 NSW Police Force

- 12.1 Supplementary to submission 12
- 12.2 Supplementary to submission 12

13 Police Federation of Australia

14 Communications Alliance

15 The Allens Hub for Technology, Law and Innovation

16 Attorney-General's Department

17 Australian National University Law Reform and Social Justice Research Hub

18 Law Enforcement Conduct Commission

19 Mr Thomas McBride

20 BSA | The Software Alliance

- 20.1 Supplementary to submission 20

21 Google

22 Commonwealth Director of Public Prosecutions

23 Digital Industry Group Incorporated

24 Synod of Victoria and Tasmania, Uniting Church in Australia

25 ACT | The App Association

26 Australian Security Intelligence Organisation

- 26.1 Supplementary to submission 26
- 26.2 Supplementary to submission 26

27 Inspector-General of Intelligence and Security

- 27.1 Supplementary to submission 27

28 Law Council of Australia

- 28.1 Supplementary to submission 28

29 Microsoft

30 Capital Punishment Justice Project

31 Australian Federal Police

32 The Australian Industry Group

B. Witnesses appearing at public hearings

Tuesday, 12 May 2020

Committee Room 1R1 (witnesses appeared via teleconference)
Canberra

Inspector-General of Intelligence and Security

- The Hon Margaret Stone AO FAAL, Inspector-General of Intelligence and Security
- Mr Jake Blight, Deputy Inspector-General

Office of the Commonwealth Ombudsman

- Mr Michael Manthorpe PSM, Commonwealth Ombudsman
- Mr Paul Pfitzner, Acting Deputy Ombudsman
- Ms Louise Cairns, Director National Assurance and Audit

Law Council of Australia

- Ms Pauline Wright, President
- Dr David Neal SC, Co-Chair, National Criminal Law Committee
- Dr Sarah Pritchard SC, Chair, National Human Rights Committee
- Dr Natasha Molt, Director of Policy, Policy Division

Wednesday, 13 May 2020

Committee Room 1R1 (witnesses appeared via teleconference)
Canberra

Microsoft Australia

- Mr Norman Barbosa, Assistant General Counsel, Law Enforcement and National Security
- Mr David Masters, Corporate Affairs Director

BSA The Software Alliance

- Mr Brian Fletcher, Director-Policy, APAC

International Civil Liberties and Technology Coalition

- Ms Sharon Bradford Franklin
- Ms Lucie Krahulcova

Australian Commission for Law Enforcement Integrity

- Ms Jaala Hinchcliffe, Integrity Commissioner
- Ms Nikki Bensch, Director Legal

NSW Police Force

- Assistant Commissioner Michael Fitzgerald APM, Commander, Forensic Evidence & Technical Services Command

Thursday, 14 May 2020

Committee Room 1R1 (witnesses appeared via teleconference)
Canberra

Australian Security Intelligence Organisation

- Mr Peter Vickery, Deputy Director-General, Enterprise Service Delivery

Australian Federal Police

- Deputy Commissioner Karl Kent, Specialist and Support Operations
- Deputy Commissioner Ian McCartney, Investigations

Department of Home Affairs

- Mr Anthony Coles, First Assistant Secretary, Law Enforcement & Intelligence Policy
- Mr Andrew Warnes, Assistant Secretary, National Security Policy Branch
- Mr Nathan Whiteman, A/g Director, Cross-Border Data & Cybercrime Section, National Security Policy Branch

Attorney-General's Department

- Ms Susan Robertson, First Assistant Secretary, International Division
- Ms Erin Wells, A/g Assistant Secretary, International Division