Submission No 96

Inquiry into potential reforms of National Security Legislation

Organisation: Law Council of Australia

Law Council
OF AUSTRALIA

National Security Legislation Reform

Parliamentary Joint Committee on Intelligence and Security

20 August 2012

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

Executive Summary

1. The Law Council of Australia welcomes the opportunity to consider a range of proposed reforms to national security legislation outlined in the Discussion Paper prepared for the purposes of this inquiry by the Parliamentary Joint Committee on Intelligence and Security (the PJCIS).

2. The Discussion Paper contains a wide range of proposed reforms which if adopted in their entirely would constitute a very significant expansion of the powers of Australia's law enforcement and intelligence agencies. The Law Council questions whether such an expansion is necessary in light of the extensive catalogue of powers already available to these agencies to investigate and address threats to national security. It also questions whether the introduction of these reforms constitutes a proportionate response to the national security threats facing Australia, particularly given their intrusive impact on the rights of individuals. For these reasons, and in light of the particular concerns outlined in this submission, the Law Council cautions against the adoption of many of the reforms proposed in the Discussion Paper.

3. In line with its past advocacy in this area, the Law Council's submission focuses on those reforms concerning the telecommunications interception and access regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) and those reforms relating to the content, use and oversight of the special powers of the Australian Security Intelligence Organisation (ASIO).

4. In relation to the proposed reforms relating to telecommunication interception and access (contained in Chapter 2 of the Discussion Paper), the Law Council:

   (a) welcomes the proposal to introduce a privacy based objective into the TIA Act, and submits that this should be accompanied by a consistent privacy impact test;

   (b) raises concerns regarding the proposed reforms that would:

      (i) simplify tests and thresholds relating to telecommunications interception warrants;

      (ii) create a single warrant with multiple interception powers;

      (iii) expand the basis of interception activities;

      (iv) require telecommunication data to be retained for up to two years; and

      (v) allow increased information sharing between agencies.

   (c) submits that any such reforms should not further limit the general prohibitions on telecommunications interception and access and disclosure of telecommunications data contained in the TIA Act unless such limitations can be justified. These reforms should also be accompanied by appropriate oversight and safeguards to protect the rights and privacy of any individuals affected.

5. In relation to the proposed reforms relating to the Australian intelligence community (contained in Chapter 4 of the Discussion Paper) the Law Council focuses on those reforms relating to the authorisation and use of the special powers available to ASIO

under Division 2 Part III of the *Australian Security and Intelligence Organisation Act 1979* (Cth) (the ASIO Act).

(a) The Law Council holds particular concerns regarding the proposed reforms that would:

(i) amend the current provisions relating to computer access warrants, such as broadening the definition of 'computer', authorising the use of third party computers and communications in transit and broadening the range of authorised acts necessary to execute a computer access warrant;

(ii) facilitate variation and renewal of warrants;

(iii) extend the current 90 days duration of search warrants to six months;

(iv) introduce named person warrants that would authorise ASIO officers to use multiple powers under a single warrant;

(v) broaden existing powers relating to person searches; and

(vi) introduce authorisation lists of classes of people authorised to execute warrants.

(b) In relation to these proposed reforms, the Law Council is concerned by:

(i) the absence of information provided in the Discussion Paper to justify why these proposed reforms are necessary, particularly in light of the already extensive powers available to ASIO;

(ii) the propensity for the Discussion Paper to focus on removing administrative burdens or addressing operational challenges, and the absence of discussion of the history and context of the existing powers; and

(iii) the lack of detail regarding the types of safeguards or reporting or oversight requirements that would accompany the proposed changes to ASIO's powers or warrant processes.

(c) The Law Council also opposes the proposed reform that would create an authorised intelligence operations scheme (or controlled operations scheme) for ASIO officers, based on that currently available to certain law enforcement officers under the *Crimes Act 1914* (Cth) (the Crimes Act).

(d) The Law Council also suggests that the PJCIS pay particular regard to the prescribed statutory functions of ASIO and the need to distinguish ASIO's intelligence gathering role from the role of law enforcement agencies when evaluating these proposed reforms.

6. While the Law Council welcomes the opportunity to comment upon these proposed reforms prior to the introduction of amending legislation, the absence of specific detail in respect to many of the reforms proposed in the Discussion Paper means that further comments will be required if and when draft legislation implementing any of the proposed reforms is released.

Introduction

7. The Law Council of Australia is pleased to provide the following submission to the PJCIS inquiry into potential reforms of national security legislation (the Inquiry).

8. The potential reforms the PJCIS is required to inquire into are outlined in a Discussion Paper provided by the Government entitled *Equipping Australia against emerging and evolving threats* (the Discussion Paper).[1] The reforms relate to the:

   (a) the TIA Act;

   (b) *Telecommunications Act 1997* (Cth) (the Telecommunications Act);

   (c) the ASIO Act; and

   (d) the IS Act.

9. The proposed reforms are separated into three different groupings: those the Government wishes to progress; those the Government is considering progressing; and those on which the Government is expressly seeking the views of the PJCIS.

10. The Inquiry's terms of reference are wide ranging.[2] For example, when inquiring into the proposed reforms, the PJCIS is asked to have regard to the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet the challenges of new and emerging technologies upon agencies' capabilities.

11. The PJCIS is also asked to have regard to whether the proposed reforms:

   (a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector;

   (b) apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the telecommunications sector and the potential for follow on effects to consumers, the economy and international competition; and

   (c) will address law enforcement reduction of capabilities from new technologies and [the] business environment, which has a flow-on effect to security agencies.

12. The Law Council has a long standing interest in the content and operation of Australia's national security legislation; it has previously raised concerns relating to the necessity and effectiveness of certain components of such legislation and whether it operates in a way that complies with rule of law principles and international human rights standards. The Law Council's past advocacy has included a focus on telecommunications interception laws and on the content, use

[1] This Discussion Paper was released in July 2012 and is available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm

[2] A document containing the Inquiry's full terms of reference is available on the PJCIS's webpage at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/tor.htm

and oversight of the special powers of the Australian Security Intelligence Organisation (ASIO).[3]

13. On the basis of this past advocacy, the Law Council's submission focuses on:

    (a) the proposed telecommunications interception reforms, particularly those that would broaden the scope of the existing powers of law enforcement and intelligence officers to intercept, access and disclose telecommunications information, and those proposed reforms that would introduce new powers into the existing regime, such as those relating to telecommunications data retention; and

    (b) the proposed reforms to the legislation regulating the Australian intelligence community, particularly those that seek to broaden the scope of ASIO's special powers under Division 2 of Part III of the ASIO Act.

14. When commenting on these proposed reforms, the Law Council will pay particular regard to the PJCIS's terms of reference that invite the PJCIS to have regard to whether the proposed reforms contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security.

15. The Law Council welcomes the opportunity for the public and the Parliament to consider reform proposals to national security legislation prior to any amendments being introduced into Parliament.[4]

16. However, the Law Council also notes that, if adopted in their entirety, the reforms proposed in the Discussion Paper would constitute one of the most significant reforms to Australia's national security legislation for over a decade. The broad scope of the reforms makes it difficult to provide comprehensive comments in the time frame available for the Inquiry.

17. Further, as the proposals are described in varying degrees of detail, it is difficult to comment on each of the proposed reforms at this stage. For example, while the Discussion Paper includes some descriptions of the operational challenges faced by law enforcement and intelligence agencies, it does not always explain how the specific proposed reform would assist in meeting these challenges, how it would interact with existing provisions and what safeguards and accountability mechanisms it would include.

---

[3] For example, Law Council of Australia submission to the Senate Standing Committee on Legal and Constitutional Affairs, *Inquiry into the Intelligence Services Legislation Amendment Bill 2011* (3 May 2011); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010* (28 October 2010); Law Council of Australia submission to the Senate Legal and Constitution Affairs Committee, *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2009* (9 October 2009); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee, *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008); Law Council of Australia submission to the Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law* (20 December 2007); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee, *Inquiry into Telecommunications (Interception and Access) Bill 2007* (July 2007); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into Telecommunications (Interception and Access) Bill 2006* (13 March 2006) These submissions are available on the Law Council's website at http://www.lawcouncil.asn.au/programs/criminal-law-human-rights/criminal-law/powers.cfm?fms_folder_uuid=8A114BB4-1E4F-17FA-D2FF-231CD8C319F3

[4] See Law Council of Australia Media Release 'Don't Rush to 'Rubber Stamp' Anti-Terror Measures, Law Council Warns' (9 September 2005) available at http://www.lawcouncil.asn.au/media/news-article.cfm?article=B55FCE0C-1E4F-17FA-D2B5-D3258229D166

18. For this reason, the Law Council would welcome the opportunity to consider any further information presented to this Inquiry and to provide further comments if and when draft legislation implementing any of the proposed reforms is released.

19. The Law Council acknowledges that other organisations are better placed to assess the ramifications of some of the proposed reforms for telecommunication industry participants or other private sector bodies. For example, the Law Council has not addressed proposals relating to:

    (a) the modernisation of the TIA Act's cost sharing framework to align industry interception assistance with industry regulatory policy and clarify the Australian Communications and Media Authority's (ACMA) regulatory and enforcement role;

    (b) extending the regulatory regime to ancillary service providers not currently covered by the legislation; or

    (c) implementing a three-tiered industry participation model.

20. The Law Council also acknowledges that other organisations hold particular expertise in the area of telecommunications or surveillance technology and for this reason anticipates that these organisations, with more detailed and direct knowledge of the operation and maintenance of computer networks, will provide more detailed views to the PJCIS on some reforms. For example, such organisations may comment on the need for ASIO's use of third party computers when executing computer access warrants and the proposed offence that would penalise industry participants for failing to assist in decryption. The Law Council also anticipates that other organisations will provide comment to the PJCIS on the impact of the proposed reforms to ASIO employment practices outlined in Chapter 4 of the Discussion Paper.

21. With these qualifications in mind, the Law Council hopes that the following comments and questions will be of assistance to the PJCIS as it undertakes this Inquiry.

Interception and the TIA Act – Outline of the reforms in Chapter 2 of the Discussion Paper

22. Chapter 2 of the Discussion Paper concerns proposed reforms to the telecommunications interception regime. Some of these proposed reforms, such as those relating to the examination of the legislation's privacy objective and reducing the number of agencies accessing communication information, are intended to improve existing safeguards for protecting the privacy of individuals and are generally supported by the Law Council.

23. The Law Council has concerns about other proposed reforms, such as those related to:

    (a) simplifying tests and thresholds relating to telecommunications interception warrants;

    (b) creating a single warrant with multiple interception powers;

    (c) expanding the basis of interception activities;

    (d) requiring telecommunication data to be retained for up to two years: and

    (e) allowing increased information sharing between agencies.

24. In particular, the Law Council submits that any such reforms should not further limit the general prohibitions contained in the TIA Act on telecommunications interception and access and disclosure of telecommunications data unless such limitations can be justified. These reforms should also be accompanied by appropriate oversight and safeguards to protect the rights and privacy of any individuals affected.

General comments relating to the reforms

25. In this section of the submission, the Law Council will:

    (a) outline the current legislative framework for intercepting or accessing telecommunications;

    (b) outline the relevant proposals in Chapter 2 of the Discussion Paper;

    (c) provide some general comments on the need to demonstrate why the proposed reforms are necessary and are a proportionate response to addressing criminal conduct or threats to national security;

    (d) provide some specific comments in relation to the following proposed reforms:

        (i) the introduction of a privacy focused objects clause;

        (ii) standardisation of warrant thresholds;

        (iii) standardisation of warrant processes;

        (iv) expansion of the basis of interception activities;

        (v) retention of data for periods for up to two years;

(vi) simplification of information sharing provisions and reporting requirements; and

(vii) creation of a single warrant with multiple telecommunication interception powers.

Current Legislative Framework for Intercepting or Accessing Telecommunications

26. The TIA Act has two key purposes:

- to protect the privacy of individuals who use the Australian telecommunications system, and
- to specify the circumstances in which it is lawful to intercept and access communications or authorise the disclosure of telecommunications data.[5]

27. The TIA Act seeks to achieve these outcomes by:

- prohibiting the listening to or recording of communications; [6]
- prohibiting access to stored communications; [7]
- establishing a warrant scheme to enable interception of or access to telecommunications to assist in the investigation of serious offences and serious contraventions or to assist in the performance of ASIO's functions;[8] and
- establishing processes to enable access to telecommunications data[9] to assist in the enforcement of the criminal law, laws imposing criminal penalties and laws aimed at protecting public revenue or to assist in the performance of ASIO's functions. [10]

28. Access to telecommunications data is otherwise prohibited under the Telecommunications Act. [11]

Telecommunication Interception Warrants

29. Part 2-5 of the TIA Act provides for the issue of telecommunications interception warrants to interception agencies. 'Interception agencies' include law enforcement, intelligence and oversight agencies such as the Australian Crime Commission (the

[5] See *Telecommunications Interception and Access Act 1979 Report for the year ending 30 June 2011* at http://www.ag.gov.au/Documents/Final+TIA+Act+Annual+Report+2010-11+-+amended+after+publication+-+v5+%283%29.pdf at p 2.
[6] Section 7 of the TIA Act prohibits the interception of a communication in its passage over the Australian telecommunications network. Section 6 defines an interception as listening to or recording, by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication.
[7] Section 108 of the TIA Act prohibits access to stored communications. Stored communications are: (a) communications which have passed over the telecommunications system, and are accessed with the assistance of a telecommunications carrier without the knowledge of one of the parties to the communication. Examples of stored communications include voice mail, e-mails and SMS messages.
[8] TIA Act Chapters 2 and 3.
[9] Telecommunications data is not defined but can include information such as subscriber details and the date, time, and location of a communication. Telecommunications data does not include the content or substance of the communication.
[10] TIA Act Chapter 4.
[11] See for example Telecommunications Act ss276, 277, 278.

ACC), Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Federal Police (AFP) and certain declared State and Territory agencies.[12]

30. Part 2-5 of the TIA Act provides that a telecommunications interception warrant may be sought by an interception agency to assist with the investigation of a 'serious offence'. A 'serious offence' is exhaustively defined in section 5D and includes:

    (a) murder, kidnapping, serious drug offences and terrorism offences;

    (b) offences punishable by at least seven years imprisonment that involve conduct resulting in serious personal injury, serious property damage, serious arson, bribery or corruption, tax evasion, fraud, or loss of revenue to the Commonwealth;

    (c) offences relating to people smuggling, slavery, sexual servitude, deceptive recruiting and trafficking in persons;

    (d) sexual offences against children and offences involving child pornography;

    (e) money laundering offences, cybercrime offences and serious cartel offences;

    (f) offences involving organised crime, and

    (g) ancillary offences, such as aiding, abetting and conspiring to commit serious offences.

31. The TIA Act provides that an 'eligible Judge'[13] or 'nominated Administrative Appeals Tribunal (AAT)[14] member' may issue a telecommunications interception warrant on application by an agency. This can be a telecommunications service warrant or a named person warrant.[15]

32. The TIA Act requires that an application for a telecommunications interception warrant be in writing and be accompanied by a supporting affidavit which contains the facts on which the application is based, the period for which the warrant is sought and information regarding any previous warrants obtained in relation to the same matter.[16] In urgent circumstances, applications may be made by telephone.

[12] Attorney General's Department, *Telecommunications (Interception and Access) Act 1979 - Annual Report for the year ending 30 June 2011* available at http://www.ag.gov.au/Publications/Pages/TelecommunicationsInterceptionandAccessAct1979AnnualReportfortheyearendingJune2011.aspx. During the reporting period of 2010-2011, the following eligible State and Territory authorities were the subject of a declaration pursuant to section 34 of the TIA Act and were able to apply for telecommunications interception warrants: Victoria Police, New South Wales Crime Commission, New South Wales Police Force, Independent Commission Against Corruption, South Australia Police, Western Australia Police, Police Integrity Commission, Corruption and Crime Commission, Tasmania Police, Northern Territory Police, Office of Police Integrity Victoria, Queensland Police Service, Queensland Crime and Misconduct Commission.

[13] TIA Act s6D. An 'eligible Judge' is a Judge who has consented in writing and been declared by the Attorney-General to be an eligible Judge which currently includes members of the Federal Court of Australia, the Family Court of Australia, and the Federal Magistrates Court.

[14] TIA Act s6DA A 'nominated AAT member' refers to a Deputy President, senior member or a member of the AAT who has been nominated by the Attorney-General to issue warrants. In the case of part-time senior members and members of the AAT, the member must have been enrolled as a legal practitioner of the High Court, the Federal Court or the Supreme Court of a State or Territory for no less than five years to be eligible for nomination to issue warrants.

[15] TIA Act ss46, 46A.

[16] TIA Act s49.

The warrant takes effect only when completed and signed by the Judge or nominated AAT member. [17]

33. Before issuing a telecommunications interception warrant, the issuing authority must consider the following matters:

- how much the privacy of any person or persons would be likely to be interfered with;
- the gravity of the offence;
- how much the information likely to be obtained would assist the investigation;
- the availability of alternative methods of investigation;
- how much the use of such alternative methods would assist the investigation, and
- how much the use of such alternative methods would prejudice the investigation by the agency, whether because of delay or for any other reason.[18]

34. Where an application for a warrant includes a request that the warrant authorise entry onto premises, section 48 of the TIA Act requires that the Judge or nominated AAT member also be satisfied that it would be impracticable or inappropriate to intercept communications by less intrusive means.

35. Under Part 2-2 of the TIA Act, telecommunication interception warrants are also available to ASIO, at the request of the Director-General of Security (the Director-General) and are issued by the Attorney-General. These warrants may be telecommunications service warrants or named person warrants.

36. In respect of telecommunication service warrants, the Attorney-General must be satisfied that:[19]

(a) the telecommunications service is being or is likely to be:

(i) used by a person engaged in, or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; or

(ii) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, such activities; or

(iii) used for purposes prejudicial to security; and

(b) the interception by ASIO of communications made to or from the telecommunications service will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relating to security.

[17] TIA Act ss50, 51. The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.
[18] TIA Act ss46, 46A.
[19] TIA Act s9.

37. When issuing a named person warrant, the Attorney-General must be satisfied that:[20]

    (a) the person is engaged in, or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and

    (b) the interception by ASIO of:

        (i) communications made to or from telecommunications services used by the person; or

        (ii) communications made by means of a particular telecommunications device or particular telecommunications devices used by the person;

    (c) the interception will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relating to security; and

    (d) relying on a telecommunications service warrant to obtain the intelligence would be ineffective.

38. The maximum duration for these warrants is six months

39. ASIO can also apply for a telecommunications service warrant or a named person warrant for collection of foreign intelligence.[21] There is also provision for emergency warrants to be issued by the Director-General.[22]

40. These interception warrants can be executed by ASIO officers and employees and other persons authorised by the Director-General, or by an officer of ASIO appointed by the Director-General in writing, to be an authorising officer. [23]

41. The TIA Act contains a number of reporting requirements in relation to telecommunication interception warrants. For example, the Attorney-General must be given copies of telecommunications interception warrants and revocations issued to interception agencies and provide reports on outcomes.[24] The Secretary of the Attorney-General's Department must maintain a General Register which includes particulars of all telecommunications interception warrants. These requirements are outlined in detail below.

42. The TIA Act also contains requirements for the destruction of records of intercepted information if the Director-General is satisfied that the information is no longer required or is unlikely to be required for ASIO's functions.[25]

43. The TIA Act also contains a number of mechanisms designed to provide independent oversight of the telecommunication interception regime. For example, the ACC, ACLEI and the AFP are required to maintain records relating to interceptions and the use, dissemination and destruction of intercepted

[20] TIA Act s9A.
[21] TIA Act ss11A, 11B.
[22] TIA Act s10.
[23] TIA Act s12.
[24] Sections 57, 59A and 94 of the TIA Act provides that the chief officer of each interception agency must give to the Attorney-General: a copy of each telecommunications interception warrant issued to that agency; each instrument revoking such a warrant, and within three months of a warrant ceasing to be in force, a written report about the use made of information obtained by interception under the warrant.
[25] See TIA Act, ss 11C, 14.

information.[26] These records must be inspected by the Commonwealth Ombudsman on a regular basis. As discussed below, the relevant State or Territory Ombudsmen generally undertake this function for State and Territory agencies.[27]

Stored communications warrants

44. Part 3-3 of the TIA Act enables a stored communications warrant to be issued to an 'enforcement agency'. An 'enforcement agency' includes the law enforcement, intelligence and oversight agencies described above, as well as agencies responsible for administering a law imposing a pecuniary penalty or relating to the protection of the public revenue, such as the Australian Customs and Border Protection Service (ACBPS), the Australian Securities and Investments Commission (ASIC), the Australian Competition and Consumer Commission (ACCC), the Australian Taxation Office (ATO), Centrelink and a range of State and Territory government organisations.[28]

45. A stored communications warrant authorises covert access to stored communications in connection with the investigation of a serious contravention. A 'serious contravention' is defined in section 5E of the TIA Act as a:

- serious offence (being an offence for which a telecommunications interception warrant may be obtained);
- an offence punishable by a maximum period of imprisonment of at least three years, or
- an offence with an equivalent monetary penalty.

46. Stored communication warrants are issued to enforcement agencies by 'issuing authorities' appointed by the Attorney-General in accordance with section 6DB of the TIA Act. These include Judges and Magistrates, certain AAT members or any person who has been appointed by the Attorney-General for this purpose.

47. An application for a stored communications warrant must be in writing and be accompanied by a supporting affidavit containing the facts on which the application is based.[29] In urgent circumstances, applications may be made by telephone.[30] In either case, the warrant takes effect only when completed and signed by the issuing authority.

48. Before issuing a stored communications warrant to an enforcement agency, an issuing authority must have regard to similar considerations to those outlined above in relation to telecommunications interception warrants, such as considerations relating to privacy effects, the seriousness of the contravention, the assistance that will be provided through the warrant and possible alternative methods of obtaining the relevant information. [31]

[26] See TIA Act Part 2.7.
[27] Instead of the State Ombudsman, inspection of the South Australian Police is undertaken by the Police Complaints Authority (South Australia), while inspections of the Victorian Police and the Office of Police Integrity Victoria are undertaken by the Special Investigations Monitor (Victoria).
[28] See TIA Act Part 2.7.
[29] TIA Act s112.
[30] TIA Act ss113-114. The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.
[31] TIA Act s116.

49. Similarly to the regime applying to telecommunications interception warrants, ASIO is also able to obtain stored communications warrants.

50. Under the TIA Act, the chief officer of an agency is required to destroy any information or record obtained by accessing a stored communication, if it is not likely to be required for the purposes for which it can be used under the TIA Act.

51. Certain records must also be kept in relation to stored communication warrants. For example, section 151 provides that the chief officer of an enforcement agency must keep: each stored communications warrant issued; each instrument of revocation; copies of authorisations which authorise persons to receive stored communications, and particulars of the destruction of information.

52. The TIA Act also provides that the Commonwealth Ombudsman must conduct regular inspections of records of enforcement agencies and report to the Attorney-General on the results of those inspections.[32] The Attorney-General is also required to prepare and table in Parliament each year a report setting out the information specified in Part 3-6 of the TIA Act.[33]

Telecommunications data authorisations

53. Part 4-1 of the TIA Act generally prohibits the disclosure of the content or substance of a telecommunication, but also enables ASIO and certain enforcement agencies to authorise the disclosure of telecommunications data in certain circumstances. While telecommunications data is not defined in the TIA Act, it is taken to mean anything that is not the content or substance of a communication. It has been described in the Attorney-General's Department *Telecommunications (Interception and Access) Act 1979 - Annual Report for the year ending 30 June 2011* as including:

- subscriber information;
- telephone numbers of the parties involved in the communication;
- the date and time of a communication;
- the duration of a communication;
- Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication; and
- location-based information.

54. Sections 171 to 180 of the TIA Act allow for the authorisation of the release of telecommunications data under certain circumstances by an authorised officer of the relevant enforcement agency.[34] For example:

- The disclosure of historical[35] or existing data may be authorised by an enforcement agency when it is considered reasonably necessary for the enforcement of a criminal law, a law imposing a pecuniary penalty, or for the protection of the public revenue.

[32] TIA Act Part 3.5 Division 2.
[33] TIA Act s161 and 164.
[34] An authorised officer includes: the head (however described) or a person acting as that head, deputy head (however described) or a person acting as that deputy head of an agency, or a person who holds or is acting in an office or position covered by an authorisation in force under subsection 5AB(1) of the TIA Act.
[35] TIA Act s178. Historical data is information which existed before an authorisation for disclosure was received. It does not include information which comes into existence after the authorisation was received.

- The disclosure of prospective data[36] may only be authorised by a criminal law enforcement agency when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years.[37]

55. Authorisations for such disclosure must include the information outlined in section 183 of the TIA Act, which includes: details of the information or documents to be disclosed and a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or the protection of the public revenue.

56. Section 180 of the TIA Act also requires authorisations for prospective access to include:

- a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years;
- a statement that the officer had regard to the impact on privacy;
- a statement that any impact on privacy was outweighed by the seriousness of the conduct being investigated, and
- the date on which the authorisation is due to end.

57. The TIA Act also allows senior ASIO officers to authorise access to historical telecommunications data and prospective data in certain circumstances.[38]

The Proposed Reforms

58. The Discussion Paper explains that lawful interception and access to telecommunications data are cost-effective investigative tools that support and complement information derived from other methods.[39] It provides some figures illustrating the number of arrests, prosecutions and convictions based on lawfully intercepted material during 2010-2011.[40]

59. The Discussion Paper also explains that intercepted information has played an important role in counter-terrorism prosecutions and in preventing planned terrorist attacks[41] and notes that espionage is an enduring threat to Australia, both through the traditional form of suborning persons to assist foreign intelligence agencies and new forms such as cyber espionage. [42]

60. The Discussion Paper also outlines some of the changes to telecommunications technology that impact on the TIA Act regime.[43] These include:

---

[36] TIA Act s180. Prospective data is data that comes into existence during the period the authorisation is in force.
[37] TIA Act Part 4.1 Division 4. Criminal law enforcement agency is defined as meaning all interception agencies and any other agency prescribed by the Attorney-General. See Attorney General's Department *Telecommunications (Interception and Access) Act 1979 - Annual Report for the year ending 30 June 2011.* During the reporting period, the ACBPS was the only body prescribed.
[38] TIA Act ss175-176.
[39] Discussion Paper p. 13
[40] Discussion Paper p. 13
[41] Discussion Paper p. 14
[42] Discussion Paper p. 14
[43] Discussion Paper pp. 18-19

- a significant growth in the number of fixed line telecommunication service providers, mobile network operators and Voice over the Internet Protocol (VOIP) service providers, satellite providers and Internet Service Providers;

- a significant increase in the number of mobile services and fixed line telephone services and internet subscribers in Australia;

- an increase in the use of multiple technologies and services and the downloading of data;

- the use of mobile phones as truly converged consumer devices, with users accessing voice, SMS, internet, email, e-payment, video, music, photography, and social networking sites;

- increased network coverage, speed and availability, which have allowed consumers to access VOIP services more effectively; and

- an increase in the use of social media resulting in more user generated content and the provision of alternative communication channels to traditional voice services.

61. The Discussion Paper states that these trends are set to continue particularly as a result of the implementation of the National Broadband Network, which will increase the amount of material that can be accessed through telecommunications devices.[44]

62. The Discussion Paper suggests that the complexity of the contemporary communications environment is not reflected in the current interception regime which is based on out-dated assumptions, for example, that communications to be intercepted are easily identified and that intercepted communications are easily interpreted or understood.[45] These assumptions mean that the TIA Act takes a technical approach to defining when an interception takes place, which now causes uncertainly about the scope of the general prohibition against interception, and fails to recognise the particular demands created by a diverse telecommunications sector.

63. It is said that the limitations created by the assumptions inherent in the TIA Act impact on the capacity of agencies to:

    - reliably identify communications of interest and to associate them with telecommunications services;

    - reliably and securely access communications and associated data of interest within networks; and

    - effectively interpret the communications to extract intelligence or evidence.[46]

64. In light of these limitations, the Discussion Paper outlines a series of reforms designed to:

    - strengthen the safeguards and privacy protections under the lawful access to communications regime in the TIA Act;

    - reform the lawful access to communications regime;

[44] Discussion Paper p. 19.
[45] Discussion Paper p. 20.
[46] Discussion Paper p. 20. These issues are outlined in further detail on pp 21- 22

- streamline and reduce complexity in the lawful access to communications regime;

- modernise the TIA Act's cost sharing framework to: align industry interception assistance with industry regulatory policy and clarify ACMA's regulatory and enforcement role.

65. Before commenting on the particular reforms proposed in Chapter 2 of the Discussion Paper, the Law Council will make some general comments about the need to demonstrate that the reforms proposed are necessary and proportionate tools to assist in the prevention and prosecution of criminal activity and to respond to threats to national security.

Proposed reforms must be shown to be necessary and proportionate

66. As noted by the UN High Commissioner for Human Rights, where a State seeks to restrict human rights, such as the rights to privacy, for legitimate and defined purposes, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective.[47]

67. In the context of telecommunications access and interception, this involves balancing the intrusiveness of the interference, against the need for it in operational terms. Interception of or access to communications will not be proportionate if it is excessive in the circumstances or if the information which is sought could reasonably be obtained by other means.[48]

68. When considering whether the reforms proposed in this Chapter of the Discussion Paper are necessary and proportionate, it is important to recognise the broad scope and intrusive nature of the existing powers available to enforcement and intelligence agencies under the TIA Act. These powers include:

- named person warrants – which authorise the interception of telecommunications from a particular person;[49]

- telecommunication service warrants – which authorise the interception of communications from a particular telecommunications service;[50]

- telecommunication device warrants – which authorise the interception of communications from a particular telecommunications device;[51]

- B-party warrants – which authorise the interception of telecommunications made to or from a person who is not a suspect and has no knowledge or involvement in a crime, but who may be in contact with someone who does;[52]

[47] Commission on Human Rights, *Statement by the United Nations High Commissioner for Human Rights, Fifty-eight session, Summary Record of the first meeting*, UN Doc E/CN.4/2002 SR.1(25 March 2002), [14].
[48] See UK Home Office *Interception of Communications Code of Practice* Pursuant to Section 71 of the *Regulation o f Investigatory Powers Act 2000* available at http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/interception-comms-code-practice?view=Binary
[49] TIA Act ss 9A and 46A.
[50] TIA Act ss 9 and 46.
[51] TIA Act ss9A and 46A.
[52] TIA Act ss 9(1)(a)(i)(ia), 46(1)(d)(ii).

- stored communication warrants – which authorise access to stored communications such as emails, voicemail messages and text messages; [53] and

- authorisations to disclose existing and prospective telecommunications data – which in the case of mobile phones, can include information about the person's location and movements.[54]

69. These warrants and authorisations can apply for periods of up to six months and can be obtained urgently in the case of emergencies. The information obtained during the exercise of powers under these warrants and authorisations can also be shared with other agencies (subject to limitations discussed in detail below).

70. The type of information that can be obtained in the exercise of these powers can be highly sensitive, such as conversations that might otherwise be considered confidential (for example those between lawyer and client) or personal (for example those between husband and wife). Telecommunications data can also reveal the precise location of a person via their mobile phone information.

71. The Law Council has previously expressed concern at the breadth of these powers and the lack of appropriate safeguards within the warrant and authorisation process to protect against unjustified intrusions into personal privacy.[55]

72. As will be outlined in further detail below, many of the reforms proposed in the Discussion Paper have the potential to significantly expand the nature or the scope of these powers. These reforms will have a direct or indirect impact on the enjoyment of individual rights and freedoms, not just in respect of persons suspected of criminal activity or of interest to intelligence agencies, but also on a wide range of innocent third parties who may, for example, have their telecommunications accessed or premises or computers searched.

73. In light of this, it is critical that the Government clearly establish, in respect of each proposed reform, why the reform is necessary, whether it will be effective and whether it is a proportionate response to criminal conduct or national security threats, having regard to its impact on human rights. In the context of the proposed reforms to the telecommunication interception regime, this means considering:

    (a) the nature of the current criminal conduct and national security threats facing the community;

    (b) the effectiveness of the current range of telecommunication interception and access powers available to law enforcement and intelligence agencies to address these threats;

    (c) the available options to address any barriers to the effectiveness of these powers;

    (d) the impact of any of these options on the rights of individuals subject to these powers;

[53] TIA Act s116.
[54] TIA Act Part 4.1, Divisions 3 and 4.
[55] See for example Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008); Law Council of Australia submission to the Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law* (20 December 2007).

(e) whether, in light of any impact on individual rights, the particular proposed power constitutes a proportionate response to the criminal conduct or national security threat it is designed to address; and

(f) if the particular proposed power has a significant impact on individual rights, what safeguards or accountability mechanisms should be put in place to ensure such a power is exercised only when absolutely necessary and is subject to independent oversight or review.

74. The Law Council is of the view that these issues have not always been satisfactorily addressed in the Discussion Paper. For example, the Law Council appreciates that the dramatic and rapid advances in technology have had a transforming impact on telecommunications in Australia and around the world, and that this in turn justifies a careful review of the adequacy of the current telecommunication interception regime. However, it does not follow that the challenges posed by technological advances must always be met by an expansion in interception or access capabilities. It may be, for example, that a more targeted approach to accessing communications or data is needed in light of the exponential increase in the generation of communications and data by the community, rather than a power that would allow a broader range of communications or data to be accessed or retained.

75. The Discussion Paper also often fails to explain why the particular power proposed is the least intrusive, most effective mechanism to address an operational need. It also provides little detail regarding the types of safeguards that should accompany the proposed power, and how it will fit within the existing accountability mechanisms in the TIA Act.

76. In addition, it is important to keep in mind that over the last decade the powers of law enforcement and intelligence agencies have not remained static in the face of this changing telecommunications environment. To the contrary, the last decade has seen considerable expansion in the powers and resources available to these agencies, many of which have been justified as necessary to respond to changing technology or investigation environments. For example, the TIA Act has been amended 39 times since 2002. At least six of these amendments were significant ones that introduced new interception and access powers, and these powers were justified at least in part by the need to respond to new and emerging technologies and new investigation environments.[56]

77. Some of these reforms, such as the B-Party warrant system[57] which authorises the interception of telecommunications made to or from a person who is *not a suspect* and *has no knowledge or involvement in a crime*, but who may be in contact with someone who does, have raised serious privacy concerns for the Law Council When these warrants were introduced, the Law Council expressed the view that unless a system of judicial oversight for the issue of B-Party warrants was introduced, and limits placed on the types of persons and communications authorised to be intercepted under a B-Party warrant, the intrusive impact on individual privacy could not be said to be proportionate to the legitimate aim of the interception regime.

[56] For example, see *Telecommunications Interception Legislation Amendment Act 2002; ASIO (Terrorism) Act 2003; Communications Legislation Amendment Act (No. 1) 2004; Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005;Telecommunications (Interception and Access) Amendment Act 2008; Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011*.

[57] B-Party warrants were introduced by the *Telecommunications (Interception) Amendment Act 2006* (Cth).

78. In light of the repeated amendment of the TIA Act regime to respond to the claimed operational needs of law enforcement and intelligence agencies, the Law Council questions the position advanced in the Discussion Paper that:

> *"… the interception regime provided by the current [TIA] Act reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the [TIA] Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act.*
>
> *In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity."*[58]

79. It may be that further reform is needed, but in light of the significant history of expanded powers for law enforcement and intelligence agencies in this area, the Law Council considers it to be necessary for the Government to clearly justify the reforms proposed. The Law Council submits that the PJCIS should ensure that adequate evidence is provided to address the issues outlined above in respect of each of the reform proposals outlined in the Discussion Paper.

Strengthening the safeguards and privacy protections

The Current Safeguards and Privacy Protections

80. Privacy is referred to in a number of sections of the TIA Act, for example in section 46, which outlines how a telecommunications service warrant is issued to a specified law enforcement officer by a Judge or AAT member. It provides that, when considering whether to issue such a warrant, one of the considerations to which the Judge or AAT member must have regard is:

> *"… how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service referred to [in the warrant]"*[59]

81. Section 180, which concerns authorisations for access to prospective information or documents, also provides that:

> *"Before making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure."*[60]

82. Under section 189 the Minister is also required to take the privacy of the users of telecommunications into account when making determinations in relation to interception capabilities applicable to a specified kind of telecommunications service that involves, or will involve, the use of a telecommunications system.[61]

83. Other safeguards in the TIA Act provide some limited protection against unjustified or unnecessary intrusion into personal privacy, such as considerations relating to privacy effects, the seriousness of the contravention, the assistance that will be

[58] Discussion Paper p. 12.
[59] TIA Act s46(2).
[60] TIA Act 180(5).
[61] TIA Act 189(4)(c).

provided through the warrant and possible alternative methods of obtaining the relevant information.[62]

84. These considerations are not required to be taken into account by the Attorney-General when he or she is considering whether to issue a telecommunication service warrant to an ASIO officer under section 9 of the TIA Act or a named person warrant under section 9A. However, the Attorney-General must not issue a warrant unless he or she is satisfied that:

(a) ASIO has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used; and that

(b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

Nature of the Proposed Reforms

85. The Discussion Paper explains that the Government wishes to progress proposals relating to strengthening the safeguards and privacy protections under the lawful access to communications regime in the TIA Act. This includes the examination of: the legislation's privacy protection objective; the proportionality tests for issuing warrants and mandatory record-keeping standards

86. The Discussion Paper explains that:

"The need to amend the Act to adapt to changes in the telecommunications environment has seen the range of exceptions to the general prohibition grow. Accordingly, it may be timely to revisit whether the privacy framework within the Act remains appropriate.

As people's use and expectations of technology have changed since the TIA Act was enacted in 1979 so community views about the types of communications that can be accessed and the purpose for which they can be accessed may also have changed." [63]

87. The Discussion Paper also states that:

"Consideration is also being given to introducing a privacy focused objects clause that clearly underpins this important objective of the legislation and which guides interpretation of obligations under the Act.[64]

Law Council's Concerns

Privacy Focused Objects Clause

88. The Law Council strongly supports the introduction of a privacy focused objects clause in the TIA Act. Such a clause could be modeled on Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) which provides that:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

[62] For example, see TIA Act 46A. See also discussion above.
[63] Discussion Paper p. 23
[64] Discussion Paper p. 23.

Everyone has the right to the protection of the law against such interference or attacks."

89. Article 8 of the *European Convention on Human Rights* (ECHR) also provides a possible model for such an objects clause. It provides that:

"Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

90. When drafting a privacy based objects clause for the TIA Act, regard could be had to the approach adopted in the exposure draft of the *Homelessness Bill 2012* recently released for discussion by the Department of Families, Housing, Community Services and Indigenous Affairs.[65] The exposure draft of the *Homelessness Bill* contains the following objects clause:

"The object of this Act is to increase recognition and awareness of persons who are, or are at risk of, experiencing homelessness".[66]

91. It also contains a provision that recognises Australia's international human rights obligations relating to the right to housing which provides:

"…, the Commonwealth recognises that reducing the number of persons who are, or are at risk of, experiencing homelessness is part of meeting Australia's international human rights obligations".[67]

92. This could be adapted for the TIA Act to provide that:

"The object of the Act is to recognise and protect the right of every person not to be subjected to arbitrary or unlawful interference with his or her privacy by way of the interception of his or her telecommunications."

"The Commonwealth recognises that in accordance with Australia's international human rights obligations there shall be no interference with the exercise of this right only when such interference is necessary in the interests of national security or public safety, or for the prevention of disorder or crime, or for the protection of the rights and freedoms of others."

93. The inclusion of this type of privacy based objects clause would acknowledge Australia's obligations under the international human rights Conventions to which it is a party,[68] and help ensure that privacy considerations are at the forefront of the minds of those exercising, authorising, or overseeing the powers under the TIA Act.

[65] A copy of the Exposure Draft Bill and other relevant materials are available at http://www.fahcsia.gov.au/our-responsibilities/housing-support/programs-services/homelessness/exposure-draft-homelessness-bill-2012/homelessness-bill-2012 .
[66] Exposure Draft *Homelessness Bill 2012* Clause 3.
[67] Exposure Draft *Homelessness Bill 2012* Clause 12.
[68] For example Article 17 of the ICCPR.

94. Such a clause would also complement the existing sections 7 and 63 of the TIA Act which contain a general prohibition on the interception of telecommunications or access to stored communications except in accordance with the TIA Act.

95. Including a privacy based objects clause would also assist in the interpretation of obligations under the TIA Act, encourage greater regard to privacy concerns and allow the courts to give full effect to any privacy based protections within the warrant provisions.

96. While it supports the inclusion of a privacy based objects clause in the TIA Act, the Law Council notes that such a clause will not of itself be sufficient to protect against unlawful or unjustified intrusion into individual privacy in the exercise of the powers under the Act. Nor will it ensure that privacy considerations are taken into account during all stages of telecommunications interception or access, from the application for a warrant to the review of information by the Ombudsman. As discussed below, specific, enforceable protections should be incorporated into the TIA Act to ensure that individual privacy is adequately protected.

Consistent Privacy Impact Test

97. One way to strengthen the existing protections against unjustified intrusion into personal privacy is to ensure that privacy considerations are taken into account before a warrant to intercept or access a telecommunication, or access to telecommunication data, is granted.

98. As noted above, the requirement to consider the extent to which the exercise of a power will interfere with personal privacy currently applies to the issuing of certain TIA Act warrants, but not all.

99. For this reason, the Law Council supports the inclusion of a single, consistent privacy test in all warrant applications and in all authorisations to intercept, access or disclose telecommunications or telecommunications data.

100. The Law Council has previously advocated for this type of test in the context of the proposed reforms to section 180 of the TIA Act relating to the authorisation of the disclosure of prospective telecommunications data.[69] In that context, the Law Council recommended that the following clause be introduced:

> *"Before an authorisation, the authorised officer must be satisfied on reasonable grounds that the likely benefit to the investigation which would result from the disclosure substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons."*

101. The Law Council suggests that a similar provision should be included in the other sections of the TIA Act that currently provide for the use of telecommunications interception, access and disclosure powers.

102. The "reasonable grounds" element of the test would ensure that the issue of privacy was more fully considered in the process. The Law Council also believes that such a test would reinforce the nature of the balancing process required when exercising powers under the TIA Act.

---

[69] Law Council of Australia submission to Joint Select Committee on Cyber-Safety *Inquiry into the Cybercrime Legislation Amendment Bill 2011* (14 July 2011) available at http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=69459E2B-C846-30EE-C1FD-17B77D7122E9&siteName=lc**a** (the 2011 Cyber Crime Submission).

Incorporating Adequate Safeguards in Warrant Process

103. In addition to the matters discussed above, the Law Council is of the view that other features of the warrant or authorisation process can operate as important safeguards against unjustifiable intrusion into personal privacy.

104. For example, in 2008 amendments were made to the TIA Act, relating to sections 16 and 60, which authorise the interception of communications from multiple devices used by a named person.[70] When these amendments were made, the Law Council raised concerns that the issuing authority could not address the privacy tests incorporated in the provisions with appropriate rigour without considering each and every telecommunications device that was to be covered by the warrant. In particular, the Law Council explained that an issuing authority cannot consider "*the impact the interception will have on the privacy of persons using the telecommunications service or device"* if the telecommunications service or device is not specified.

105. The type of safeguards to be incorporated into the warrant process in respect of each of the particular interception, access and disclosure powers in the TIA Act are discussed in further detail below.

Particular Privacy Concerns with Overt Access to Stored Communications

106. The Law Council is also concerned by the gaps in the privacy safeguards contained in the TIA Act with respect to access to stored communications. In particular, the warrant authorisation process in Part 3-3 of the TIA Act only deals with circumstances in which stored communications are *covertly* accessed by enforcement agencies.[71] This means that the TIA Act is silent on:

    (a) the circumstances in which government agencies are able to overtly (but nonetheless without the permission of the sender or recipient) access stored communications;

    (b) the use that government agencies can make of information obtained in this way and the circumstances in which secondary disclosure is permitted;

    (c) when information obtained in this way may be retained and for how long; and

    (d) the type of records that agencies need to produce about when and why they have accessed information in this way and what use they have made of it.

107. This means that where an enforcement agency overtly accesses stored communications (that is, after having given written notice of the access to the intended recipient of the communication) it can no longer be said that that the information is "accessed pursuant to the TIA Act." Instead, from a regulatory perspective, the information will be accessed pursuant to the separate pieces of legislation which govern each individual enforcement agency and which set out each agency's power to lawfully compel the production of information, for example by

[70] Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008); Law Council of Australia submission to the Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law* (20 December 2007); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee 's Inquiry into the *Telecommunications (Interception and Access) Bill 2008* (4 April 2008).
[71] This is a result of a combination of the effect of ss108(1)(b) and 6AA of the TIA Act. For further discussion see Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008).

issuing notices to produce to telecommunication carriers or carriage service providers.

108. This means that the requirement for issuing authorities to have regard to how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant contained in section 116(2)(a) of the TIA Act does not apply to stored communications accessed overtly.

109. The Law Council suggests that the PJCIS take these considerations into account when evaluating the proposals in the Discussion Paper designed to strengthen the safeguards and privacy protections in the TIA Act.

Reform of the lawful access regime for agencies

Nature of the Proposed Reforms

110. The Discussion Paper explains that the Government intends to reduce the number of agencies eligible to access communications information and standardise warrant tests and thresholds.[72]

111. The Discussion Paper explains that the offence thresholds that must be met before a TIA Act warrant can be issued to a law enforcement agency were traditionally limited to an offence that carries a penalty of at least seven years imprisonment (a serious offence), but notes that subsequent amendments have "… confused the policy in relation to the circumstances in which interception is available."[73] The Discussion Paper explains that:

"There are occasions where the general penalty threshold is too high to cover a range of offences for which it is already recognised that general community standards would expect interception to be made available. For example, child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks (including offences committed using a computer or involving telecommunications networks) do not meet the general 7 year policy threshold." [74]

112. The Discussion Paper also explains that the threshold for access to stored communications is lower than for interception:

> *"… because it was considered at the time the provisions were introduced that communicants often have the opportunity to review or delete these communications before sending them, meaning covert access can be less privacy intrusive then real-time listening. However, this logic, while valid several years ago, has become less compelling as technology use and availability has changed."*[75]

113. The Discussion Paper suggests that:

"Implementing a standard threshold for both content and stored communications warrants would remove the complexities inherent in the current interpretation of

[72] Discussion Paper pp.8, 24.
[73] Discussion Paper p. 24.
[74] Discussion Paper p. 24.
[75] Discussion Paper p. 24.

what is a serious offence, recognise the growing number of online offences and provide consistent protection for 'live' and 'stored' content."[76]

114. The Discussion Paper also proposes to introduce a simplified warrant regime that focuses on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest. It explains that:

"How and for what purposes an interception agency can intercept a communication depends on limited characteristics or features of communication relating to the type of service or device used or the name of a person. Defining attributes by communicant, carrier-provided service or technology made more sense in an era where carriers, device types and users were limited but is more complex in the current environment where the carrier or means of conveyance is not always readily apparent. This is both time consuming and costly for agencies in terms of analysing unnecessary information and potentially invasive from a privacy perspective as the communications of innocent parties may be unduly affected."

115. In addition to these proposals, the Government is also expressly seeking the views of the PJCIS on the following matters:

- expanding the basis of interception activities;
- establishing an offence for failure to assist in the decryption of communications;
- instituting industry response timelines; and
- applying tailored data retention periods for up to two years for parts of a data set, with specific timeframes taking account into agency priorities and privacy and cost impacts.[77]

Law Council's Concerns

Reducing the number of agencies eligible to access communications information

116. The Law Council supports efforts to reduce the number of agencies eligible to access stored communications information under the TIA Act.[78]

117. Section 110(1) of the TIA Act currently provides that "an enforcement agency "may apply to an issuing authority for a stored communications warrant in respect of a person. "Enforcement agency" is defined in section 5 of the TIA Act and includes the AFP, the ACLEI, the ACC, CrimTrac and a broad range of Commonwealth, State and Territory law enforcement, intelligence and oversight bodies including bodies which impose pecuniary penalties and protect public revenue, such as the ATO.

118. The current provisions regulating covert access to stored communications and introducing an expansive definition of "enforcement agency" were introduced and

[76] Discussion Paper p. 24.
[77] Discussion Paper p.10.
[78] As noted above, the regulatory reach of the TIA Act is limited to stored communications accessed covertly. The Law Council also supports efforts to reduce the number of agencies able to access stored communications overtly but this appears to be outside of the scope of the current Discussion Paper.

passed in 2006.[79] The 2006 amendments sought to clarify the position surrounding access to stored communications which had previously been under dispute.

119. The 2006 amendments were subject to an inquiry by the Senate Committee on Legal and Constitutional Affairs.[80] During this Inquiry, many submissions argued that the range of agencies that are able to apply for stored communications warrants should be limited. It was submitted that the extension of access provided by the 2006 amendments struck the wrong balance between protection of privacy and other public interests.[81]

120. The Senate Committee shared this concern and expressed the view that:

> *"The Bill would result in a wide number of government agencies being able to covertly obtain material for investigating a significant range of sometimes relatively minor offences.*
>
> *The Committee is of the view that the invasion of privacy resulting from covert interception of communications is significant and should therefore only be accessible to core law enforcement agencies."*[82]

121. The Senate Committee recommended that the enforcement agencies able to access stored communications should be limited to those agencies eligible under the pre-existing arrangements for telecommunications interception, which was limited to law enforcement agencies responsible for investigating criminal matters. [83]

122. However, this recommendation was not reflected in the amendments as passed.[84] Nevertheless, the Law Council maintains the view that the number of agencies which currently have access to stored communications under the TIA Act should be limited as suggested in the Discussion Paper.

123. As the Law Council has previously submitted,[85] unless a compelling case can be made for why the agencies or bodies referred to in section 5 of the TIA should remain within the definition of an enforcement agency, they should be removed.

Standardisation of warrant thresholds

124. The Law Council supports efforts to review the current offence thresholds that apply to obtaining a warrant to access or share a stored communication. Currently, two penalty thresholds must be met in relation to accessing and using stored communications:

---

[79] See *Telecommunications (Interception) Amendment Act 2006*

[80] Senate Committee on Legal and Constitutional Affairs *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* 27 March 2006 available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/ti/report/index.htm.

[81] For example see Submission by the Australian Privacy Foundation *Telecommunications (Interception) Amendment Bill 2006* Inquiry by the Senate Legal & Constitutional Committee (March 2006) available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/ti/submissions/sublist.htm

[82] Senate Committee on Legal and Constitutional Affairs *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* 27 March 2006 paras 3.40-3.41.

[83] Senate Committee on Legal and Constitutional Affairs *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* 27 March 2006 Recommendation 2

[84] The Government's response to the recommendations of the Senate Committee is available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/ti/index.htm

[85] Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into Telecommunications (Interception and Access) Bill 2007* (July 2007).

(a) an initial penalty threshold that must be met for a stored communications warrant to be issued; and

(b) a lower penalty threshold for the secondary use and disclosure of information which has been accessed under a stored communications warrant.

125. In relation to the initial penalty threshold, section 116(1)(d) of the TIA Act provides that stored communications warrants may be issued to agencies if the information likely to be obtained would assist in connection with an investigation of a "serious contravention". A "serious contravention" is defined in section 5E (1) as a contravention of a law of the Commonwealth, a State or a Territory that:

(a) is a serious offence; or

(b) is an offence punishable:

(i) by imprisonment for a period, or a maximum period, of at least 3 years; or

(ii) if the offence is committed by an individual--by a fine, or a maximum fine, of at least 180 penalty units; or

(iii) if the offence cannot be committed by an individual--by a fine, or a maximum fine, of at least 900 penalty units; or

(c) could, if established, render the person committing the contravention liable:

(i) if the contravention were committed by an individual--to pay a pecuniary penalty of 180 penalty units or more, or to pay an amount that is the monetary equivalent of 180 penalty units or more; or

(ii) if the contravention cannot be committed by an individual--to pay a pecuniary penalty of 900 penalty units or more, or to pay an amount that is the monetary equivalent of 900 penalty units or more.

126. In relation to the secondary use penalty threshold, section 139 of the TIA Act provides that an enforcement agency may share lawfully accessed information or stored communications warrant information with another person for purposes connected with an investigation by the agency or by another agency of a contravention of a law of the Commonwealth, a State or a Territory that is:

(a) a serious offence;[86] or

(b) an offence punishable by imprisonment for a period, or a maximum period, of at least 12 months or a fine, or a maximum fine, of at least 60 penalty units (for individuals) or at least 300 penalty units (for organisations); or

(c) could, if established, render the person committing the contravention liable to pay a pecuniary penalty of 60 penalty units or more (for an individual), or 300 penalty units or more (for organisations).

127. Lawfully accessed information or stored communication warrant information can also be shared by an agency for the purposes of a proceeding by way of a prosecution for an offence of a kind referred to above, as well as a proceeding:

[86] As defined in section 5D of the TIA Act.

(a) for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of such an offence; or

(b) under the *Spam Act 2003* ; or

(c) for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to such an offence; or

(d) for the extradition of a person from a State or a Territory to another State or Territory, in so far as the proceeding relates to such an offence; or

(e) for recovery of a pecuniary penalty for a contravention of a kind referred above; or

(f) a police disciplinary proceeding.

128. The penalty thresholds for which a stored communications warrant may be issued, are significantly less than those applying to the issue of telecommunications interception warrants, which can only be issued in respect of offences punishable by imprisonment for a period of at least seven years. At the time these thresholds were introduced, the Attorney-General's Department advised that the distinction between the penalty thresholds had been recommended by the 2005 Blunn report of the review of the regulation of access to communications[87] and was based on the supposition that something that is in writing, such as emails or a text message, involves more consideration of the expression than other more spontaneous forms of communication which do not provide the opportunity for 'second thoughts' prior to transmission'.[88]

129. During its inquiry into the 2006 amendments that introduced the current penalty thresholds in respect of stored communications, the Senate Committee on Legal and Constitutional Affairs received a number of submissions that contradicted this view. For example, the Australian Privacy Foundation submitted that:

> *"The principle that invasion of privacy through covert interception should only be allowed in relation to genuinely serious offences is clearly established in the existing regime. In our view, no convincing case has been mounted for why a lower threshold should apply to stored communications, which can contain information just as private, sensitive and even intimate. In the absence of any such case, it is difficult to have a rational discussion about where the threshold should be set, but we strongly urge the Committee to recommend higher thresholds than those proposed".*[89]

130. Many submissions also raised concerns about the lower secondary threshold for sharing stored communication information which allows such information to be

[87] Anthony S Blunn, *Blunn report of the review of the regulation of access to communications* (August 2005) available at http://www.ag.gov.au/Publications/Pages/BlunnreportofthereviewoftheregulationofaccesstocommunicationsAugust2005.aspx at 1.4

[88] Senate Committee on Legal and Constitutional Affairs *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* 27 March 2006 available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/ti/report/index.htm

[89] Australian Privacy Foundation submission to the Senate Committee on Legal and Constitutional Affairs *Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* available at http://www.privacy.org.au/Papers/index.html

shared for the purpose of proceedings into offences carrying a punishment of 12 months imprisonment or 60 penalty units, for example.[90]

131. The Senate Committee recommended that the penalty thresholds in relation to the issue of stored communications warrants be raised to include only criminal offences.[91] However this recommendation was not adopted in the amendments as passed.

132. The Law Council is of the view that it is appropriate for the offence threshold for stored communication warrants to be reviewed and raised to apply only to criminal offences. Consideration should also be given to raising this threshold to 'serious offences', as defined in section 5D of the TIA Act, in recognition of the private nature of stored communication information and to better align the stored communication warrant process with that required for telecommunication interception warrants. As acknowledged in the Discussion Paper:

> *"The threshold for access [to stored communications] is lower than for interception because it was considered at the time the provisions were introduced that communicants often have the opportunity to review or to delete these communications before sending them, meaning covert access can be less privacy intrusive than real-time listening. However, this logic, while valid several years ago, has become less compelling as technology use and availability has changed."*[92]

133. The Law Council also suggests that the lower threshold for sharing stored communication needs to be reviewed. It is not clear why the sharing of this information should be authorised in respect of proceedings and investigations relating to much less serious offences. In the absence of compelling evidence to the contrary, the Law Council suggests that there should be no distinction made between the offence thresholds prescribed in sections 110 and 139 of the TIA Act.

134. In making this suggestion, the Law Council also notes that it has previously raised concerns with the penalty thresholds relating to telecommunications interception warrants, particularly when amendments have been introduced that have expanded the telecommunication interception regime to cover a range of new offences of a substantially different character to the original definition of 'serious offence'.[93]

Standardisation of warrant processes

135. The Discussion Paper provides only a broad outline of what is meant by a 'simplified warrant regime', but it would appear to be referring to warrants authorising interception of telecommunications and warrants authorising access to stored communications.[94] It also suggests that such a simplified regime would remove or amend the current provisions that require warrant applications to include details such as the communicant, carrier-provided service or telecommunication device on

---

[90] For example, see Electronic Frontiers Australia submission to the Senate Committee on Legal and Constitutional Affairs *Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* available at https://www.efa.org.au/Issues/Privacy/tia-bill2006.html

[91] Senate Committee on Legal and Constitutional Affairs *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006* 27 March 2006 Recommendation 3

[92] Discussion Paper p. 24.

[93] Law Council of Australia submission to the Senate Committee on Legal and Constitutional Affair's Inquiry into the provisions of the *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009* (29 August 2009) available at http://www.lawcouncil.asn.au/shadom.x/apps/fms/fmsdownload.cfm?file_uuid=5FEEEFAE-1E4F-17FA-D2E6-8084811EA9AC&siteName=lca.

[94] Discussion Paper p. 25.

the basis that complying with these provisions can be time consuming and costly for agencies and can result in the analysis of unnecessary information.

136. The Law Council recognises the challenges existing and emerging telecommunications technologies pose for agencies attempting to accurately identify the communications they intend to intercept or access. For this reason, the Law Council generally supports efforts to develop a warrant regime that focuses on better targeting the characteristics of a communication and enables it to be isolated from communications that are not of interest. However, the Law Council is keen to ensure that any proposed "simplification of the warrant process" does not occur at the expense of specific provisions designed to ensure that each particular device or service to be intercepted or communication to be accessed is clearly identified and shown to be justifiable and necessary, and that it occurs in a manner that has the least intrusive impact on individual rights and privacy.

137. This means that, at a minimum, the issuing authority or authorising officer needs to be satisfied that:

- the person whose telecommunications are to be intercepted or accessed is a legitimate target of suspicion from a security or law enforcement perspective; and
- in relation to telecommunication interception, that:
  - each and every telecommunications service or telecommunications device to be intercepted is, in fact, used or likely to be used by the relevant person of interest;
  - each and every telecommunications service or telecommunications device to be intercepted can be uniquely identified such that relevant telecommunications made using that service or device can be isolated and intercepted with precision; and
- in relation to accessing a stored communication or data, that:
  - there are reasonable grounds for suspecting that a particular carrier holds stored communications: that the person of interest has made; or that another person has made and for which the person is the intended recipient.

138. In addition, the issuing authority or authorising officer should have regard to:

- the likely benefit to the investigation which would result from the interception or access substantially outweighing the extent to which the interception or access is likely to interfere with the privacy of any person or persons;
- the gravity of the conduct constituting the offence or offences being investigated;
- how much the information referred to would be likely to assist in connection with the investigation by the agency of the offence or offences; and
- to what extent methods of investigating the offence or offences that do not involve intercepting communications or accessing data have been used by, or are available to, the agency.

139. Requiring the issuer of the warrant to be satisfied of all these matters recognises that there are a number of ways that telecommunications interception or accessing stored communications may inadvertently result in the unjustified invasion of a person's privacy. For example the agency which seeks to intercept or access the telecommunication:

- may have erroneously identified their suspect, perhaps as a result of acting prematurely or on the basis of unreliable information; or
- may have misjudged the nature of the communications that the targeted person was likely to engage in using the intercepted service or device and as a result the information obtained may be entirely personal and of no relevance to the investigation; or
- may have correctly identified their suspect *but* may have erroneously identified the telecommunications services or devices used by that person (again perhaps on the basis of incomplete or unreliable information), with the result that the communications of an innocent third party are intercepted; or
- may have correctly identified their suspect and correctly identified the telecommunication service or devices used by that person *but* may not be technically able to uniquely identify telecommunications made using that service or device without the risk of intercepting communications made via an unrelated service or device.

140. The Discussion Paper provides a number of examples of changes in telecommunications device technology and the way communications and data is transferred, that are said to be giving rise to complexities and difficulties for interception agencies.[95]

141. While it may not always be possible to identify communicants, carrier-provided services or particular communication devices in the same way that such characteristics of communications have been identified before, this does not of itself point to the need to dispense with the need to isolate the particular communication or communications subject to the warrant. Rather, it suggests that alternative means of uniquely identifying particular communication or communications must be adopted or developed to ensure that the warrant process remains transparent and capable of effective external review.

142. Similar matters have been raised by the Law Council and other bodies each time amendments have been introduced into the TIA Act that seek to overcome the challenges posed by changes in telecommunications technology and the way communications are transferred between users. Many of these amendments have diluted the requirement to accurately identify the communication the subject of the warrant, and as a result, weaken those protections designed to protect against or limit intrusion into personal privacy.

143. An example is the *Telecommunications (Interception and Access) Amendment Bill 2008,* which extended the pre-existing device-based named person warrant regime to authorise the interception of communications made by multiple telecommunications devices. When this Bill was introduced, the Law Council raised concerns that the amendments effectively authorised interception of communications from any telecommunications device used by the named person, regardless of whether the device had been referred to at all in the warrant process.

[95] Discussion Paper p. 21.

144. These amendments constituted a significant departure from the pre-existing provisions governing the issue of device-based named person warrants which required the officer seeking the warrant to provide sufficient details to identify *the particular* device that the person named in the warrant was using or likely to use. Under the previous provisions, if a warrant was issued, the particular telecommunications device had to be identified in the warrant and only communications made by means of that particular device could be intercepted pursuant to the warrant.

145. While the Law Council recognised the efficacy of a single warrant to authorise interception of telecommunications made by means of multiple devices, it submitted that each of those devices must be named in the warrant and the issuer of the warrant must be satisfied that:

- the person named in the warrant is using or is likely to use each device from which communications will be intercepted;
- each of the devices used or likely to be used by the named person can be uniquely and reliably identified for interception purposes; and
- the communications likely to be made by means of each device from which communications will be intercepted are likely to yield information useful to the investigation.

146. However these recommendations were not adopted in the amendments as passed. As a result, under the current provisions of the TIA Act, ASIO and law enforcement agencies are able to obtain a blanket authorisation to intercept all communications made to or from any telecommunications device used by the named person, regardless of whether the device has been referred to at all in the warrant process. [96] They are also able to obtain a blanket authorisation to intercept all communications made to or from *any telecommunications service* used by a named person of interest, without having to exhaustively list those services.[97]

147. The Law Council believes that the provisions which govern the issue of these warrants, which can cover all the devices and services used by a certain person, provide inadequate external oversight and safeguards against the inadvertent interception of the private communications of innocent third parties.

148. The Law Council cautions against further amendments which consider these more liberal provisions to be the default standard to which other warrant regimes are aligned. The Law Council also cautions against any attempt to remove or reduce the list of matters that a relevant officer must take into account when issuing a warrant to law enforcement officers, such as those outlined in sections 46 and 116, which include the gravity of the offence being investigated, the impact the interception or access will have on the privacy of the individual and the availability of any alternative means of obtaining the relevant information.

149. To ensure that these important components of the warrant process are not diluted, the Law Council suggests that the PJCIS requests further detail regarding the proposal in the Discussion Paper. For example, the following questions could be asked:

[96] See TIA Act ss9A and 46A.
[97] See TIA Act ss9 and 46.

- What particular interception and access activities are being hindered or limited by the current warrant processes?

- What particular requirements within the existing warrant provisions are giving rise to complexity and the analysis of unnecessary information? Are these issues more strongly felt in relation to particular interception or access activity?

- What recent efforts have been made to develop a unique and indelible identifier of the source of telecommunications as a basis for access?

- If attributes such as communicant, carrier provided service or devices are not used to identify and isolate communications for the purpose of interception and access, what alternative characteristics could be used for this purpose?

- How would the 'simplified warrant regime' strengthen and enhance existing and proposed provisions designed to protect against unjustified or unnecessary intrusion into personal privacy?

Expanding the basis of interception activities

150. The Discussion Paper provides that the Government is expressly seeking the views of the PJCIS on "expanding the basis of interception activities" under the TIA Act. While this proposal is not fully outlined in the Discussion Paper, the Paper does note that the current exclusion of providers such as social networking providers and cloud computing providers creates potential vulnerabilities in the interception regime that are capable of being manipulated by criminals. It suggests that consideration should be given to extending the interception regime to such providers to remove uncertainty.[98]

151. Given the absence of detail in relation to this particular proposal in the Discussion Paper, it is difficult for the Law Council to assess the degree to which such a reform would undermine the primary purpose of the TIA Act and the impact the reform may have on the privacy rights of individuals. There is also little specific information provided to explain why expanding the basis of interception activities is necessary for the purposes of investigating criminal activity or threats to national security, and whether such an expansion is a proportionate response, particularly in light of the already extensive interception and access powers currently contained in the TIA Act.

152. While the Law Council does not have any particular expertise or insights into the challenges that may be posed by social networking providers and cloud computing providers in the investigation and prosecution of criminal activity or in the investigation of threats to national security, it suggests that compelling evidence would need to be shown that existing or alternative mechanisms are currently inadequate to meet these challenges, before the current basis for interception and access of telecommunications is further expanded. The Government would also need to explain how such interception or access would work in practice and address any technical concerns relating to its effectiveness.

153. The Law Council also suggests that a thorough and independent assessment of the privacy impacts of the proposed reform would need to be undertaken that would consider for example, how a particular individual's information or communication would be isolated from information or communications made by other individuals who are not of interest to law enforcement or intelligence agencies, and how

[98] Discussion Paper p. 27.

particularly sensitive personal information (including visual images or information disclosing attributes such as sexual preference or relationship status) would be handled. The information that could be obtained from intercepting or accessing social media, for example, has the potential to be considerably more privacy intrusive than that obtained from existing interception and access powers.

154. As noted above, the unrelenting advances in telecommunication technologies should not of themselves give rise to an equally unrelenting expansion of interception and access powers for law enforcement and intelligence officers – particularly when the privacy impacts of these powers are significant and their effectiveness at combating criminal activity or threats to national security are not yet clear. It is important to keep in mind that one of the primary purposes of the TIA Act is the protection of individual privacy and the criminalisation of unauthorised interference with telecommunications. The remaining provisions are intended as exceptions to this general rule. Any proposed additional exception must be subject to robust scrutiny to ensure that it is necessary and proportionate, both in terms of the criminal activity or national security threat it aims to prevent, and in terms of its privacy impact.

155. If more detailed information on this proposal is provided, the Law Council would be pleased to provide further views, including views regarding the types of safeguards that would need to be incorporated in any additional interception or access activities authorised under the TIA Act.

Establishing an offence for failure to assist in the decryption of communications

156. The Discussion Paper explains that changes to the telecommunications environment, combined with increased data flows and volumes, "mean that it is now extremely costly to reliably identify and access communications."[99] It further provides that once a communication has been accessed, its content is not necessarily clear:

> *"In IP based communications, the content of communications is embedded in data packets in a form which is not readily able to be reconstructed and interpreted outside of the transmitting and receiving terminal devices and the applications running on them. Data used to route, prioritise and facilitate the communications is also embedded along with the content, in the communications packets. This means that agencies must further process communications accessed under an interception warrant to extract and reconstruct the content.*
>
> *The use of encryption and propriety data formats and typically large data volumes, makes reconstructing communications into an intelligent form difficult for agencies."*[100]

157. The Discussion Paper states that the Government is seeking the views of the PJCIS on the establishment of an offence for failure to assist in the decryption of communications.

158. It is difficult for the Law Council to respond in detail to this proposal, which is referred to only in general terms in the Discussion Paper.

159. As discussed above, the Law Council supports a robust authorisation procedure regarding access to stored communications which permits access to

[99] Discussion Paper p. 22.
[100] Discussion Paper p. 22

communications only when such access has been shown to be necessary after a range of factors, including privacy, have been taken into account.

160. However, the Law Council also appreciates the need to ensure that officers who have been authorised to access communications can do so in an effective, meaningful way.

161. To this end, the Law Council does not oppose mechanisms to assist agencies to reconstruct or decrypt the content of communications to which access has been authorised.

162. It notes for example, that the Telecommunications Act already obliges carriers and carrier service providers to provide such help to agencies as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting public revenue and safeguarding national security.[101]

163. However, it is not clear on the basis of the information provided in the Discussion Paper that the introduction of a criminal offence, presumably aimed at participants in the telecommunications industry such as carriers and carriage service providers, would be an effective or appropriate response, particularly when other non-punitive efforts may to be available to enhance cooperation between the agencies and the telecommunication industry.

164. Before introducing criminal liability for failing to assist in the decryption of communications, the Law Council suggests that the PJCIS requests that information be provided by the Attorney-General's Department that explains whether the proposed offence adheres to the principles contained in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.[102] The following questions could also be put to the Attorney-General's Department to assist in the PJCIS's consideration of this proposed offence:

- What is the prevalence of the use of encryption in the communications law enforcement or intelligence agencies have accessed or seek to access?
- What impact is this having on the ability of these agencies to fulfil their investigative functions?
- What role has the telecommunication industry previously played in assisting these agencies to decrypt these communications? What impact has this had on the industry in terms of financial and human resources?
- To what extent has the telecommunications industry complied with its existing obligations under the Telecommunications Act to provide reasonable assistance to law enforcement and other agencies?
- Would the introduction of a criminal offence of this nature enhance any existing levels of cooperation from the telecommunication industry?
- What would be the penalty for failing to assist and how would this offence be investigated and enforced?

[101] See for example Telecommunications Act s280.

[102] This Guide is developed by the Criminal Justice Division of the Attorney-General's Department to assist officers in Australian Government departments to frame criminal offences, infringement notices, and enforcement provisions that are intended to become part of Commonwealth law A copy can be found at http://www.ag.gov.au/Publications/Pages/GuidetoFramingCommonwealthOffencesCivilPenaltiesandEnforcementPowers.aspx.

- How would the offence identify which industry participant is responsible for decrypting the communication, and how would it address a situation where the particular participant lacks the technical skills or resources necessary to assist in decryption?

- Would the offence seek to capture telecommunication industry participants located outside of Australia?

Tailored data retention periods for up to 2 years

165. The Discussion Paper states that the Government is 'expressly seeking' the views of the PJCIS on a proposal that would require telecommunication industry participants to retain certain telecommunications data for up to two years, with specific timeframes taking into account agency priorities and privacy and cost impacts. [103]

166. This proposal is not outlined in any detail in the Discussion Paper, however, it is noted that:

> *"Currently, authorised access to telecommunications data, such as subscriber details, generated by carriers for their own business purposes is an important source of information for agencies. As carrier's business models move to customer billing based on data volumes rather than communication events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations."*[104]

167. Currently, telecommunications industry participants are not required to retain telecommunications data for a prescribed period. While some companies voluntarily retain data for such periods, others delete users' call records and internet usage data almost as quickly as they receive it.

168. As the Law Council has previously submitted to the ALRC's 2007 Privacy Inquiry, while telecommunications data does not include the content and substance of a person's private communications, it nonetheless contains information about crucial matters such as their associations and their whereabouts.[105] For that reason, while a wide range of agencies have access, without a warrant, to telecommunications data, the highly personal nature of such data should not be underestimated and its use and retention ought to be tightly controlled.

169. Introducing a requirement to retain certain data for up to two years, even with accompanying safeguards, constitutes a significant expansion of the telecommunications interception and access regime, and one that the Law Council considers has not yet been shown to be a necessary or proportionate response to investigating serious criminal activity or safeguarding national security, particularly given the very serious impacts such a reform will have on the privacy rights of many members of the community.

170. From the little information provided in the Discussion Paper, it is not clear that such a requirement will be technically feasible or even useful to law enforcement or intelligence agencies. For example, how will those responsible for retaining the data guarantee confidentiality and security when it is stored? Once the data has been

[103] Discussion Paper p. 21
[104] Discussion Paper p. 21
[105] See Law Council of Australia submission to the Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law* (20 December 2007).

retained, how will it be matched with a particular person or communication? How will it be verified, and if it is used as evidence in court, how will it be protected from public disclosure? In addition, how will authorised agencies deal with the sheer volume of data retained when attempting to identify and request the data needed for a particular investigation?

171. As noted briefly in the Discussion Paper, this reform will also have significant cost implications for industry participants responsible for retaining such data, which could ultimately be passed onto consumers.

172. The Law Council notes that some data retention schemes have been established in overseas jurisdictions and have generated considerable public debate. For example:

    (a) In 2006 the European Union issued the Data Retention Directive, which requires Member States to ensure that communications providers retain, for a period of between six months and two years, necessary data as specified in the Directive for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. Since its introduction, serious concerns have been raised about its compatibility with the rights to privacy and other rights protected under the ECHR.[106]

    (b) The United Kingdom (UK) has a system of voluntary data retention which derives from Part 11 of the *Anti-Terrorism, Crime and Security Act 2001*. Telephone operators and Internet Service Providers retain some data under a voluntary arrangement with the UK Home Office.

    (c) The UK has also recently been considering a compulsory scheme of data retention, which has attracted serious criticism from service providers in response to compliance costs. Such a scheme may also fail to comply with the UK's obligations under the ECHR*,* particularly Article 8 which protects the right to privacy and provides only limited exceptions if an interference with an individual's right to privacy is necessary in the interests of national security and the prevention and detection of certain types of crime.[107]

173. There are a number of features of the reform proposed in the Discussion Paper that suggest that, if such a data retention requirement were introduced in Australia, it would be contrary to the human rights obligations Australia has assumed, such as the obligation in Article 17 of the ICCPR to protect against unjustified intrusion into personal privacy. These features include:

    - The privacy invasive nature of telecommunications data which can reveal the geographical movements of a person, as well as details of a person's political, financial, sexual, religious stance, or other interests. For example, in the case of mobile phones, telecommunications data includes information not only about who the user has communicated with, when and for how long; it also includes accurate information about the user's location.

[106] For example see Bignami, Francesca (2007), "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law* 8 (1): 233–256, Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11(3) *European Law Journal, ,* pp. 365–375.

[107] For further discussion see Patrick Breyer, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11(3) *European Law Journal, ,* pp. 365–375.

- The fact that the data that would be retained under this requirement would not be limited to data generated by criminal suspects or persons of interest to ASIO, but would include the data generated by all members of the community using telecommunication services and devices. As Patrick Breyer has noted, commenting on the experience of data retention requirements in Europe, this effectively amounts to monitoring of citizens by the state just in case this information is useful for future investigations or inquiries by law enforcement or intelligence agencies. It constitutes an approach which does not sit easily with the notion of the presumption of innocence or other traditional criminal law or human rights principles. [108]

- The absence of clear evidence that retention of telecommunications data is effective at preventing crime or safeguarding national security. For example, the existence of various ways of communicating anonymously, the use of which is likely to increase as a reaction to the introduction of mandatory data retention, raises fundamental doubts as to the effectiveness of data retention in terms of investigating or preventing criminal activity or safeguarding national security. Any proposed benefits of data retention are also likely to be undermined by the expanding use of telecommunication industry participants located outside Australia that may not be required to retain such data.

- The potential for errors or oversight to occur when telecommunications data is accessed or used in criminal investigations and court procedures. This can occur due to the difficulties in determining a user's identity for a given telecommunications service, at a given time, and the fact that access to telecommunications data affects a multitude of individuals simultaneously.

- The potential for misuse of the data by third parties. Innumerable facts about the private life of members of the public could be obtained by unauthorised third parties analysing telecommunications data, and once such misuse occurs it could be difficult to repair any harm caused to individuals or communities.

174. From the information provided in the Discussion Paper, neither the positive nor the negative effects of telecommunications data retention can be determined with certainty. The Law Council suggests that further empirical information about the benefits of telecommunication data retention for the purposes of investigating and preventing criminal activity and safeguarding national security would need to be provided before such a proposal could be approved.

175. Even if such information is available and provided to the PJCIS, the Law Council submits that the implementation of this reform, which includes serious and irreversible restrictions on human rights, should not occur unless it is shown to be indispensable to protect the community from serious threats of criminal activity or national security.

176. The Law Council also queries whether the use of specific time frames or safeguards within a compulsory data retention scheme would be effective at mitigating the types of intrusions into personal privacy described above. Although the Discussion Paper does not outline what time frames or safeguards would apply, it is clear that the existing safeguards and accountability provisions in respect of telecommunications data in the TIA Act would be inadequate in the face of the extensive intrusion into the personal privacy that a requirement to retain data would pose. The gaps in privacy safeguards in the current provisions relating to telecommunications data

[108] Ibid.

have been discussed earlier in this submission; the inadequacies in the reporting and information sharing provisions relating to telecommunications data are discussed below.

177. The Law Council also cautions against adopting a voluntary retention of data scheme as an alternative to that proposed in the Discussion Paper. Voluntary schemes may result in less data being retained as some providers may opt out of retaining data. Therefore they may be less effective at achieving their aims. If telecommunication industry participants can choose to opt out, this may provide an option for sophisticated criminals to use those participants.

178. If telecommunication industry participants opt in to a voluntary scheme, the impact on the privacy rights of individual users of those providers may still be the same as for a mandatory scheme of data retention, depending on the privacy safeguards included in the schemes. However, as users may be able to choose a provider who has opted out, the proportion of users affected by privacy impacts may be less than under a mandatory scheme.

179. The Law Council considers that these factors relating to mandatory or voluntary data retention schemes need to be carefully weighed in assessing whether either proposal should be adopted. The experience in overseas jurisdictions should be taken into account.

Streamlining and reducing complexity in the lawful access regime

Current Information Sharing and Reporting Requirements

Information obtained from Telecommunication Interception Warrants

180. The TIA Act contains a number of reporting requirements in relation to telecommunication interception, as well as requirements to destroy records of intercepted information. For example:

- The Attorney-General must be given copies of telecommunications interception warrants and revocations and reports on outcomes;[109]
- The Managing Director of a carrier who enables interception to occur under a warrant must report to the Attorney-General within three months of the warrant ceasing to be in force.[110]
- The Secretary of the Attorney-General's Department must maintain a General Register which includes particulars of all telecommunications interception warrants[111] and this must be delivered to the Attorney-General for inspection every three months.[112]

[109] Sections 57, 59A and 94 of the TIA Act provides that the chief officer of each interception agency must give to the Attorney-General: a copy of each telecommunications interception warrant issued to that agency; each instrument revoking such a warrant, and within three months of a warrant ceasing to be in force, a written report about the use made of information obtained by interception under the warrant.
[110] TIA Act s97. The report must include details of the acts done by employees of the carrier to effect interception under the warrant and to discontinue interception when the warrant expires or is revoked.
[111] TIA Act s81A.
[112] TIA Act s81B. Interception agencies are notified once the Attorney-General has inspected the General Register to enable the destruction of restricted records in accordance with section 79 of the TIA Act.

- The Attorney-General's Department must maintain a Special Register recording the details of telecommunications interception warrants which did not lead to a prosecution within three months of the expiry of the warrant.[113]

- Agencies must destroy restricted records which are original records.[114] Once the chief officer of the agency is satisfied that the record will not be needed for any permitted purpose and the Attorney-General has inspected the relevant Register, those records must be destroyed.

181. The TIA Act also contains a number of mechanisms designed to provide independent oversight of the telecommunication interception regime, such as:

- The Attorney-General must prepare and table in Parliament each year a report setting out the information specified in Part 2-8 of the TIA Act.[115]

- The ACC, ACLEI and the AFP are required to maintain records relating to interceptions and the use, dissemination and destruction of intercepted information.[116] These records must be inspected by the Commonwealth Ombudsman on a regular basis.

- The Commonwealth Ombudsman is required to report to the Attorney-General regarding these inspections and to include in his or her report a summary of any deficiencies identified and any remedial action taken. [117]

- Parallel requirements are imposed by State and Territory legislation on State and Territory interception agencies. [118]

182. As it noted in the Discussion Paper, while the Commonwealth Ombudsman is responsible for inspecting the records of the ACC, ACLEI and the AFP, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies.[119] The reports of the inspections of the declared State and Territory agencies are given to the responsible State or Territory Minister who must provide a copy to the Commonwealth Attorney-General.[120]

183. Section 63 of the TIA Act contains a general prohibition on the communication or use of any lawfully intercepted information. The following sections then provide a range of exceptions to this general rule. For example, these exceptions permit:

(a) an employee of a carrier to communicate or use lawfully intercepted information other than foreign intelligence information or interception warrant information for a purpose or purposes connected with the investigation by an agency of a serious offence;[121]

---

[113] TIA Act s81C. The Special Register is delivered to the Attorney-General for inspection together with the General Register.
[114] TIA Act s79. Once the chief officer of the agency is satisfied that the record will not be needed for any permitted purpose and the Attorney-General has inspected the relevant Register, those records must be destroyed.
[115] TIA Act s99, 104.
[116] TIA Act s80.
[117] TIA Act ss83-86.
[118] TIA Act ss34, 35, 92A.
[119] Instead of the State Ombudsman, inspection of the SA Police is undertaken by the Police Complaints Authority (South Australia), while inspections of the Vic Police and the OPI are undertaken by the Special Investigations Monitor (Victoria). See Attorney General's Department *Telecommunications (Interception and Access) Act 1979 - Annual Report for the year ending 30 June 2011.*
[120] TIA Act s35.
[121] TIA Act s65A.

(b) subject to certain limitations, the Director General of ASIO or an officer of ASIO to communicate, use or record lawfully intercepted information other than foreign intelligence information or interception warrant information in connection with the performance by ASIO of its functions, or otherwise for purposes of security;[122]

(c) the chief officer of an agency to communicate lawfully intercepted information that was originally obtained by the agency or interception warrant information to the Director General of ASIO if the information relates, or appears to relate, to activities prejudicial to security, or if the information relates, or appears to relate, to the commission of a relevant offence in relation to another agency, to that agency (such as the AFP or a Police Force of a State).[123]

184. Section 77 of the TIA Act provides that intercepted material and interception warrant information will generally not be admissible in criminal proceedings.

Information obtained under a Stored Communications Warrant

185. Under the TIA Act certain records must also be kept in relation to stored communication warrants. For example, section 151 provides that the chief officer of an enforcement agency must cause to be kept: each stored communications warrant issued; each instrument of revocation; copies of authorisations which authorise persons to receive stored communications, and particulars of the destruction of information.

186. The TIA Act also provides that the Commonwealth Ombudsman must conduct regular inspections of records and report to the Attorney-General on the results of those inspections. [124] The Attorney-General is also required to prepare and table in Parliament each year a report setting out the information specified in Part 3-6 of the TIA Act.[125]

187. Section 133 of the TIA Act contains a general prohibition on communicating, using or recording accessed information or stored communication warrant information, or giving this information in evidence in a proceeding.[126] The Act then outlines certain exceptions to this general rule, for example:

(a) an employee of a carrier can communicate information obtained by accessing stored communications under a stored communications warrant to the officer of the enforcement agency;[127]

(b) a person can communicate to another person, make use of, or make a record of lawfully accessed information (other than foreign intelligence information) or stored communications warrant information in connection with the performance by ASIO of its functions, or otherwise for purposes of security; [128]

[122] TIA Act s64.
[123] TIA Act s68.
[124] TIA Act s153.
[125] TIA Act s161 and 164.
[126] TIA Act s133.
[127] TIA Act s135.
[128] TIA Act s136.

(c) the Director-General of Security or an officer or employee of ASIO can use or record foreign intelligence information in connection with the performance by the ASIO of its functions[129]

(d) the Director-General of Security can, in accordance with the relevant provisions of the ASIO Act,[130] communicate lawfully accessed information or stored communications warrant information to another person, for example a police officer if the information relates, or appears to relate, to the commission, or intended commission, of a serious crime;[131]

(e) an employee of a carrier can communicate lawfully accessed or stored communication warrant information to an enforcement agency for a purpose connected with that agency's functions, such as the ACMA in the performance of its functions under the *Spam Act 2003;*[132] and

(f) an officer or staff member of an enforcement agency or a Royal Commission can communicate or use lawfully accessed information (other than foreign intelligence information) or stored communications warrant information for purposes connected with an investigation by an enforcement agency of certain offences and other proceedings, such as the investigation of a serious criminal offence or a proceeding under the *Spam Act 2003.* [133]

188. Section 147 of the TIA Act provides that information obtained by accessing a stored communication will generally not be admissible in criminal proceedings.

Authorisations to Access Telecommunications Data

189. As noted earlier in this submission, section 172 of the TIA Act contains a general prohibition on disclosure of the contents or substance of a communication, or a document that contains the content or substance of a communication. Prohibitions on disclosure of this nature are also contained in Subdivision A of Division 3 of Part 13 of the Telecommunications Act. For example under section 276 of the Telecommunications Act it is an offence punishable by up to two years imprisonment for a person to disclose or use any information or document that relates to the contents or substance of a communication or the affairs or personal particulars (including any unlisted telephone number or any address) of another person. It is also an offence to disclose this information to other persons.[134]

190. However, the TIA Act also makes it clear that the relevant provisions of the Telecommunications Act[135] do not prohibit voluntary disclosure by the holder of information or documents:

(a) to ASIO if the disclosure is in connection with the performance by ASIO of its functions;[136]

(b) to a law enforcement agency if disclosure is reasonably necessary for the enforcement of the criminal law; [137]

[129] TIA Act s136.
[130] ASIO Act ss 18(3) or (4A), or s19A(4).
[131] TIA Act s137.
[132] TIA Act s138.
[133] TIA Act s139 .
[134] Telecommunications Act s277.
[135] Telecommunications Act ss276, 277, 278.
[136] TIA Act s174.
[137] TIA Act s177.

(c) to another enforcement agency if disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue.[138]

191. The TIA Act also allows senior ASIO officers to authorise access to historical telecommunications data.[139]

192. Authorisations can also be made allowing access to prospective telecommunications data. However, the senior ASIO officer must not make the authorisation unless he or she is satisfied that the disclosure would be in connection with the performance by ASIO of its functions and is for a period of not more than 90 days.[140]

193. The TIA Act also allows an authorised officer of an enforcement agency to authorise the disclosure of historical telecommunications data, if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law,[141] or for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue.[142]

194. Authorisations can also be also be made by enforcement agencies and State agencies for access to existing telecommunications data if this is necessary for the purpose of locating missing persons.[143]

195. Authorisations can also be made allowing access to prospective telecommunications data.[144]

196. Section 182 of the TIA Act prohibits secondary disclosure of telecommunications data, and contains an offence for contravening the section which is punishable by imprisonment for up to two years. However, certain disclosures are exempt from this provision, where the disclosure is reasonably necessary for the performance by ASIO of its functions, or for the enforcement of the criminal law, or for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. Exemptions are also provided for disclosure of missing person information to State or Federal police.

197. The TIA Act also requires the head of an enforcement agency to retain an authorisation to access telecommunications data for three years beginning on the day the authorisation is made, [145] and to provide to the Attorney-General statistics about the number of authorisations made.[146] The Attorney-General is also required to prepare and table in Parliament each year a report setting out this information.[147]

Nature of the Proposed Reforms

198. In addition to the reforms discussed above, the Government intends to pursue a range of additional reforms designed to streamline and reduce complexity in the lawful access to communications regime. This would include simplifying the information sharing provisions that allow agencies to cooperate.

[138] TIA Act s177.
[139] TIA Act s175.
[140] TIA Act s176.
[141] TIA Act s178.
[142] TIA Act s179.
[143] TIA Act s178A.
[144] TIA Act s180.
[145] TIA Act s185.
[146] TIA Act s186.
[147] TIA Act s186.

199. According to the Discussion Paper, the Government is also considering:

(a) creating a single warrant with multiple telecommunication interception powers;

(b) implementing detailed requirements for industry interception obligations;

(c) extending the regulatory regime to ancillary service providers not currently covered by the legislation; and

(d) implementing a three-tiered industry participation mode.

200. This submission will focus on those reform proposals that concern the information-sharing and reporting requirements under the TIA Act and the proposal to create a single warrant with multiple telecommunication interception powers.

Simplifying information sharing provisions and reporting requirements

201. In relation to the proposal to simplify the existing information sharing provisions, the Discussion Paper explains that:

- the Act prohibits the use and communication of information obtained under a warrant except for the purposes explicitly set out in the TIA Act;
- information obtained under the TIA Act is subject to more rigorous legislative protections than other forms of information in an agency's possession;
- the provisions are detailed and complex in relation to record keeping, retention and distribution and can present a barrier to effective information sharing both within an agency and between agencies; and
- this is particularly an issue now that more agencies are defined as interception agencies and because of the national and transnational nature of many contemporary security and law enforcement investigations. [148]

202. The Discussion Paper also explains that different record keeping requirements apply to intercepted communications compared with those applying to stored communications.[149]

"Oversight of law enforcement agencies' use of powers is split between the Commonwealth Ombudsman and equivalent State bodies in relation to interception activities. The Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications. This split in responsibility contrasts with the Surveillance Devices Act 2004, where the Commonwealth Ombudsman inspects all agencies." [150]

203. The Discussion Paper states that:

"The current regime is focused on administrative content rather than recording the information needed to ensure that a particular agency's use of intrusive powers is proportional to the outcomes sought. The existing provisions take a one size fits all approach, resulting in a lack of flexibility for each agency to determine the best way to record and report on information having regard to individual practices, procedures and use of technology.

[148] Discussion Paper p. 25.
[149] Discussion Paper p. 26.
[150] Discussion Paper p. 26.

The same provisions also impede the Ombudsman's ability to report on possible contraventions and compliance issues by prescribing detailed and time limited procedures that need to be checked for administrative compliance, rather than giving the Ombudsman scope to determine better ways of assisting agencies to meet their requirements.

Consideration should be given to introducing new reporting requirements that are less process orientated and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes."[151]

Law Council's Concerns

Simplifying Information Sharing Provisions

204. The Discussion Paper proposes to 'simplify' the existing information-sharing provisions in the TIA Act. Although it is not made clear in the Discussion Paper, the Law Council assumes this proposal relates to information obtained though telecommunications interception warrants, stored communications access warrants and authorisations to disclose telecommunications data ('information obtained under a TIA Act warrant or authorisation'). The Law Council also notes that this proposal appears to be limited to the information sharing provisions in the TIA Act that concern law enforcement agencies (which would suggest that it does not extend to intelligence agencies such as ASIO).[152] It is on this basis that the Law Council provides the following comments.

205. While the Law Council supports efforts to clarify the obligations of law enforcement officers when dealing with or sharing information obtained under the TIA Act, it does not support any proposals that would remove any current restrictions on the communication, use or disclosure of information obtained under a TIA Act warrant or authorisation.

206. It is important to recognise that under the TIA Act the sharing of information obtained under a warrant or authorisation is generally prohibited. Limited exceptions apply and these should be strictly applied to give effect to the primary purpose of the Act.

207. The Law Council is of the view that it is appropriate that information obtained under the TIA Act is subject to more rigorous legislative protections than other forms of information in a law enforcement agency's possession.

208. Sharing this type of information must necessarily be more restricted than sharing other information in order to recognise its particularly sensitive nature and the intrusive impact on a person's rights and privacy. It could include, for example, details of a person's most private conversations or the precise location of a person, and may include information in relation to non-suspects or other innocent third parties. Provisions relating to the sharing of this type of information must also reflect limits on the types of officers who are able to have primary access to this information.

209. While the Law Council agrees that the provisions should not be unnecessarily complex and could be clarified, it challenges the suggestion in the Discussion Paper that reforms should be introduced to "prevent a barrier to effective information

[151] Discussion Paper p. 26.
[152] See Discussion Paper footnote 27, p. 26.

sharing both within an agency and between agencies". The Law Council is of the view that there needs to be some barrier on information sharing to ensure that this information is only communicated, used or disclosed when absolutely necessary, and to protect against the potential for misuse or overuse of this information.

210. If reforms are considered in respect of the current information sharing provisions, the Law Council suggests that consideration be given to strengthening and clarifying the existing provisions, recognising that different restrictions on communication, use and disclosure may be appropriate in light of the nature of the information obtained, and depending on what types of agencies are able to have primary access to such information.

211. For example, the sharing of intercepted information is appropriately limited to law enforcement agencies and does not include other 'enforcement agencies' such as ACMA. Currently, a broader range of agencies are able to access stored communications information and it follows that the provisions relating to the communication, use and disclosure of this information are also broader. As the Law Council has argued earlier in this submission, it may be appropriate to review the range of agencies able to apply for stored communication warrants, and in turn limit the range of agencies with which this information can be shared.

212. Use and disclosure of telecommunications data is currently subject to different restrictions depending on whether the data is historical or prospective. For example, the disclosure of prospective telecommunication data cannot be made to general enforcement agencies, whose functions are limited to administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.

213. However, the Law Council believes that these limitations on which agencies can authorise the disclosure of prospective telecommunications data, and on the purposes for which they can authorise such disclosure, are undermined by unnecessarily broad secondary disclosure provisions.

214. For example, subsections 182(2) and (3) allow data obtained pursuant to a section 180 disclosure authorisation to be shared and used for a broad range of purposes such as for the performance by ASIO of its functions; or for the enforcement of the criminal law; or for the enforcement of a law imposing a pecuniary penalty; or for the protection of the public revenue.

215. The Law Council believes that the secondary disclosure provisions in section 182 should not allow a criminal law enforcement agency to disclose information obtained under a section 180 authorisation to an agency which is not itself able to authorise and access prospective telecommunications data.

216. Likewise, the Law Council believes that the secondary disclosure provisions in section 182 should not allow a criminal law enforcement agency to disclose information obtained under a section 180 authorisation for a purpose which is not itself capable of providing grounds for a section 180 authorisation.

217. The Law Council urges the PJCIS to take these considerations into account when considering proposals to 'simplify' the current provisions relating to information sharing. If any reforms of this nature are pursued, they should have as their goal the strengthening and clarifying of the existing limitations on communication, use and disclosure in line with the general prohibitions in the TIA Act, rather than merely making information sharing easier between and within agencies.

Simplifying Reporting Requirements

218. The Law Council notes that this proposal appears to be limited to the reporting requirements concerning law enforcement agencies which would suggest that it does not extend to intelligence agencies such as ASIO.[153] It is on this basis that the Law Council provides the following comments.

219. The Law Council strongly supports efforts to ensure that the reporting requirements and oversight mechanisms contained in the TIA Act are "…attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes", as suggested by the Discussion Paper. This may involve review and reform of the different procedural and administrative requirements currently contained in the TIA Act relating to reporting, and to the role of the Commonwealth Ombudsman and his or her State and Territory counterparts. It may also involve consideration of additional or alternative mechanisms to enhance accountability under the TIA Act.

220. However, the Law Council cautions against removing requirements for agencies to collect and record certain information about the exercise of their powers under the Act. For example, currently the Secretary of the Attorney-General's Department is required to keep a General Register of interception warrants that contains detailed information about each warrant, such as: the date it was issued; who issued it and to whom; the telecommunications service to which it relates; the name of the person likely to use this service; the period for which it is in force; and the serious offence to which it relates.[154] This can be contrasted with the less rigorous requirements that apply to stored communication warrants, which must be the subject of annual reporting by the chief officer of a law enforcement agency, but which are not required to be described in the same level of detail as interception warrants.

221. Each of these requirements have been included in the TIA Act as mechanisms to ensure that the Parliament and the public have a clear picture of how often these powers are being used, whether the requirements of the Act are being complied with and how useful the information obtained under the Act is to the legitimate purposes of the authorised agencies. Even if these requirements are administratively burdensome, they should not be removed in favour of "flexibility" or a "less process orientated" approach unless they are not fulfilling their accountability function.

222. The Discussion Paper notes that oversight of law enforcement agencies' use of powers is split between the Commonwealth Ombudsman and equivalent State bodies in relation to interception activities, and that the Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications.

223. It suggests that this contrasts to the reporting requirements currently contained in the *Surveillance Devices Act 2004* (Cth) (the SD Act), where the Commonwealth Ombudsman is required to inspect the records of Commonwealth and State and Territory law enforcement agencies to determine the extent of their compliance with the SD Act.[155] Under section 6(1) of the SD Act, the term 'law enforcement agency' includes the ACC, the AFP, the Australian Commission for Law Enforcement Integrity, police forces of each State and Territory and other specified State and Territory law enforcement agencies.

[153] See Discussion Paper footnote 27, p. 26.
[154] TIA Act s 81A.
[155] *Surveillance Devices Act 2004* (Cth) (the SD Act) ss 48, 49.

224. The SD Act contains a detailed reporting regime that includes the following features:

- anyone to whom a surveillance device is issued must provide a written report to an eligible Judge or eligible magistrate and to the Attorney-General[156]
  - stating whether or not a surveillance device was used pursuant to the warrant; and
  - specifying the type of surveillance device (if any) used; and
  - specifying the name, if known, of any person whose private conversation was recorded or listened to, or whose activity was recorded, by the use of the device; and
  - specifying the period during which the device was used; and
  - containing particulars of any premises or vehicle on or in which the device was installed or any place at which the device was used; and
  - containing particulars of the general use made or to be made of any evidence or information obtained by the use of the device; and
  - containing particulars of any previous use of a surveillance device in connection with the relevant offence in respect of which the warrant was issued.
- the Attorney-General is required to prepare, and table in Parliament, an annual report that includes the following information:[157]
  - the number of applications for warrants by, and the number of warrants issued to, law enforcement officers during that year;
  - the number of applications for emergency authorisations by, and the number of emergency authorisations given to, law enforcement officers during that year; and
  - any other information relating to the use of surveillance devices and the administration of this Act that the Attorney-General considers appropriate.
- the chief officer of a law enforcement agency is required to keep a register of warrants and emergency authorisations, that includes information such as:[158]
  - when warrants were issued;
  - the name of the Judge or Magistrate who issued the warrant;
  - the name of the law enforcement officer named in the warrant;
  - the relevant offence in relation to which the warrant is issued; and
  - the period during which the warrant is in force and any details of any variations or extensions of the warrant.

[156] SD Act s44.
[157] SD Act s45.
[158] SD Act s47.

- the Ombudsman is required to inspect the records of each law enforcement agency (other than the ACC) to determine the extent of compliance with this Act by the agency and law enforcement officers of the agency.[159]

- the Ombudsman must then make a written report to the Attorney-General at six-monthly intervals on the results of an inspection, which must then be tabled in Parliament.[160]

- the objective of the inspection is to determine the extent of compliance with the SD Act by agencies and their law enforcement officers. The Ombudsman's 2011-12 report under the SD Act explains that the following criteria were applied to assess compliance:

    - Were applications for warrants and authorisations properly made?

    - Were warrants and authorisations properly issued?

    - Were surveillance devices used lawfully?

    - Were revocations of warrants properly made?

    - Were records properly kept and used by the agency?

    - Were reports properly made by the agency?

225. The Law Council supports consideration of this model for potential application to the TIA Act warrant regime, which currently imposes inspection and reporting obligations on State bodies in respect of State agencies' interception activities under the TIA Act. However, if a reform of this nature is to be pursued it must be developed in consultation with State and Territory Ministers and should not detract from the other reporting requirements outlined in the TIA Act, such as those contained in Parts 2.7 and 2.8 and described above.

226. The Law Council also notes that if the Commonwealth Ombudsman is to be exclusively responsible for inspecting and reporting on compliance by all law enforcement agencies with the interception provisions of the TIA Act, consideration will need to be given to the other provisions of the Act that concern the relationship between State agencies and their respective oversight bodies.

227. For example, it may be necessary to retain section 36 of the TIA Act which allows States to legislate to specifically require State Minsters to receive copies of warrants, without offending against the TIA Act. The Law Council has previously noted that this section enables States with different standards of accountability or different evaluation frameworks, such as those States with a Charter of Human Rights, to ensure State Ministers have immediate access to copies of all interception warrants.

228. In the course of past inquiries into amendments concerning the reporting requirements of State and Territory agencies, the Attorney-General's Department has noted that the ability of State Governments to enact laws requiring the chief officer of a State interception agency to provide a specified Minister in that State

[159] SD Act s48.
[160] SD Act s 49.

with a copy of each warrant issued to the agency and a copy of each instrument revoking such a warrant constitutes an important safeguard under the TIA Act.[161]

229. In past submissions the Law Council has also considered a number of different mechanisms that could be utilised to enhance accountability of agencies who exercise powers under the TIA Act.[162] Some of these mechanisms have also been supported by the Australian Law Reform Commission (ALRC). For example both the ALRC and the Law Council support:

- Broadening the powers of the Commonwealth Ombudsman to ensure that he or she has the same powers to inspect records and to compel the presence of officers to answer questions relevant to the inspection of records, regardless of whether the records relate to intercepted or stored communications.

  - Currently no equivalent to section 87 of the TIA Act exists in relation to stored communication warrants. Section 87 provides, among other things, that the Ombudsman may require an officer of an agency to give information to the Ombudsman and to attend a specified place to answer questions relevant to the inspection of interception records; and where the Ombudsman does not know the officer's identity, requires the chief officer of an agency, or a person nominated by the chief officer, to answer questions relevant to the inspection.[163]

- Consideration of the establishment of a public interest monitor (PIM), similar to that established under the *Crime and Misconduct Act 2001* (Qld) and the *Police Powers and Responsibilities Act 2000* (Qld) which could bring a greater degree of scrutiny to bear on the grounds advanced for seeking a warrant and for claiming that it is a necessary and justified intrusion into the privacy of individuals.

  - The PIM could: appear at any application made by an agency for interception and access warrants under the Act; test the validity of warrant applications; gather statistical information about the use and effectiveness of warrants; monitor the retention or destruction of information obtained under a warrant; provide to the Inspector General of Intelligence and Security (IGIS), or other authority as appropriate, a report on non-compliance with the Act; and appear at any application made by an agency for interception and access warrants under the Act.[164]

  - The Law Council notes that section 45A of the TIA Act currently acknowledges the existence of the PIM in Queensland and requires the PIM to be notified of applications made for interception warrants by Queensland agencies.

[161] Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008).
[162] Law Council of Australia submission to the Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law* (20 December 2007).
[163] Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) 12 August 2008 available at http://www.alrc.gov.au/publications/report-108, Recommendation 73-6.
[164] Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice (ALRC Report 108) 12 August 2008 para73.1332- 141 . The ALRC recommended that the Australian Government initiate a review of telecommunications legislation, and that the review should consider whether the TIA Act should be amended to provide for the role of a PIM.

230. Other mechanisms to enhance accountability under the TIA Act supported by the Law Council concern ASIO's access to telecommunications data and include:

(a) the incorporation of record keeping and reporting obligations, which are consistent with those provided for in sections 32 and 34 of the ASIO Act, should attach to the issue of telecommunication data warrants and these records should be subject to review by the IGIS in the same manner that records produced in connection with tracking device warrants are subject to review by the IGIS; and

(b) the expansion of the mandate of the IGIS to incorporate oversight of the use of powers to obtain prospective telecommunications data by ASIO. As an independent body, the IGIS could play an important role in ensuring ASIO adheres to its obligations under the TIA Act and gives practical effect to safeguards aimed at protecting individual privacy.

231. The Law Council submits that the PJCIS should give consideration to these mechanisms that would enhance accountability under the TIA Act, and cautions against proposals that attempt to remove reporting requirements.

232. To this end, the Law Council supports the observation in the Discussion Paper that:

> *"Consideration should be given to introducing new reporting requirements that are less process orientated and more attuned to providing the information needed to evaluate whether intrusion in to privacy under the regime is proportionate to public outcomes."*[165]

Creating a Single Warrant with Multiple Telecommunication Interception Powers

233. Listed among the proposals the Government is considering is the creation of a single warrant with multiple telecommunication interception powers. Although the Discussion Paper outlines some of the current differences in the warrant regimes applying to the different interception powers available under the TIA Act and the administrative burdens these pose for agencies, it does not provide any further detail in respect of this particular proposal. For example, it is not clear:

- which interception powers would be included (for example, named person warrants, B-party warrants, device based warrants, service based warrants)
- whether they would cover warrants for stored communications or authorisations for disclosure of telecommunications data;
- whether they would be available to law enforcement agencies, or ASIO or the broader range of enforcement agencies; or
- whether they would be accompanied with stronger safeguards, or additional reporting or oversight requirements.

234. In the absence of these important details, the Law Council generally cautions against the adoption of this proposal for the reasons outlined above with respect to the proposal to streamline the existing warrant authorisation processes.

235. While the Law Council does not oppose the idea of improving the efficiency of authorisation and warrant processes, it is concerned that allowing multiple telecommunication interception powers to be listed in a single warrant risks diluting

[165] Discussion Paper p. 26.

the particular safeguards that currently apply to the use of each specific power. These concerns have been realised in past efforts to consolidate warrants under the TIA Act, such as when the named person warrants were introduced in 2006.

236. As the Law Council pointed out in its submission in relation to those and subsequent amendments, the privacy tests included in the named person warrant provisions are rendered meaningless if the officer applying for the warrant is no longer required to uniquely identify each particular device or service the named person is likely to use.[166]

237. These concerns would be increased if a single warrant containing multiple interception powers were introduced. Such a warrant could include, for example, multiple targets, multiple telecommunication devices and multiple telecommunication services. It could apply to suspects and third parties. Not only would it be extremely difficult for issuing authorities to adequately assess the privacy impacts of the powers under the warrant, it would also be difficult to assess the benefit of the exercise of the powers to the investigation or inquiry, or to determine the appropriate duration of the warrant.

238. It would also be difficult to set out a range of safeguards that would adequately protect against unjustified intrusion into personal privacy and ensure transparency and accountability. However, if a proposal of this nature were pursued, the Law Council would suggest that the issuing authority must be satisfied of the following minimum requirements:

- that any person whose telecommunications are to be intercepted is specifically identified as a legitimate target of suspicion from a security or law enforcement perspective;
- that each and every telecommunications service or telecommunications device to be intercepted is, in fact, used or likely to be used by the relevant person of interest; and
- each and every telecommunications service or telecommunications device to be intercepted can be uniquely identified such that relevant telecommunications made using that service or device can be isolated and intercepted with precision.

239. In addition, the issuing officer should also have regard to:

- the likely benefit to the investigation which would result from the intercepted information substantially outweighing the extent to which the interception is likely to interfere with the privacy of any person or persons;
- the gravity of the conduct constituting the offence or offences being investigated;
- how much the information referred to would be likely to assist in connection with the investigation by the agency of the offence or offences; and

[166] See for example Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into Telecommunications (Interception and Access) Bill 2006* (13 March 2006); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008).

- to what extent methods of investigating the offence or offences that do not involve intercepting communications have been used by, or are available to, the agency.

240. As noted above, the authority or officer empowered to issue warrants currently varies under the TIA Act depending on the nature of the power exercised under the warrant and the agency applying for the exercise of this power. This distinction, which has in the past been justified on the basis of the different functions and investigation environments of the particular agencies exercising the powers and their respective oversight requirements, must be kept in mind when considering reforms designed to allow multiple powers to be authorised in a single warrant. The range of agencies able to apply for such warrants also varies depending on the nature of the power, as does the relevant criminal penalty threshold that might apply. Consideration must be given as to how to address these differences.

241. The Law Council would suggest that if this reform is pursued it should be available only to criminal law enforcement agencies or senior ASIO officers and be issued by an independent authority such as a Judge. It should also be limited to the investigation of serious offences, the meaning of which should also be reviewed if this new form of warrant is considered.

242. The Law Council also suggests that the duration of any warrant authorising multiple telecommunication interceptions should be shorter than that currently available under the TIA Act. This would be in recognition of the potential for such a warrant to have very significant impacts on the privacy of any individuals concerned and the need to encourage a limited and particularly disciplined use of this power.

243. Existing reporting and oversight requirements would also need to be strengthened to respond to this new form of warrant.

Australian Intelligence Community Legislation Reform – Outline of the Reforms in Chapter 4 of the Discussion Paper

244. Chapter 4 of the Discussion Paper contains a number of proposed reforms to the legislation relating to the Australian Intelligence Community.

245. According to the Discussion Paper, the Attorney-General's Department and the Australian Intelligence Community Agencies – including ASIO, the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO) - have identified a number of practical difficulties with the legislation governing the operation of these agencies, specifically the ASIO Act and the IS Act.[167] The Discussion Paper explains that the proposed reforms in this Chapter:

> *"… seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.*
>
> *At the same time, it is important that legislation governing intelligence agencies continues to include appropriate checks and balances on the exercise of their powers. Ensuring these agencies remain accountable for their actions helps to maintains public confidence in and support for the critical work of intelligence agencies. The proposed reforms seek to maintain a strong and accountable legislative regime under which intelligence agencies can respond effectively when threats to our community emerge."*[168]

246. Many of the reforms proposed in this Chapter focus on the warrant processes governing the use of ASIO's powers, and in particular ASIO's special powers in Division 2 of Part III of the ASIO Act.

247. The Discussion Paper explains that the Government wishes to progress the following proposals:

    (a) Amending the ASIO Act to modernise and streamline ASIO's warrant provisions:

        (i) to update the definition of 'computer' in section 25A; and

        (ii) to enable warrants to be varied by the Attorney-General, simplifying the renewal of the warrants process and extending the duration of search warrants from 90 days to 6 months.

248. The Government is also considering amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

    (a) establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target;

[167] Discussion Paper p. 40
[168] Discussion Paper p. 40

(b) align surveillance device provisions with the *Surveillance Devices Act 2007* (Cth);

(c) enable the disruption of a target computer for the purposes of a computer access warrant; and

(d) establish classes of persons able to execute warrants.

249. The Government is also considering amending the ASIO Act to create an authorised intelligence operations scheme which would provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

250. The Government is also 'expressly seeking' the views of the PJCIS on whether the ASIO Act should be amended to:

(a) enable ASIO to use third party computers and communications in transit to access a target computer under a computer access warrant;

(b) clarify that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant; and

(c) clarify that reasonable force may be used at any time during the execution of a warrant, not just on entry.

General Comments relating to the reforms

251. In line with its past advocacy on the expansion of ASIO's powers,[169] the Law Council intends to respond to many of these proposed reforms by addressing concerns such as:

(a) the absence of information provided in the Discussion Paper to justify why these proposed reforms are necessary, particularly in light of the already extensive powers available to ASIO under the TIA Act and ASIO Act;

(b) the propensity for the Discussion Paper to focus on removing administrative burdens or addressing operational challenges, and the absence of discussion of the history and context of the existing powers, many of which have already been amended many times in response to similar claims; and

(c) the lack of detail regarding the types of safeguards or reporting or oversight requirements that would accompany the proposed changes to ASIO's powers.

252. The Law Council will also provide some general comments on the need to distinguish ASIO's role from that of law enforcement agencies, and on the impact of the proposed reforms on the right to privacy. These general comments apply to all of the reforms proposed in this Chapter of the Discussion Paper.

[169] A description of the Law Council's advocacy in this area, along with copies of relevant submissions and correspondence is available at http://www.lawcouncil.asn.au/programs/criminal-law-human-rights/anti-terror/asio.cfm

Distinguishing ASIO's Roles and Functions from those of Law Enforcement Agencies

253. ASIO's main role is to gather information and produce intelligence that will enable it to warn the Commonwealth Government about activities or situations that might endanger Australia's national security.[170] ASIO's functions are prescribed in subsection 17(1) of the ASIO Act as:

    (a) to obtain, correlate and evaluate intelligence relevant to security;

    (b) for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;

    (c) to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities;

    (d) to furnish security assessments to a State;

    (e) to advise Ministers, authorities of the Commonwealth and such other persons as the Minister, by notice in writing given to the Director-General, determines on matters relating to protective security; and

    (f) to obtain within Australia foreign intelligence pursuant to section 27A or 27B of the ASIO Act or section 11A, 11B or 11C of the TIA Act, and to communicate any such intelligence in accordance with the ASIO Act or the TIA Act ; and

    (g) to cooperate with and assist bodies referred to in section 19A in accordance with that section.

254. Subsection 17(2) of the ASIO Act explains that it is not a function of ASIO to carry out or enforce measures for security within an authority of the Commonwealth. Section 20 of the ASIO Act also provides that the Director-General shall take all reasonable steps to ensure that the work of ASIO is limited to what is necessary for the purposes of the discharge of its functions.

255. These functions can be contrasted with Commonwealth law enforcement agencies, such as the AFP, whose role is to enforce Commonwealth criminal law and to protect Commonwealth and national interests from crime in Australia and overseas. The AFP's functions are set out in section 8 of the *Australian Federal Police Act 1979* (Cth) and include:

    (a) the provision of police services in relation to the laws of the Commonwealth and the ACT and for the investigation of State offences that have a federal aspect;

    (b) to perform the functions conferred by the *Witness Protection Act 1994* (Cth);

    (c) to perform functions under the *Proceeds of Crime Act 2002* (Cth) ; and

    (d) the provision of police services and police support services for the purposes of assisting, or cooperating with: an Australian or foreign law enforcement agency; or intelligence or security agency; or government regulatory agency.

[170] See ASIO website at http://www.asio.gov.au/

256. Many of the reforms proposed in Chapter 4 suggest a convergence of the roles and functions of ASIO with those of law enforcement agencies such as the AFP. For example, the Discussion Paper contains a proposal to introduce an authorised intelligence operations regime for ASIO officers (similar to a controlled operations regime for police) and to expand ASIO's powers in respect of personal and property searches (currently conducted by police). Many of the other reforms also point to processes that apply to law enforcement officers in relation to the exercise of powers or applications for and enforcement of warrants.

257. This approach blurs the line between ASIO's intelligence gathering role and the law enforcement role of other agencies and fails to have adequate regard to the particular oversight and accountability regimes that apply to these different agencies. The Law Council is concerned that, if adopted, many of the proposed reforms would compromise the critical distinction between ASIO and its law enforcement colleagues, and run the risk that ASIO's powers are not subject to the type of independent scrutiny and oversight that similar powers attract when exercised by law enforcement agencies. For example, because ASIO's statutory functions currently do not extend to gathering evidence in support of criminal prosecutions, it does not have the same obligations as those imposed on law enforcement agencies to inform prospective interviewees, particularly those under suspicion, about their rights to silence and to legal representation.

258. As Professor George Williams has previously commented in the context of the *ASIO Legislation Amendment (Terrorism) Bill 2002* which introduced questioning and detention warrants into Part 3 of the ASIO Act:

> *"ASIO is a covert intelligence-gathering agency. It is not a law enforcement body. If ASIO is to be granted coercive police powers, the Bill must subject the organisation to the same political and community scrutiny and controls that apply to any other police force. However, this is not compatible with the current intelligence gathering work of ASIO and its organisational structure (such as the secrecy applying to the identity of its employees). It would be difficult, if not impossible, for ASIO both to be sufficiently secretive to adequately fulfil its primary mission, as well as to be sufficiently open to scrutiny to exercise the powers set out in the ASIO Bill."*[171]

259. These comments are apposite to the proposed reforms in Chapter 4 of the Discussion Paper, which although not relating to coercive powers, may include intrusive and extensive personal and property search powers and protections for participating in authorised intelligence operations.

260. The proposed reforms would also add to the recently expanded functions of ASIO to collect and communicate evidence about Australians overseas. These functions were introduced by the *Telecommunications (Interception and Access) Amendment Bill 2008 (Cth)*. When this Bill was introduced, the Castan Centre for Human Rights made the following observations that are also relevant to the reforms proposed in the Discussion Paper, particularly those relating to the use of ASIO's covert search and access powers. The Centre explained that as a result of the 2008 reforms it would be:

> *"… in practice, difficult if not impossible for individuals to be aware of the information that ASIO may be collecting and communicating in respect of*

[171] Professor George Williams "One year on: Australia's legal response to September 11" [2002] AltLawJl 79; (2002) 27(5) Alternative Law Journal 212 available at http://www.austlii.edu.au/au/journals/AltLawJl/2002/79.html

them. To the extent that these amendments would have the tendency to increase the secrecy of government information, and to increase the reliance by Australian government agencies upon clandestine means of gathering information about Australians, they undermine the relationship between citizen and government that is at the heart of the Australian system of government, namely, that the government is ultimately the servant and not the master of the citizen, and is therefore answerable and accountable, through open administration, the operation of Parliament, and (ultimately) the votes of an informed electorate."[172]

261. The relationship between ASIO and the AFP and other law enforcement agencies has been subjected to past inquiry and review, such as the 2007 review undertaken by the Honourable Sir Laurence Street AC KMCG QC on the interoperatability between the AFP and its national security partners (the Street Review).[173] Although many of these reviews have encouraged ASIO and the AFP to strengthen formal and informal communications and means of cooperation, they have also maintained the need for the roles and functions of these agencies to remain distinct.[174]

262. This distinction must survive, even in the face of a changing investigation environment and in the context of rapid advances in technology. As the Law Council has previously observed,[175] while it is accepted that in recent years the concept of national security has come to encompass a much broader range of threats, including those posed by serious and organised crime, cybercrime, money laundering, resource shortages and environmental disasters, it does not necessarily follow from this that ASIO's role should be expanded exponentially to cover all these matters. Rather, the implication of this expanded understanding of the factors which may impact on Australia's national interest is that the work of other agencies may become to be regarded as relevant to national security, where previously it was not.

263. The Law Council submits that the PJCIS should be mindful of the critical distinction between the role of ASIO and that of law enforcement agencies, and the different oversight and accountability regimes applying to these different agencies, when evaluating the reforms proposed in the Discussion Paper.

General Concerns about Privacy

264. Earlier in this submission the Law Council drew attention to the potential for the proposed reforms in Chapter 2 of the Discussion Paper to have an intrusive impact on the right to privacy. In past advocacy the Law Council has also raised concerns about whether the legislative tests applied by the Attorney-General when determining whether to authorise ASIO to use telecommunication interception or access powers are sufficiently precise to adequately balance privacy rights against the need to safeguard national security.

---

[172] Castan Centre for Human Rights , submission to the Senate Committee on Legal and Constitutional Affairs Inquiry into the *Telecommunications (Interception and Access) Amendment Bill 2008 (Cth)* available at http://www.law.monash.edu.au/castancentre/publications/castan-tele-interception-intelligence-services.pdf

[173] Honourable Sir Laurence Street AC KMCG QC on the interoperatability between the AFP and its national security partners (the Street Review) (11 December 2007) available at http://www.afp.gov.au/media-centre/~/media/afp/pdf/t/the-street-review.ashx

[174] See for example, Street Review para 1.8

[175] Law Council of Australia submission to Senate Legal and Constitutional Affairs Committee Inquiry into the *Intelligence Services Legislation Amendment Bill 2011* (14 June 2011) available at http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=417BEA58-C1A1-0204-7DE3-200690C9D53D&siteName=lca

265. These concerns also arise in the context of the reforms proposed in Chapter 4, particularly those that relate to the warrants issued to ASIO under Division 2 Part III of the ASIO Act.

266. In addition to these concerns, the Law Council submits that ASIO's powers should not be exponentially expanded without due regard to their potential to interfere with individual human rights. This concern is particularly acute given that the ASIO Act has been amended more than 20 times since 2002, with significant amendments resulting in an expansion of ASIO's powers being made in many cases.[176] As stated by a former Inspector General of Intelligence and Security (IGIS) in a written submission to the Senate Committee on Legal and Constitutional Affairs:

> *"While it is clearly imperative for the Organisation to move with the times and improve its efficiency and effectiveness if ASIO is to meet the needs of government, it is important that these goals should not be achieved at the cost of an unreasonable diminution of the freedoms which all Australians have come to expect and enjoy."*[177]

267. The Law Council respectfully agrees with this view and considers the right to privacy to be one of the core rights that must be considered when evaluating any proposals designed to improve ASIO's effectiveness or efficiency. As outlined in detail below, it is not enough for the Government to cite operational needs as justifying a particular reform, unless it can also be shown that such a reform is necessary for one of ASIO's statutory functions and is a proportionate means of achieving that function.

268. It is also noted that, unlike certain provisions in the TIA Act, the warrant provisions in Division 2 Part III of the ASIO Act do not contain any specific requirements for the officer issuing the warrants to have regard to privacy considerations. The Law Council notes that the Attorney-General has issued guidelines under section 8A of the ASIO Act in relation to the performance by ASIO of its functions.[178] One of these guidelines provides that when obtaining information concerning the nature of any activities of a person or group for the purpose of an inquiry or investigation, ASIO should use 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.

269. The Law Council submits that the PJCIS should have regard to privacy considerations when evaluating the proposed reforms. It also suggests that the PJCIS consider recommending that a consistent privacy test, based on that described earlier in this submission in relation to warrants obtained under the TIA Act, be introduced into the ASIO Act. If this approach is not adopted, the Law Council submits that the PJCIS should recommend strengthening the privacy

---

[176] For example see *Australian Security Intelligence Organisations Legislation Amendment (Terrorism)* Act 2003; *Anti-terrorism Act (No. 3) 2004*; *Intelligence Services Legislation Amendment Act 2005; Anti-Terrorism Act (No. 2) 2005*; *Telecommunications (Interception) Amendment Act 2006*; *ASIO Legislation Amendment Act 2006; Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011; Intelligence Services Legislation Amendment Act 2011.*

[177] Submission by the Inspector-General of Intelligence and Security (IGIS), Mr Bill Blick PSM, to the Senate Committee on Legal and Constitutional Affairs inquiry into the *Australian Security Intelligence Organisation Legislation Bill 1999*, (April 1999).

[178] See Guideline 10 of the Guidelines issued by the Attorney General available at http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf

protections in the ASIO Guidelines and in any other instruments governing the conduct of investigations or information sharing by ASIO.[179]

Modernising and streamlining ASIO's warrant provisions

270. This submission will comment on proposed reforms relating to modernising and streamlining ASIO's warrant provisions including:

(a) amendments to the current provisions relating to computer access warrants, such as broadening the definition of 'computer', authorising the use of third party computers and communications in transit and broadening the range of authorised acts necessary to execute a computer access warrant;

(b) amendments that would facilitate variation and renewal of warrants;

(c) amendments to the duration of search warrants that would extend the current 90 days duration to six months;

(d) the introduction of named person warrants;

(e) the broadening of existing powers relating to personal searches; and

(f) the introduction of authorisation lists for officers authorised to execute warrants.

The Existing Warrant Powers and Processes under Division 2 Part III of the ASIO Act

271. The proposed reform proposals outlined in Chapter 4 of the Discussion Paper appear to be directed at the warrant processes and the exercise of ASIO 'special powers' contained in Division 2 Part III of the ASIO Act. This Division provides ASIO with the power to:

(a) request information or documents from operators of aircraft or vessels;

(b) enter and search premises and remove and record items found;

(c) conduct an ordinary or frisk search of a person at or near the premises subject to a search warrant;

(d) enter premises and use computers and other electronic equipment, and take action to conceal this entry and access;

(e) install and remove a listening device and listen to or record words, images, sounds or signals;

(f) use a tracking device for the purpose of tracking a person or an object;

(g) inspect postal articles or delivery service articles; and

(h) obtain foreign intelligence.

[179] For further discussion of potential reforms to the Guidelines see Law Council of Australia, Letter to Attorney General re Requirement for ASIO to Disclose Information Prior To Questioning (23 April 2010). This letter and the response received are available at http://www.lawcouncil.asn.au/programs/criminal-law-human-rights/anti-terror/asio.cfm

272. Warrants under this Division are issued by the Minister at the request or direction of the Director-General. Generally, the Director-General, or a senior officer of ASIO appointed by the Director-General in writing, are the officers authorised to approve ASIO officers and employees to exercise powers under these warrants.[180]

273. The precise matters in respect of which the Minister must be satisfied vary depending on the power to be exercised under the warrant, but generally require the Minister to be satisfied that there are reasonable grounds for believing that the exercise of the power will substantially assist the collection of intelligence in respect of a matter that is important to security. The warrants are also required to specify the particular activities or things that are authorised in the particular circumstances. For example, in respect of search warrants, the Minister is required to specify the particular premises and whether it is appropriate to remove any items or use force to enter the premises or search a person on the premises.

274. More stringent requirements apply to the issue of warrants authorising the use of listening devices and tracking devices, for example, in respect of listening devices the Minister must be satisfied that the person, whose words, images, sounds or signals are being listened to, is engaged in, or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security.[181] The provisions relating to the use of listening and tracking devices generally prohibit their use unless authorised.[182]

275. The majority of warrants in this Division are subject to a maximum duration of six months, however search warrants may only be granted for a maximum of 90 days. Further details about the particular warrant processes in this Division are discussed below.

276. The Law Council notes that this Division is distinct from ASIO's 'special powers relating to terrorism offences' contained in Division 3 of Part III that include powers to question and detain persons suspected of involvement in terrorist activity.

Law Council's concerns regarding proposals relating to warrants

Computer warrants

277. The procedure for obtaining a computer access warrant is outlined in section 25A of the ASIO Act. It provides that the Minister can issue a computer access warrant:

> *"… if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a particular computer (the target computer) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the security matter) that is important in relation to security."*[183]

278. Subsection 25A(3) provides that the target computer must be specified in the warrant, along with any restrictions or conditions on the activities authorised in the warrant.

279. "Computer" is currently defined in section 22 of the ASIO Act as a "computer, a computer system or part of a computer system". The Discussion Paper explains that this means that if a person has more than one computer which is not part of the

[180] ASIO Act s24
[181] ASIO Act s26
[182] ASIO Act ss26, 26A
[183] ASIO Act s25A(2)

same system or has data stored on a computer network, more than one warrant may be necessary. This can be discovered only upon entering premises, and then it is necessary to obtain a second warrant and enter the premises a second time.

280. The Discussion Paper states that this is "inefficient" and that it "does not increase the level of accountability around the issue of warrants".[184] The Discussion Paper proposes, as a possible solution, amending the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on particular premises, computers connected to a particular person or a computer network.

281. The Law Council appreciates that the current definition of "computer" in the ASIO Act may not be broad enough to encompass the increasingly complex array of computer devices that an individual may use or possess, and that this may pose certain administrative challenges for ASIO officers executing computer access warrants.

282. However, the Law Council also notes that the test for granting a computer access warrant is critically dependent on the ability of the Minister to identify a *particular* computer and be satisfied that access by ASIO to data held on that particular computer will substantially assist the collection of intelligence in respect of a matter that is important to security. If the particular computer is not sufficiently identified in the application for the warrant, it is difficult to see how this test can be satisfied. The need to identify the particular computer the subject of the warrant is also critical to authorising the activities that can be undertaken when executing the warrant, pursuant to subsection 25A(3).

283. These requirements constitute important safeguards and limits on the exercise of ASIO's powers under computer access warrants. They acknowledge the intrusive nature of this power, and the potential for the privacy rights of non-suspect individuals to be compromised, by requiring the Minister to turn his or her mind to the benefit to be gained by access to each particular computer identified in the warrant application.

284. It is not clear how this level of oversight could be maintained if the solution proposed in the Discussion Paper is accepted and a computer access warrant could be issued in relation to a computer, computers on particular premises, computers connected to a particular person or a computer network.

285. It would significantly dilute the existing safeguards in section 25A if, for example, there was no longer any requirement for ASIO to identify each particular computer that they sought to access, but merely to identify particular premises on which computers may be found. It would also be difficult for the Minister to be satisfied that access by ASIO to data held on any computer found on the premises would substantially assist the collection of intelligence in respect of a matter that is important to security, particularly if the premises in question were inhabited or visited by a range of different individuals who may also possess or use computers on those premises. Similar issues would arise in respect of computers that may be connected to a particular person but are used, possessed or owned by other individuals.

286. For these reasons, the Law Council cautions against adopting this proposal.

287. The Law Council notes that other provisions in Division 2 Part III also authorise certain activities relating to a 'computer', for example section 25 which provides for

[184] Discussion Paper, p 41

the authorisation of search warrants, allows the Minister to authorise an officer to use a computer to obtain access to data when conducting a search of certain premises. These provisions could also be affected by a change to the meaning of "computer".

Use of third party computers and communications in transit

288. The Discussion Paper also explains that advancements in technology have made it increasingly difficult for ASIO to execute its computer access warrants.[185] It explains, for example, that where a target is security conscious, innovative methods of achieving access to the target computer have to be employed.[186]

289. To overcome this problem, the Discussion Paper suggests that it may be appropriate to amend the ASIO Act to enable a third party computer or communication in transit to be used to lawfully access a target computer.[187] The Discussion Paper notes that using a communication in transit or a third party computer may have privacy implications and, as a result, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.[188]

290. The Law Council does not hold the appropriate expertise to evaluate the claims outlined in the Discussion Paper that it may be necessary to use a communication that is in transit or use a third party computer for the purpose of executing a computer access warrant. However, the Law Council suggests that before amendments are made in line with those suggested in the Discussion Paper, evidence would need to be provided to justify this claim.

291. The Law Council is pleased that the Discussion Paper recognises the privacy implications arising from the proposed amendments, which could potentially include the covert use of, or access to, computers or communications of innocent third parties. The Law Council suggests that consideration be given to enacting a separate authorisation process for the use of such a power that could include the requirement for the Minister to be satisfied that:

    (a) each communication or third party computer to be accessed is specifically identified;

    (b) the target computer is specifically identified;

    (c) access by ASIO to data held on the target computer will substantially assist the collection of intelligence in respect of a matter that is important to security;

    (d) access to the particular communication in transit or third party computer is reasonably necessary to access the target computer in the circumstances; and

    (e) the likely benefit to the investigation which would result from the access to the communication or third party computer substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons.

[185] Discussion Paper p. 50
[186] Discussion Paper p. 50
[187] Discussion Paper p. 50
[188] Discussion Paper p. 50

292. The Law Council also suggests that such a warrant should have a more limited duration than other computer access warrants so that its necessity and effectiveness can be reconsidered in the light of new or emerging technologies.

Authority for acts necessary to execute a computer access warrant

293. As noted above, section 25A allows the Minister to issue a warrant authorising a relevant ASIO officer to gain remote access to data held in a computer, where such access will substantially assist the collection of intelligence in respect of a matter that is important to security. Section 25A also allows the Minister to authorise the relevant officer to add, delete or alter data for the purpose of gaining access to data in a target computer and to do things that are reasonably necessary to conceal that anything has been done under the warrant. When this provision was introduced, the Explanatory Memorandum stated that this would include modifying access control and encryption systems.[189]

294. Subsection 25A(5) provides a limit on this power by prohibiting ASIO from obstructing the lawful use of a computer or doing anything that causes loss or damage to a person lawfully using the computer or other electronic equipment.

295. The Discussion Paper suggests that this provision could be amended so that the prohibition "does not apply to activity proportionate to what is necessary to execute the warrant." [190] It explains that this is necessary due to the:

> *"…increasingly complex nature of the global information technology environment and the use by some targets of sophisticated computer protection mechanisms [which] can adversely impact ASIO's ability to execute a computer access warrant for the purpose of obtaining access to data relevant to security."*[191]

296. When section 25A was first introduced, concerns were raised that allowing ASIO to add, delete or alter data would undermine public trust and confidence in the integrity of electronic transactions and could create:

- a risk to business (small changes can have extreme, unforeseen and costly effects);
- a risk of accidental damage to software or data (what redress is available to the owner of the computer if the intrusion was covert and the perpetrator is therefore unknown); and
- a risk of evidence being planted. [192]

297. In response to these concerns, in his second reading speech to the Bill introducing section 25A, the then Attorney-General referred to the power to add, delete or alter data if this is necessary in order to execute a computer access warrant. He stressed, however, that this will be subject to subsection 25A(5) containing the:

---

[189] Explanatory Memorandum to the *Australian Security Intelligence Organisation Legislation Amendment Bill 1999*
[190] Discussion Paper p. 48
[191] Discussion Paper p. 48
[192] For example see Electronic Frontiers Australia, *Submission No. 10*, p. 2, as quoted in Parliamentary Joint Committee on ASIO, An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999 (May 1999) p. 18

"… limitation that a warrant does not permit ASIO to do anything that interferes with the lawful use of a computer or causes loss or damage to other persons lawfully using the computer."[193]

298. The extent to which ASIO can 'interfere' with a target computer was explained further by the Director-General in his evidence to the then Parliamentary Joint Committee on ASIO:

"Under the proposed amendments, we would be allowed to interfere with a computer in so far as it enables us to compromise the protection mechanism that may surround the information in the computer. However, we would not be allowed to interfere with the information in the computer itself or indeed the use of the computer."[194]

299. In its written submission to the then Parliamentary Joint Committee on ASIO, the Attorney-General's Department emphasised that 'in gaining entry to a target computer ASIO is not permitted to cause damage to either computer or data.' It went on to make the point that it would, in fact, be:

"… in ASIO's interests to go to extreme lengths to ensure that it did not cause damage that might compromise its operations."[195]

300. Having regard to this legislative history, the Law Council questions the basis of this proposed reform in relation to sub-section 25A(5). This key provision was considered important to the community and the Parliament when it was introduced and the Discussion Paper does not justify its removal other than through the general statement about the global information technology environment and sophisticated computer protection mechanisms adversely impacting on ASIO's ability to execute computer access warrants.

Variation and renewal of warrants

301. The Discussion Paper explains that currently the ASIO Act does not specifically provide for a warrant to be varied if the circumstances justify such a variation. A new warrant is required in every instance where there is a significant change in circumstances. It proposes that a variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability, but does not outline the content of this provision in any detail.[196]

302. The Discussion Paper also explains that certain threats to security can endure for many years, requiring a significant proportion of warrants issued under the ASIO Act to continue beyond the initial authorisation period. However, the current provisions in the ASIO Act do not enable a warrant to be extended.[197] In such circumstances, an authorised ASIO officer must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant change to either.

---

[193] Hon Daryl Williams AM QC MP (Attorney-General), *House of Representatives Hansard*, 25 March 1999 p. 4364

[194] Dennis Richardson (Australian Security Intelligence Organization), *Transcript of Evidence*, 27 April 1999, p. 13 as quoted in Parliamentary Joint Committee on ASIO, An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999 (May 1999) p. 20.

[195] Attorney-General's Department, *Submission No. 9*, p. 3, as quoted in Parliamentary Joint Committee on ASIO An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999 (May 1999) p. 20

[196] Discussion Paper p. 41

[197] Discussion Paper p. 42

303. The Discussion Paper suggests that a renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources, but does not expand upon this claim in any detail.[198]

304. In the absence of this information, is difficult for the Law Council to respond in detail to this proposal. For example, it is not clear whether the proposed variation and renewal provisions would apply to each warrant obtained under Division 2 Part III and, if so, whether these provisions would be tailored to each particular warrant or expressed in general terms. For example, would there be different requirements for seeking a variation of a search warrant under section 25 compared with a variation of warrant to use a listening device under section 26? Would there be different limits on the period in respect of which an existing warrant could be renewed, depending on the nature of the power to be exercised?

305. If general provisions allowing for variations and renewals of warrants are to be introduced, the Law Council submits that variations and renewals should be subject to a rigorous approval process that demands careful, thorough consideration by the officer making the application, as well as by the Minister issuing the warrant.

306. The Law Council's views are influenced by the intrusive nature and potentially broad scope of the powers that ASIO officers can exercise under warrants issued under Division 2 Part III, which include searching a home, accessing a computer, covertly listening to a person's conversations and tracking a person's movements. These powers can be exercised in respect of a person who has not been convicted of or even suspected of a criminal offence, and can be exercised without the knowledge of the person, or anyone else who may be residing with or communicating with that person. In light of these characteristics, the Law Council is of the view that these special powers must be subject to strict authorisation processes, even when an existing authorisation is sought to be varied or renewed. Such powers should be able to be exercised only when shown to be necessary for one of ASIO's statutory functions, and in a manner that has the least impact on individual rights.

307. While the Law Council continues to hold concerns about the adequacy of the current warrant process in Division 2 Part III, the fact that it does not provide for variations or renewals to be made, provides an important incentive for ASIO officers to pursue other less intrusive alternatives to achieve their functions if available, and encourages a disciplined use of their special powers.

308. For these reasons, the Law Council considers it to be appropriate that authorised ASIO officers seek a new warrant in every instance in which there is a significant change in circumstances - which could include a change in the premises subject to a search warrant, the identity of a person subject to a listening device or tracking device, or the range of activities needed to be authorised to execute a warrant. Similarly, the Law Council considers it to be appropriate that ASIO seek a new warrant if an existing warrant has expired, even if the intelligence case remains unchanged. In both cases, there is a strong public interest in requiring ASIO to satisfy a rigorous authorisation procedure.

Duration of search warrants:

309. Section 25 of the ASIO Act authorises the Minister to issue a search warrant, on the request of the Director-General, if he or she is satisfied that there are reasonable grounds for believing that access by ASIO to records or other things on particular

[198] Discussion Paper p. 42

premises will substantially assist the collection of intelligence in respect of a matter that is important to security.[199]

310. The powers that can be authorised by ASIO under such a search warrant are extensive and can include:[200]

- entering premises;
- searching the premises;
- inspecting or examining any records or other things found;
- removing or making copies or transcripts of any record or other thing found;
- doing anything reasonably necessary to conceal the fact that anything has been done under the warrant; and
- doing any other thing reasonably incidental to any of the above.

311. Search warrants can also authorise ASIO officers to conduct personal searches of a person at or near the subject premises when the warrant is executed.[201] As noted above, such warrants can also authorise ASIO officers to use or access a computer, equipment or device to obtain information or data.[202]

312. A search warrant issued under section 25 must specify the period during which it is to be in force. The period must not be more than 90 days, although the Minister may revoke the warrant before the period has expired. Subsection 25(11) also provides that the issue of further warrants is not prevented. It is also noted that pursuant to section 30, the Director-General can revoke a search warrant before the 90 days have expired.

313. The Discussion Paper states that the 90 days duration of search warrants is shorter than the duration of other warrants contained in Division 2 Part III of the ASIO Act, which currently last for a maximum of six months. It proposes that the maximum duration of a search warrant could be increased from 90 days to six months, making it consistent with the other warrant powers in the ASIO Act. [203] The Discussion Paper explains that:

> *"… [a] warrant enabling a search to take place within a six month period would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors. Indeed, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control, and a new warrant would be required."*[204]

314. The Law Council cautions against the adoption of this proposal. Insufficient information has been provided in the Discussion Paper to justify doubling the current maximum duration of a search warrant.

[199] ASIO Act s25(2)
[200] ASIO Act s24(3)
[201] ASIO Act s25(4A)
[202] ASIO Act s25(5)
[203] Discussion Paper p. 42
[204] Discussion Paper p. 42

315. Such a proposal must also be considered in light of the broad and intrusive powers that can be authorised under a search warrant, and can be exercised covertly. The nature of these powers highlights the need to ensure strict limits are placed on the duration of any warrant authorising their use. Those limits should be relaxed only if it can be shown to be absolutely necessary for the performance of ASIO's statutory functions. The Law Council suggests that the Discussion Paper has not provided adequate information to demonstrate this need.

316. The Law Council also notes that subsection 25(8) already acknowledges the potential operational challenges associated with investigations and inquiries undertaken by ASIO by allowing for delayed commencement of search warrants for a period of up to 28 days from the time the warrant is issued. This effectively provides a maximum period of close to four months from the time the warrant is issued to the time it must be executed. In addition, section 29 of the ASIO Act permits certain warrants (including a search warrant) to be issued by the Director-General without requiring the consent of the Minister in the case of an emergency. The Discussion Paper does not explain why these provisions are insufficient to meet the current operational challenges faced by ASIO.

317. In addition, the Law Council notes that section 25 has previously been amended to extend the maximum duration period of search warrants following very similar claims of the need for greater operational flexibility for ASIO.

318. For example, in 1999 the provision was amended to extend the duration of search warrants from seven to 28 days.[205] In 2005 the provision was further amended by the *Anti-Terrorism (No 2) Act 2005* to allow a maximum duration of 90 days. The 2005 amendments were rushed through Parliament alongside many other very significant reforms that expanded the powers of law enforcement and intelligence agencies with very little opportunity for public debate or scrutiny. The Explanatory Memorandum to the *Anti-Terrorism (No 2) Bill 2005* stated that the amendments to the maximum duration of search warrants in section 25 of the ASIO Act would "reduce the need for fresh warrants to be sought in unavoidable situations where it has not been practicable or possible to execute the warrant within 28 days".[206]

319. The Law Council submits that it is not sufficient for the Government to continue to cite broad "operational needs" as a basis for extending the maximum duration of search warrants. Further specific and compelling evidence must be provided that explains why the current 90 day maximum (which is more than ten times the maximum prescribed prior to 1999) is inadequate.

Named person warrants

320. The Discussion Paper includes a proposal that would allow ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.[207] It explains that:

> *"In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the*

[205] *Australian Security Intelligence Organisation Legislation Amendment* Act 1999
[206] Explanatory Memorandum , *Anti-Terrorism (No 2) Bill 2005* (Cth) available at http://www.austlii.edu.au/au/legis/cth/bill_em/ab22005224/memo_0.html
[207] Discussion Paper p. 47

different legislative requirements of the various warrant types, which is administratively burdensome.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied."[208]

321. While there is insufficient detail provided in the Discussion Paper to enable the Law Council to respond to this proposal in detail, the Law Council is concerned that such a proposal would remove or dilute the existing tests and requirements relating to the authorisation and use of special powers.

322. A range of factors point to the need for caution in this area. For example, currently the warrant provisions contain different tests in terms of the matters of which the Minister must be satisfied before a warrant can be issued. For example, section 25 which allows for search warrants to be issued, requires that the Minister is satisfied that:

*"… there are **reasonable grounds** for believing that access by the Organisation to records or other things on particular premises **will substantially assist** the collection of intelligence in accordance with this Act in respect of a matter that is important in relation to security (emphasis added)".*

323. Section 26B relating to tracking devices in respect of persons, provides that the Minister must be satisfied that:

*"... the use by the Organisation of a tracking device applied to any object (a target object) used or worn, or likely to be used or worn, by the subject to enable the Organisation to track the subject **will, or is likely to, assist** the Organisation in carrying out its function of obtaining intelligence relevant to security (emphasis added)".*

324. The differences in these tests would need to be carefully considered under any proposal designed to allow ASIO to apply for a single warrant covering all ASIO Act warrant powers.

325. In addition, it is important to recognise that there are a range of special powers authorised under the various warrants in Division 2 Part III of the ASIO Act from powers to inspect postal articles under section 27 of the ASIO Act to powers to install tracking and listening devices. The current warrant processes require the Minister to consider each power separately, which allows the Minister to have regard to the particular nature of the power to be exercised, and the benefit this is likely to have to the collection of intelligence relevant to national security. This type of assessment would be made significantly more difficult if a single warrant covering multiple powers were introduced.

326. In addition, the types of activities the Minister can authorise under a warrant vary depending on the particular power – for example, the use of force can be authorised under a search warrant but is not available under other warrants. Consideration would need to be given as to whether and how the range of activities that can be authorised under the different warrant provisions would be incorporated under a single warrant regime.

[208] Discussion Paper p 47

327. It should also be noted that provisions relating to listening and tracking devices contain specific prohibitions on the use of these devices except for the purposes prescribed in the Act, and have different requirements in terms of the persons authorised to execute these warrants or retrieve listening and tracking devices. The Law Council would be concerned if these more stringent requirements were removed or diluted under a single warrant regime.

328. The impact a single warrant regime would have on the respective record keeping, reporting and oversight requirements under the ASIO Act would also need to be carefully considered.

329. Where named person warrants have been introduced in other regimes, such as under the TIA Act, the Law Council has raised concerns about the dilution of safeguards and the reduction in the level of accountability for the use of such powers. The Law Council has also noted that these types of warrants, which authorise the use of multiple powers, also leave open the possibility for misuse or overuse of these powers by law enforcement or intelligence agencies.

330. For example, the Law Council has submitted that named person warrants place the focus of the applicant agency on the person of interest, and remove the requirement for the agency and the issuing officer to consider whether a sufficient case has been made out that would justify the use of each particular power.[209] Named person warrants also remove the incentive for agencies to consider alternatives to the use of intrusive powers and the incentive for agencies to use their special powers selectively. By contrast, the existing provisions require ASIO to establish an intelligence case for the use of each particular power and encourage ASIO to adopt the least intrusive techniques of information collection.

331. If a named person warrant reform were to be pursued, the Law Council submits that the existing safeguards and accountability provisions in the ASIO Act would need to be strengthened. In particular, the Law Council submits that consideration be given to reinforcing the privacy protections currently contained in Guideline 10 of the ASIO Guidelines by expressly incorporating a consistent privacy impact test into the relevant legislative provisions of the ASIO Act. As noted above, Guideline 10 requires ASIO officers to use "… as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions" when carrying out an investigation or inquiry consistent with its statutory functions. [210] This obligation should be reinforced by requiring the officer or authority issuing the warrant to be satisfied on reasonable grounds that the likely benefit to the investigation or inquiry which would result from the use of each of the warrant powers substantially outweighs the extent to which exercise of these powers is likely to interfere with the privacy of any person or persons.

332. The Law Council notes that the Discussion Paper does not mention which of ASIO's warrant powers could be included in the proposed named person warrant. The Law Council has assumed the Discussion Paper is referring to Division 2 Part III warrants, given that this has been the focus of other proposals. If the proposal were intended to also include Division 3 Part III warrants, which contain special powers relating to terrorism offences including questioning and detention powers, the Law

[209] See for example, Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into Telecommunications (Interception and Access) Bill 2006* (13 March 2006)
[210] See Guideline 10 of the current Guidelines issued by the Attorney General at http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf

Council's concerns would be increased in light of the significant human rights concerns associated with the use of these powers.[211]

Personal searches

333. As noted above, under section 25 of the ASIO Act, a warrant can be obtained to search premises. Contained within this provision the is power to search:

> *"… a person who is at or near the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to the security matter."*[212]

334. The Discussion Paper explains that this means that:

> *"… where ASIO assess that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched. However, it is not always feasible to execute a search warrant on a person of interest while they are 'at or near' the premises specified in the warrant.*
>
> *For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible."* [213]

335. The Discussion Paper suggests that this limitation could be addressed by:

> *"… enabling ASIO to request a warrant to search a specified person rather than premises (subject to existing safeguards in subsections 25(4B) and 25AA) so that there would be sufficient operational flexibility while maintaining appropriate accountability via the warrant process."*[214]

336. The Law Council cautions against the implementation of this proposed reform. Providing ASIO with a general power to conduct a personal search would constitute a significant expansion of ASIO's special powers and continue to blur the distinction between ASIO's intelligence and security functions and the role and function of law enforcement agencies.

337. It has been noted that "… the common law is generally antagonistic to personal search powers on the basis that they are "an affront to dignity and privacy of the individual".[215] While these powers have been extended by statute, including Commonwealth statute,[216] they are generally considered to be extraordinary powers that are most appropriately utilised in dangerous or emergency situations where the safety of an officer or community member is at risk, such as where there are concerns that a person might have a weapon or other prohibited or dangerous

[211] For further discussion of the Law Council's concerns with these powers see http://www.lawcouncil.asn.au/programs/criminal-law-human-rights/anti-terror/asio.cfm
[212] ASIO Act s25(4A)
[213] Discussion Paper p. 48
[214] Discussion Paper p. 48
[215] Department of the Parliamentary Library, *Bills Digest No. 128 2001–02 Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002* (1 May 2002) available at http://www.aph.gov.au/binaries/library/pubs/bd/2001-02/02bd128.pdf
[216] For example, personal search powers are found in the *Crimes Act 1914*, *Customs Act 1901*, and *Migration Act 1958*.

item.[217] This appears to be a context different to an investigation by ASIO, where it is suggested that the power to search a person is necessary to determine whether the person is "carrying items of relevance to security".

338. As noted above, something more than a broad reference to enhancing operational flexibility would need to be demonstrated before such a significant expansion of ASIO's powers should be considered necessary, particularly in light of the breadth of the existing provisions in section 25 that enables ASIO to search a person on or near specified premises and the range of other special powers available to ASIO.

Authorisation lists of classes of persons

339. Currently, under section 24 of the ASIO Act the Director-General[218] may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act.

340. The Discussion Paper provides that:

> *"The requirement to maintain a list of the individual names of each officer who may be involved in executing a warrant can create operational inefficiencies for ASIO. For example, sometimes the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to quickly expand the list of authorised persons."*[219]

341. The Discussion Paper suggests that this problem could be overcome if the Director-General could approve classes of people to execute a warrant. For example, if the Director-General could authorise officers of a certain level within a particular Division of ASIO to do so. The Discussion Paper states that these persons would be readily ascertainable ensuring that the level of accountability is not diminished, while improving operational efficiency.[220]

342. The Law Council draws attention to the fact that the current provisions already provide for an important level of operational efficiency by allowing the Director-General to specify a list of officers who may be involved in executing the warrant, rather than having to identify a particular officer. It is also noted that section 29 of the ASIO Act permits the Director-General to issue warrants without having to adhere to the usual requirements in cases of an emergency. It is not clear from the Discussion Paper why these provisions are insufficient to meet current operational demands.

343. For the Law Council, moving beyond the existing level of flexibility to allow the Director-General to authorise a list of persons based on a certain level within a particular Division of ASIO would tip the balance too far in favour of operational efficiency, and away from the need to strictly regulate the use of these intrusive and extraordinary powers. As noted elsewhere in this submission, improving operational efficiency, while a worthy goal, is not of itself enough to justify an expansion of powers or in this case, a dilution of important safeguards. The Law Council suggests that further evidence of the need for such a reform should be provided, along with reasons why alternative efficiency measures could not be employed to achieve the same level of operational flexibility.

---

[217] Department of the Parliamentary Library, *Bills Digest No. 128 2001–02 Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002* (1 May 2002) available at http://www.aph.gov.au/binaries/library/pubs/bd/2001-02/02bd128.pdf

[218] Or senior officer authorised in writing by the Director-General for the purposes of ASIO Act section 24.

[219] Discussion Paper p. 49

[220] Discussion Paper p. 49

Use of force and incidental entry

344. The Discussion Paper also contains proposals that suggest a need to "clarify" the scope of certain ASIO powers for the purpose of executing warrants relating to searching premises, accessing computers and applying tracking devices to objects used or worn by certain persons, as allowed by sections 25, 25A, 26B and 26C.

345. The Discussion Paper explains that subsections 25(7), 25A(5A), 26B(4) and 26C(4) relate to the use of force when exercising a power under these warrants and when entry into premises is authorised under the warrant.[221] It suggests that the powers in those subsections relating to the use of force are not limited to the target premises. It proposes that technical amendments may therefore be necessary to correct this "drafting anomaly".[222]

346. The sections referred to in the Discussion Paper concern search warrants, computer access warrants and tracking device warrants allowing tracking of persons and objects. Under the heading "Authorisation of entry measures" each of these sections contains a subsection which provides that the warrant must:

> *"… authorise the use of any force that is necessary and reasonable to do the things specified in the warrant."*[223]

347. In other subsections, these provisions state that the premises to which the warrant relates must be specified in the warrant. [224]

348. One interpretation of these subsections, contrary to that stated in the Discussion Paper, is that the use of force is to be authorised only in respect of the premises specified in the warrant. The subsections in questions are within a section designed to place strict limitations on the exercise and scope of these powers presumably in recognition of the impact of these powers on an individual's rights and liberties. This factor would favour a narrow construction of the provisions.[225]

349. The basis for the alternative construction in the Discussion Paper, namely one that would enable the use of force to be authorised in respect of premises not specified in the warrant, is not clear. However, if such a construction is advanced and accepted by the PJCIS, the Law Council would caution against using this construction as a reason to make "technical amendments" to the sections described above.

350. As discussed earlier in this submission, care should be exercised before expanding the already considerable powers of ASIO to enter and search premises, access computers and place tracking devices on people and objects. Evidence should be sought that would justify the need for such an expansion which should be considered in light of the privacy intensive nature of these powers, before any amendments of this nature are made.

---

[221] Discussion Paper p. 50
[222] Discussion Paper p. 50
[223] For example ASIO Act s25(7)
[224] For example ASIO Act s25(2)
[225] For example, the common law interpretation principle of legality assumes that the legislature did not intend to abrogate fundamental rights and freedoms 'unless such an intention is clearly manifested by unambiguous language, which indicates that the legislature has directed its attention to the rights or freedoms in question, and has consciously decided upon abrogation or curtailment", see *Al-Kateb v Godwin* (2004) 208 ALR 124 at [19] (Gleeson CJ), see also Pearce and Geddes *Statutory Interpretation in Australia* 7th edition (2011) pp. 190-198

351. Similar concerns arise in respect of the proposal to clarify the scope of the power to "do any thing that is reasonably incidental to the exercise of powers under that warrant" currently contained in sections 25 and 25A of the ASIO Act which relate to search and computer warrants. [226]

352. The Discussion Paper explains that is not clear whether this incidental power includes entry to a third party's premises for the purposes of executing the search or computer warrant. While it is not clear what particular amendments would be drafted to "clarify" the incidental power in this provision, the Law Council would caution against an approach which would extend the existing power to explicitly authorise entry to a third party's premises for the purposes of executing the warrant.

353. The Discussion Paper also suggests that it may be necessary to enter a third party's premises for the purposes of installing a surveillance device.[227] The Law Council also cautions against expanding the power to install a surveillance device to allow entry to a third party's premises for this purpose.

354. Allowing entry to a third party's premises for these purposes would constitute a significant expansion of ASIO's powers under these warrants and should be permitted only if shown to be necessary and proportionate to a security threat.

355. Even if evidence is adduced that justifies the need for powers of this nature, care should be taken before characterising these powers as "incidental". It may be more appropriate, for example, to consider whether a new warrant provision should be enacted that would set out a specific authorisation procedure for authorising entry to a third party's premises.

Creation of an authorised intelligence operations scheme

Nature of the Proposed Reforms

356. One of the most significant reforms proposed in the Discussion Paper is that concerning the creation of an authorised intelligence operations scheme (or controlled operations scheme) for ASIO officers, based on that currently available to certain law enforcement officers under the Crimes Act "with appropriate modifications and safeguards that recognise the scheme would operate in the context of covert intelligence gathering investigations or operations".[228]

357. The Discussion Paper explains that:

> *"An authorised intelligence operations scheme would significantly assist covert intelligence operations that require undercover ASIO officers or human sources to gain and maintain access to highly sensitive information concerning serious threats to Australia and its citizens."*[229]

358. Anticipating the potential for this proposed reform to raise serious concerns, the Discussion Paper also provides that:

> *"Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility*

[226] Discussion Paper p. 50
[227] Discussion Paper p. 50
[228] Discussion Paper p 46
[229] Discussion Paper p 46

and appropriate oversight and accountability. Key features that may contribute to such could include:

- *the Director-General of Security to issue authorised intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months);*
- *oversight and inspection by the IGIS, including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General;*
- *specifying conduct which cannot be authorised (for example, intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person), and*
- *independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement."*[230]

Law Council's concerns regarding an authorised intelligence operations scheme

359. The Law Council submits that the PJCIS should reject this proposed reform for the following reasons:

    (a) It constitutes a further blurring of the important distinction between the role and functions of ASIO as an intelligence agency and the role and functions of law enforcement agencies, and fails to address the differences in the oversight and accountability regimes that apply to these different agencies.

    (b) It has not been demonstrated to be necessary to fulfil ASIO's statutory functions, particularly in light of the range of other extensive powers available to ASIO.

    (c) There are other mechanisms available to protect ASIO officers from criminal prosecution. For example, even where an ASIO officer does engage in unlawful conduct, the Commonwealth Director of Public Prosecutions can elect not to prosecute.

    (d) In the context of prosecution for terrorism offences, it would not be necessary if these offences were properly defined. As academics Jennifer Goh and Nicola McGarrity have pointed out, the proposal "… says more about the excessive breadth of Australia's terrorism offences than it does about the need for ASIO officers to be given immunity from civil and criminal liability". [231]

    (e) It would threaten public confidence in the relationship between the citizen and the state by providing ASIO officers with indemnity if they break the law.

360. The Law Council has previously raised a number of concerns with attempts to expand controlled operations provisions in respect of law enforcement agencies. For example, in its submission on the *Crimes Legislation Amendment (Serious and*

[230] Discussion Paper pp. 46-47
[231] Jennifer Goh and Nicola McGarrity 'Just the beginning of a national security debate' *Inside Story* (2 August 2012) http://inside.org.au/just-the-beginning-of-a-national-security-debate

Organised Crime) Bill 2009[232] the Law Council raised a range of concerns with the amendments to the Crimes Act providing protection against criminal and civil liability for law enforcement officers who participate in controlled operations. The Law Council's primary concerns relate to the absence of necessary safeguards to limit the scope of these extraordinary powers and ensure appropriate accountability.

361. If, contrary to the Law Council's submission, the PJCIS recommends the introduction of an authorised intelligence operations regime that would cover ASIO officers, the Law Council submits that the following safeguards must be included:

(a) A requirement that an authorisation for an intelligence operation specify the nature of the criminal activities covered by the authorisation, the identity of each participant in the operation and the nature of the conduct in which the authorised participant may engage.

(b) Authorisation by an independent and external authority.

The Law Council notes that the Discussion Paper provides that it would be the Director-General of ASIO who would be empowered to authorise intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months). This would be accompanied by oversight and inspection by the IGIS, including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General.

The Law Council considers this authorisation process could be enhanced by removing the role of the Director-General and replacing this with an independent and external issuing officer, such as a Judge or AAT member, in addition to the proposed oversight by the IGIS. As the Law Council has previously submitted in the context of controlled operations for law enforcement officers,[233] this type of independent oversight is necessary to ensure that controlled operations are only authorised and conducted in strictly defined circumstances.

(c) A prescribed maximum duration for authorised intelligence operations of not more than six months

The Law Council is pleased to note that the Discussion Paper refers to the need to specify the period of any authorised operation, but queries whether 12 months would be appropriate.

(d) No extension of immunity from criminal and civil liability to informants

The Law Council has previously opposed controlled operation regimes that seek to provide immunity from criminal and civil liability to third parties such as informants,[234] and notes that this appears to be contemplated in the Discussion Paper by the reference to "undercover ASIO officers or *human sources*". The Law Council has previously submitted that this extension of

[232] Law Council of Australia submission to the Senate Committee on Legal and Constitutional Affairs Inquiry into the provisions of the *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009* (Cth) (10 August 2009).
[233] Law Council of Australia submission to the Senate Committee on Legal and Constitutional Affairs Inquiry into the provisions of the *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009* (Cth) (10 August 2009).
[234] Law Council of Australia submission to the Senate Committee on Legal and Constitutional Affairs Inquiry into the provisions of the *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009* (Cth) (10 August 2009).

indemnity is a cause for concern, and demands particularly robust external, independent authorisation processes that currently do not exist for controlled operations in respect of law enforcement officers and do not appear to be contemplated under this proposal. The Law Council has also submitted that, if obtaining admissible evidence from informants requires empowering police to confer immunity on known criminals, then such evidence comes at too high a price and is unlikely to be in the interests of justice in the long-term.

Conclusion

362. The Law Council recognises that Australian law enforcement and intelligence agencies confront operational challenges as a result of rapid changes in telecommunications technology and in terms of the way that this technology is used in the community. It is clear that the types of devices and services we use to communicate, and the frequency and volume of those communications, have changed dramatically since the legislation first introducing telecommunications interception powers was introduced. It is also clear that the way ASIO and other intelligence agencies go about collecting intelligence on matters relevant to national security has changed.

363. Notwithstanding this, it should also be emphasised that Australian law enforcement and intelligence agencies have requested enhanced powers many times in recent years on the basis of the need to respond to these challenges. In nearly all cases these requests have been granted, generally without a corresponding enhancement of safeguards and accountability provisions. As result, the current legislative regime contains a vast array of powers available to law enforcement and intelligence agencies to intercept and access telecommunications and to disclose telecommunication data. Similarly, the ASIO Act contains a set of special powers that have been continually expanded in the last decade to include personal and property searches, computer searches, and the covert use of listening and tracking devices.

364. It is against this background that the proposed reforms in the Discussion Paper must be assessed. Unless each of the proposed reforms can be shown to be necessary and proportionate in light of threats to national security, they should be rejected. It is not enough to point to the need to remove administrative burdens or enhance efficiencies – the proposed reforms must be shown to be the least intrusive means of achieving the law enforcement or national security outcome, having regard to their impact on individual rights.

365. Care must also be taken to ensure that any expansion in power is accompanied by a review of whether the existing safeguards and accountability measures remain appropriate. In many cases, the Law Council is of the view that these safeguards and accountability mechanisms should be enhanced, particularly in terms of those provisions designed to protect against unjustified intrusion into personal privacy.

366. Consideration must also be given to the different statutory functions and roles bestowed on intelligence agencies such as ASIO when compared with law enforcement officers such as the AFP. The Law Council cautions against attempts to replicate those powers currently available to law enforcement agencies, such as protection from liability under controlled operations, within the ASIO Act. These efforts risk extending ASIO's functions beyond those prescribed under the ASIO Act.

367. In conclusion, the proposed reforms are a clear attempt to ensure that Australia's law enforcement and intelligence agencies are appropriately equipped to respond to the challenges of the modern national security environment. While this aim should be pursued, it must not come at the cost of diluting the safeguards and accountability provisions that have been included in the existing legislative regimes.

Attachment A: Profile of the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its constituent bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Large Law Firm Group, which are known collectively as the Council's constituent bodies. The Law Council's constituent bodies are:

- Australian Capital Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Independent Bar
- The Large Law Firm Group (LLFG)
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of approximately 56,000 lawyers across Australia.

The Law Council is governed by a board of 17 Directors – one from each of the constituent bodies and six elected Executives. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive, led by the President who serves a 12 month term. The Council's six Executive are nominated and elected by the board of Directors. Members of the 2012 Executive are:

- Ms Catherine Gale, President
- Mr Joe Catanzariti, President-Elect
- Mr Michael Colbran QC, Treasurer
- Mr Duncan McConnel, Executive Member
- Ms Leanne Topfer, Executive Member
- Mr Stuart Westgarth, Executive Member

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