April | 2020

Australian Government
Attorney-General's Department

Parliamentary Joint Committee on Intelligence and Security

Review into the effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

SUBMISSION

Attorney-General's Department

Table of Contents

Overview of submission

1. The Commonwealth Government Attorney-General's Department (AGD) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security's review into the effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill), for the Committee's consideration.

2. The Bill will strengthen international crime cooperation by streamlining the system of sharing communications data essential for criminal prosecutions and investigations. The Bill contains important safeguards for data protection and human rights and provides for independent oversight of the new International Production Order (IPO) regime established by the Bill by the Commonwealth Ombudsman (Ombudsman) and the Inspector-General of Intelligence and Security (IGIS).

3. This submission addresses those policy aspects of the Bill that are relevant to AGD's responsibilities. These include:

   - the interaction of the proposed IPO regime with the existing international crime cooperation arrangements relating to mutual legal assistance (MLA) under the *Mutual Assistance in Criminal Matters Act 1987* (MACMA)
   - procedures for issuing IPOs in Australia by a judge, magistrate or Administrative Appeals Tribunal (AAT) member in their respective *persona designata* functions, as well as the Attorney-General's role in consenting to applications for IPOs relating to national security
   - the establishment of the Australian Designated Authority in the IPO process
   - human rights safeguards, including death penalty assurances
   - data protection and safeguards contained in the *Privacy Act 1988* (Privacy Act)
   - the admissibility of evidence obtained under IPOs in Australian courts
   - oversight of the IPO process by the Ombudsman and the IGIS.

4. Unless otherwise specified, all references to clauses, subclauses or Parts are references to provisions of Schedule 1 to the TIA Act, which is to be inserted by clause 43 of Schedule 1 to the Bill.

Advantages over existing crime cooperation arrangements

5. By way of brief summary, the Bill enables Australian law enforcement and the Australian Security and Intelligence Organisation (ASIO) to apply to an Australian judge, magistrate or AAT member for an IPO. The Bill creates three broad categories of IPOs for the following purposes:

   - enforcement of the criminal law (Part 2)
   - monitoring of a person subject to a control order (Part 3)

- national security (Part 4).

6. Under each of these categories, agencies may seek different forms of communications data for the purposes of carrying out investigations or undertaking legal proceedings in relation to serious crimes. These include interception of live communications, stored communications data (content data), and telecommunications data (data about a communication or account holder).

7. Once an IPO is issued, the ADA reviews it for compliance with the relevant Designated International Agreement (DIA) and, if the IPO is found compliant with the DIA, subsequently transmits it directly to a specified Designated Communications Provider (DCP) in the relevant foreign country. The DCP then sends the communications data sought in the IPO either directly or indirectly (through the ADA) to Australian authorities. The same process will operate in reverse for orders Australia receives from the relevant foreign country.

8. The biggest advantage of the Bill will be the increased speed at which relevant data can be shared between crime cooperation partners. This is because Australian IPOs will be given directly to the foreign DCP rather than via the foreign government.
The Department of Home Affairs' (DoHA) departmental submission to the Committee sets out the policy rationale for the Bill, including reasons why the existing MLA regime is limited in its capacity to effectively support the timely sharing of communications data for the purposes of criminal investigations and prosecutions in the digital, globalised age.

9. AGD has seen a significant rise in the number of outgoing MLA requests from Australian agencies for communications data over the last 10 years, particularly in the United States (US) where most of the world's largest communications and technology companies are based. Timeframes for processing MLA requests vary, but for this type of information are on average between 10 and 12 months. Reasons for delays include the time needed to fulfil statutory requirements associated with MLA requests (such as each country's domestic legal requirements concerning search warrants, or requirements of the requesting country as to the form in which material must be provided by the requested country). These extended timeframes mean that the value of the information for the purposes of criminal investigations or prosecutions may be lost.

10. The proposed new IPO process will not replace the MLA process. Rather, it would be complementary to MLA and other crime cooperation channels, including police-to-police assistance and the ability for communications service providers to provide information to law enforcement or national security agencies voluntarily, at their discretion. The benefit of the proposed new regime would be that the provision of the material under an IPO could be admissible in court (see the discussion on evidentiary certificates at paragraphs 61-64 below), noting that currently material obtained from foreign communications providers is admissible only where it has been obtained pursuant to an MLA request. The Bill will also allow relevant information obtained under an IPO to be used to support an Australian extradition request.

11. The MLA process already allows for information of the kind covered by the Bill to be obtained from another country where that country's laws permit. MLA also allows for Australia to provide information of the kind covered by the Bill to other countries (with the exception of live intercept material) where that information is sought for the purposes of a criminal matter. The IPO process will enable this to be done more expeditiously. Further, as is also the case for information obtained through MLA, the Bill will also amend relevant legislation to enable Australia to share information obtained in response to an IPO with the International Criminal Court and with international war crimes tribunals, as appropriate under the Bill and the particular DIA. This will strengthen Australia's compliance with existing international law cooperation obligations.

Issuing IPOs – accountable and independent decision making

12. The Bill provides for a range of independent decision-makers to authorise the use of interception activities, as well as access to stored communications and telecommunications data. The Bill sets out the process for Australian law enforcement agencies or ASIO to apply to a judge, magistrate or nominated AAT member for an IPO.

13. As noted in paragraph 5 above, under the Bill IPOs may be issued for purposes of enforcement of the criminal law, for the purposes of monitoring compliance with control orders, and for national security purposes. For each of these purposes, the Bill provides for three types of IPOs, relating to interception, stored communications and telecommunications data.

14. Under Parts 2 and 3 of the Bill, for purposes in connection with the investigation of an offence of a serious nature or the monitoring of a person subject to a control order, an *eligible judge* (defined in clause 14) or *nominated AAT member* (defined in clause 15) is able to issue IPOs relating to interception. For these same purposes, an issuing authority is able to issue IPOs relating to stored communications and telecommunications data. An *issuing authority* means a judge, magistrate or AAT member who satisfies certain eligibility criteria (clause 16).

Persona designata functions

15. Under the TIA Act, certain functions are performed by authorised judges, magistrates and members of the AAT acting in their personal capacity (*persona designata*). When a judge, magistrate or member of the AAT performs certain *persona designata* functions, they are not exercising the formal judicial or administrative powers of the court or tribunal of which they are a member, but are acting as an independent decision-maker.

16. The conferral of *persona designata* powers recognises that federal judges, magistrates and AAT members are well-placed to conduct dispassionate assessments of evidence, and to balance the rights and liberties of individuals with the interests of law enforcement agencies. The Bill ensures that the system for issuing IPOs will be applied with fairness and accountability owing to the skill, experience and independence of the individuals appointed.

17. 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.

18. AGD notes that Commonwealth legislation currently confers *persona designata* functions on judges, magistrates and AAT members through a number of provisions across a range of legislation. The powers and functions that judges, magistrates and AAT members perform, including the eligibility requirements for being authorised and the criteria to exercise a power or function, vary across legislation.

19. The power to issue a warrant, including for the purpose of telecommunications interception and access to stored communications, is a common function exercised by a judge, magistrate or AAT member in their personal capacity.

20. *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 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.

21. In general, the incompatibility test will be satisfied where the exercise of powers vested in judges:

    - is sufficiently independent from the functions of the legislature or the executive
    - is exercised independently of the instruction, advice or wishes of the legislature or the executive
    - does not impose such a workload so as to affect the performance of the judge's official functions for an indefinite period of time.

    The incompatibility test, and by extension evaluating the appropriateness of the conferral of *persona designata* powers*,* is also enlivened when considering the conferral of powers on magistrates.

22. 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.

23. 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.

24. 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.

25. 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.

26. The Bill contains a broad range of matters which must be considered before issuing an IPO, including the impact on the privacy of affected individuals, and any other matters which the authorised judge, magistrate or AAT member considers relevant. This ensures that the rights of affected individuals are always considered, and that the decision to issue an IPO is independent from the functions of law enforcement agencies.

IPOs for national security purposes

27. Under Part 4 of the Bill, ASIO will be able to seek an IPO for national security purposes to access information that has been obtained via interception, stored communications data or telecommunications data.

28. All national security IPOs must be independently authorised by a nominated AAT Security Division member. Prior to applying to the AAT Security Division for an IPO related to interception or stored communications, ASIO must first obtain the Attorney-General's consent to the application being made. The Attorney-General is not required to consent to applications for IPOs that only relate to telecommunications data. These differing consent requirements reflect the more intrusive nature of requests for interception and stored communications compared to telecommunications data.

Interception and access to stored communications

29. Information that may be accessed under interception and stored communications IPOs will include the content of communications, such as messages and voice calls, including those made over the internet (for example via mobile applications) and related telecommunications data. Interception IPOs will compel a DCP to intercept live communications in transit whereas stored communications IPOs capture sent and received communications at rest and still held by the DCP. Given the intrusiveness of both access to stored communications and interception activities and the relation to security, the Attorney-General will be required to consent to those IPOs before an application is made to an AAT Security Division member.

30. Under the Bill, it is proposed that prior to making an application to obtain an IPO for intercepted communications or disclosure of stored communications, ASIO would be required to first obtain the Attorney-General's consent to the application being made (subclauses 83(6) and 92(6) respectively). ASIO (the Director-General or Deputy Director-General of Security, or an ASIO employee who is authorised in writing by the Director-General of Security) would then apply to a nominated AAT Security Division member to issue the IPO.

31. In order to give consent for an IPO request to be made to an AAT Security Division member, the Attorney-General would need to be satisfied that:

    - there are reasonable grounds for suspecting that the individual who is being targeted through an IPO is engaged in, or is likely to engage in, activities prejudicial to security
    - the information that would likely be obtained from the IPO would be likely to assist ASIO in carrying out its function of obtaining intelligence relating to security.

32. 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.

33. The Bill provides that the Attorney-General's consent would ordinarily be given in writing, but permits consent to be provided orally in urgent circumstances (subclauses 83(9) and 92(8)). This would enable ASIO to respond efficiently to time critical threats, and is similar to the procedures for authorisation of domestic warrants in the TIA Act and other IPOs under the Bill (telephone applications can be made in urgent circumstances). Where the Attorney-General provides oral consent to an application, ASIO must follow with a written report to the Attorney-General setting out the urgent circumstances and whether the IPO application was granted or refused by the AAT Security Division member. Importantly, the process would also ensure that even in emergency situations the Attorney-General will retain control over ASIO's application for IPOs.

34. The requirement for the Attorney-General to consent to ASIO's applications for IPOs reflects the Attorney-General's longstanding role in authorising intelligence collection in Australia. It provides the Attorney-General with oversight over the intended use of intrusive powers for national security purposes, and establishes ministerial accountability, a central principle of Australia's Westminster parliamentary system. The additional requirements for the Attorney-General to consent to ASIO applications for IPOs prior to authorisation by a nominated AAT Security Division member provides a second tier of accountability and independence.

Access to telecommunications data

35. Information that can be accessed under an IPO request for telecommunications data is less intrusive than information that can be accessed under IPO requests for interception or access to stored communications. Telecommunications data is not communications content. Rather, telecommunications data includes information about a communication (such as the telephone number of the recipient, time and date of the communication) and information about the account holder (such as name, billing details and address).

36. Under the Bill, it is proposed that to obtain an IPO to access telecommunications data, ASIO (the Director-General or Deputy Director-General of Security, or an ASIO employee who is authorised in writing by the Director-General of Security) will apply to a nominated AAT Security Division member to issue the IPO (clause 101). The Attorney-General's consent is not required. This is consistent with the existing legislative arrangements where the Attorney-General does not play a role in authorising ASIO to access to domestic telecommunications data (Division 3, Chapter 4 of the TIA Act).

The establishment of an Australian Designated Authority (ADA)

37. The Bill establishes an ADA to promote the effective functioning of the IPO regime, including through the ADA's role as an intermediary between agencies in Australia and foreign DCPs. The ADA would fulfil a central role in ensuring IPOs are utilised consistently with DIAs, including checking each IPO for compliance with the relevant DIA before transmitting the IPO to the relevant DCP, and undertakes activities to support accountability including maintaining records, facilitating auditing by the Ombudsman and reporting to the Minister for Home Affairs. In addition, the ADA may undertake any other functions agreed in a DIA.

38. The Bill provides that the AGD Secretary will be the ADA, with the ADA functions and powers able to be delegated to AGD officers. AGD is well placed to undertake the ADA function and perform oversight functions in relation to the IPO regime due to AGD's existing role in managing the MLA process for Australia and the department's separation from law enforcement and security agencies in the Home Affairs portfolio.

39. 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, 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.

40. 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. Further, Part 6 of the Bill provides that where an agency has revoked an IPO it has obtained, the agency must provide the instrument of revocation to the ADA, and the ADA must notify the relevant DCP. The IPO would cease to be in force from the time the DCP is notified of the cancellation or revocation of the IPO.

41. Under Part 9, the ADA has a number of reporting and record-keeping requirements, including the provision of an annual report to the Minister for Home Affairs, the establishment of a register of IPOs, and keeping other records associated with IPOs (clauses 130 and 137-139).

Safeguards – human rights and data protection/privacy

Death penalty safeguards

42. Australia maintains a long-standing, bipartisan policy of opposition to the death penalty, in all circumstances, for all people. As with MLA, it is feasible that Australia may wish to make agreements with countries that retain the death penalty for certain serious offences. Accordingly, 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 (clause 3).

43. 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.[1]

44. While the Bill provides the mechanism for international agreements to be designated by regulation (clause 3), before getting to this point agreements will be subject to considerable Parliamentary scrutiny through the treaty-making process. It is appropriate that consideration about death penalty matters and the adequacy of any assurances received from the foreign government are considered during this process. Once this process is complete, the proposed agreement would be subject to regulation-making processes. Regulations which seek to prescribe a DIA for the purposes of the Bill will be legislative instruments and, accordingly, subject to the process of disallowance by members of Parliament.

[1] Under section 8 of the MACMA, the Attorney-General is authorised to refuse to provide MLA to a foreign country in support of a death penalty matter. Depending on the circumstances of the criminal matter this ground of refusal is either mandatory (subsection 8(1A)) or discretionary (subsection 8(1B)). Subsection 8(1A) relevantly provides that where a person has been arrested, detained, charged or convicted in relation to a death penalty offence, the Attorney-General must refuse to grant assistance requested by a foreign country in relation to that matter unless the Attorney-General is satisfied it is appropriate to grant the assistance, having regard to any 'special circumstances' of the case. The Explanatory Memorandum to the Mutual Assistance in Criminal Matters Legislation Amendment Bill 1996 (at paragraphs 60-61) provides that 'special circumstances' exist if the evidence sought is exculpatory or if the foreign country has given an assurance concerning the death penalty, for instance that it will not be sought, or if sought will not be imposed, or if imposed will not be carried out.

Other safeguards

45. There are various safeguards in section 8 of the MACMA 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.

Data protection and privacy

46. We draw to the Committee's attention the following aspects of the Bill that help protect the privacy of individuals.

International law obligations

47. Australia has human rights obligations not to subject individuals to arbitrary or unlawful interference with their privacy, family, home or correspondence (Article 17 of the International Covenant on Civil and Political Rights). 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.

48. In light of the safeguards outlined below as well as the assessment made by DoHA in the explanatory memorandum to the Bill, AGD supports the view that the Bill provides adequate statutory safeguards against arbitrary or unlawful interference with privacy and would be permissible under international human rights law.

Safeguards in IPOs

49. An IPO could direct a foreign communications provider to provide personal information of Australian citizens living within Australia and abroad (apart from those living in the relevant foreign country) as well as individuals who are not Australian citizens, including those living within Australia. In deciding whether to issue an IPO under Part 2 of the Bill, the decision-maker must have regard to how much the privacy of any person would be interfered with, and also take into account the availability and use of other means to achieve the same law enforcement purpose. This safeguard ensures that only information that is reasonably required to achieve the policy objective is collected, used or disclosed.

50. For IPOs relating to the monitoring of compliance with control orders under Part 3 of the Bill, the decision-maker must also consider whether intercepting communications would be the method that is likely to have the least interference with any person's privacy. This is an

additional privacy safeguard, as these IPOs can be issued for monitoring a person in order to protect the public from a terrorist act or prevent support for a hostile act overseas, and not necessarily because the person is currently suspected of a specific serious offence.

51. For IPOs relating to national security under Part 4 of the Bill, the consent of the Attorney-General is required before ASIO can apply to a decision-maker for an IPO (when requesting interception or stored communications). While the decision-maker is not required to consider privacy directly under the legislation, they must have regard to whether other less intrusive means of obtaining information are available. The explanatory memorandum explains that ASIO's Ministerial Guidelines (Guidelines) require that its actions be proportionate to the gravity of the threat posed, and that investigations should be done with as little intrusion into privacy as possible. Accordingly, ASIO will have to consider the impact of its operations on the privacy of any person before applying for an IPO.

B-Party IPOs

52. B-Party interception involves the interception of a communications service of a person who is not a person directly suspected of a relevant offence (B-Party), where the person suspected of involvement in the offence (A-Party) is likely to communicate using the B-party. AGD supports the requirement that, in deciding whether to issue a B-Party IPO, the decision-maker must have regard to how much the privacy of any person would be likely to be interfered with, and must also take into account the availability and use of other means to achieve the objectives of the IPO.

53. For B-Party IPOs sought by ASIO, there must be reasonable grounds for suspecting the person involved in the offence is likely to communicate using the B-Party's service, and the decision-maker must also consider whether less intrusive means are available and whether all other practicable methods have been exhausted to obtain the information. ASIO must conduct its operations with adequate consideration of privacy, pursuant to its Guidelines.

54. The IPO provisions in relation to interception, stored communications, telecommunications data, whether targeted at an A-Party or B-Party, adequately address privacy considerations. The provisions ensure that IPOs do not constitute arbitrary or unlawful interference with a person's privacy, and provide sufficient safeguards to ensure that any interference is reasonable, necessary and proportionate.

Disclosure of Protected Information

55. The prohibition on disclosure in Part 11 of the Bill is intended to protect the privacy of persons whose communications and information have been obtained pursuant to an IPO, and control the disclosure of information relating to law enforcement and national security. The exceptions to this prohibition generally relate to law enforcement and national security purposes.

56. AGD supports the exemption in subclause 153(1)(r), which allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of investigations under the Privacy Act or any other Commonwealth law concerning the privacy of personal information.

Privacy safeguards in incoming requests

57. Part 13 of the Bill authorises disclosures by Australian communications providers to overseas law enforcement authorities for the purposes of the Privacy Act to the extent the disclosure is in accordance with an incoming request from a foreign government with which Australia has a DIA. This provides a clear authorisation under Australian Privacy Principle (APP) 8.2.c of the Privacy Act. However, before an Australian communications provider relies on this authorisation, it should establish administrative arrangements, memorandums of understanding or protocols that set out mutually agreed standards for the handling of personal information that provide privacy protections comparable to the APPs.

58. The Bill provides for agreements to be specified as DIAs in the regulations. The explanatory memorandum confirms that these regulations are legislative instruments and the text of each designated agreement will be publicly available. The Government will need to satisfy itself that any foreign party to a DIA will provide adequate privacy safeguards to the information it receives from Australian communications providers. While this is not specified in the Bill, the policy is reflected in the explanatory memorandum which provides: 'In practice, it is expected that consideration of protections and safeguards related to privacy will also be a consideration when developing international agreements'.

59. Since 2019, the US and Australia have been formally negotiating an agreement for cross-border access to communications data consistent with the US CLOUD Act, which is intended to be the first DIA for the purposes of the Bill. AGD has been supporting DoHA in these negotiations to ensure adequate privacy protection are included in this agreement.

Evidentiary requirements

60. The Bill contains measures for entities involved at various stages of the IPO process (such as DCPs, the ADA and requesting agencies) to provide evidentiary certificates for the purposes of assisting with the admissibility of relevant communications data obtained through the process in subsequent prosecutions. The following analysis considers the use of evidentiary certificates generally, and goes on to consider the use of *prima facie* evidence certificates and conclusive evidence certificates within this context.

Evidentiary certificates

61. Evidentiary certificates are documents that can be admitted by courts or tribunals as evidence of facts stated within. They allow relevant witnesses in proceedings to provide evidence to decision-makers without necessarily having to provide witness testimony or provide the information under affidavits. Evidentiary certificates are most effective where their content:

    - is non-controversial
    - covers matters sufficiently removed from the main facts in issue
    - is unlikely to be challenged.

62. The explanatory memorandum to the Bill (at paragraph 540) indicates that the primary benefit of the evidentiary certificate provisions is to reduce the need for officers of foreign DCPs to have to travel internationally to Australia to appear in court to give evidence:

> […] the use of evidentiary certificates for IPOs is of significant utility as requiring the appearance of employees of foreign designated communications providers in court proceedings held in Australia will be complex and, at times, impractical.

63. 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.

64. 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)).

65. Part 10 of the Bill provides for a system of oversight by the Commonwealth Ombudsman to determine the compliance of the Secretary of AGD (as the ADA) with the IPO regime. This Part has evidentiary implications as it abrogates the privilege of self-incrimination in relation to information that is provided to the Ombudsman. This is addressed further below in relation to oversight mechanisms by the Ombudsman (paragraphs 74-78).

Prima facie evidence

66. Evidentiary certificate provisions should generally state that certificates are *prima facie* evidence, rather than conclusive evidence, of the matters and information contained within. Where *prima facie* certificates are admitted, courts can rely on the evidence unless challenged by defendants leading evidence to contradict the facts, in line with the ordinary rules of evidence.

Conclusive evidence

67. Legislative provisions purporting to deem evidentiary certificates as providing conclusive evidence of ultimate facts can raise constitutional issues. To ensure such provisions do not contravene the separation of powers doctrine that prevents the legislature from usurping judicial power, as well as section 80 of the Constitution that guarantees the essential features of trial by jury for indictable offences, it is appropriate to use conclusive evidentiary certificates in limited circumstances with legitimate policy reasons.

68. 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.

69. 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*.[2] 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.

Oversight of the IPO framework

Ombudsman

Role of Ombudsman

70. The Ombudsman is responsible for assessing whether relevant agencies except ASIO (i.e. interception agencies, criminal law enforcement agencies, enforcement agencies, or a control order IPO agency) and the ADA are complying with the IPO scheme. The functions and powers of the Ombudsman are outlined in Part 10 of the Bill.

71. 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

[2] In *R v Cheikho* [2008] NSWCCA 191; 75 NSWLR 323, the New South Wales Court of Criminal Appeal upheld the conclusive nature of an evidentiary certificate issued under subsection 18(2) of the TIA Act. In that case, Mr Cheikho was charged under the *Crimes Act 1914* with conspiracy to commit acts in preparation of terrorist acts. A fact relied on by the prosecution was that the applicant downloaded certain documents through his internet service provider. A conclusive evidentiary certificate was issued by Optus that set out the steps taken by Optus employees to enable ASIO to carry out an intercept warrant. The certificate did not make any assertions about the content of intercepted communications (i.e. whether particular documents were downloaded). The court found that the matters stated in the certificate were 'too far removed' from the facts in issue to grant leave to appeal the admissibility of the certificate (at paras [185]-[188]).

- 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.

72. 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).

73. The powers and responsibilities of the Ombudsman under the Bill ensure that the Ombudsman can carry out effective and meaningful oversight of the IPO scheme. Ombudsman oversight of the scheme provides assurance to Parliament and the public that the powers under the Bill are exercised by relevant agencies and the ADA in accordance with the terms of the legislation.

Privilege against self-incrimination

74. As foreshadowed above at paragraph 65, the oversight role of the Ombudsman raises issues around the privilege against self-incrimination. Subclause 145(1) abrogates the privilege against self-incrimination when a person is providing information to or answering questions posed by the Ombudsman under Part 10, which relates to oversight of the IPO regime by the Ombudsman. This departs from the common law privilege against self-incrimination which applies not only to the disclosure of information in a court proceeding, but also as a protection wherever information may be compulsorily acquired by investigators, or by administrative agencies imposing penalties.

75. Further, subclause 145(2) provides that any information a person has provided to the Ombudsman is not admissible against the person, with the exception of court proceedings for the prosecution of:

- an offence against clause 152 (on prohibition on use, recording or disclosure of protected information or its admission in evidence)
- an offence against Part 7.4 or 7.7 of the *Criminal Code 1995* (Criminal Code) (on the giving of false or misleading statements and forgery or falsification of documents) (clause 145(2)(b)).

76. The privilege against self-incrimination should only be abrogated where there exists a significant policy justification for doing so. In this regard, AGD understands the aim of subclause 145(1) is twofold. Firstly, it ensures consistency between the Ombudsman's powers under the TIA Act and existing powers conferred by section 9 of the *Ombudsman Act 1976* (Ombudsman Act) which similarly includes an abrogation of the privilege against self-incrimination. Secondly, it recognises the public interest in effective monitoring of highly intrusive powers.

77. The two exceptions set out above are specifically aimed at prosecutions that result from a person's actions in defrauding or misleading the Ombudsman by providing false information or documents, or providing information where there is no legitimate purpose for doing so.

78. Further, paragraph 476 of the explanatory memorandum to the Bill states the intention of subclause 145(2) is to 'encourage cooperation with the Ombudsman's activities' by limiting the admissibility to offences under clause 152 or Parts 7.4 or 7.7 of the Criminal Code. We note this subclause appears to operate in a similar manner to subsection 7A(1B) of the Ombudsman Act.

IGIS

79. 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:

    - 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.

80. 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.