14 March 2014

Law Council
OF AUSTRALIA

Ms Sophie Dunstone
Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

Dear Ms Dunstone

Comprehensive Revision of the Telecommunications (Interception And Access) Act 1979

Attached is the Law Council of Australia's submission to the Senate Standing Committee on Legal and Constitutional Affairs inquiry into the Comprehensive Revision of the *Telecommunications (Interception and Access) Act 1979.*

The Law Council is grateful for the opportunity to make this submission.

Yours sincerely

MARTYN HAGAN
SECRETARY-GENERAL

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

Law Council
OF AUSTRALIA

Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979 (Cth)

Senate Committee on Legal and Constitutional Affairs

14 March 2014

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

Acknowledgement

The Law Council wishes to acknowledge the assistance of its National Criminal Law Committee, National Human Rights Committee, the Business Law Section's Privacy Law Committee and the Business Law Section's Media and Communications Committee in the preparation of this submission.

Executive Summary

The Law Council of Australia welcomes the opportunity to consider the *Telecommunications (Interception and Access) Act 1979* ('the TIA Act') and, in particular, the recommendations of the Australian Law Reform Commission ('ALRC') *For Your Information: Australian Privacy Law and Practice* report ('the ALRC Report'), dated May 2008, particularly recommendation 71-2, and recommendations relating to the TIA Act from the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') *Inquiry into the Potential Reforms of Australia's National Security Legislation* report ('the PJCIS Report'), dated May 2013.

In this submission, the Law Council expresses general support for the need for a comprehensive review of the TIA Act that considers: how this legislation fits within the broader surveillance and interception legislative regime; whether the TIA Act can and should respond to emerging technological developments; and what safeguards and other provisions should be included in the TIA Act to ensure that it does not unduly burden individual rights, including the right to privacy. The Law Council's position in response to the particular recommendations forming the Terms of Reference for this Review is outlined below.

The Law Council notes the ALRC observation that legislation dealing with surveillance in general, is not uniform throughout Australia.[1] Telecommunications interception and access under the TIA Act is only a part of surveillance regulation within Australia. The Law Council considers that concrete proposals for reform that seek coherence, consistency and uniformity across Australian jurisdictions in the area of surveillance regulation, including telecommunications interception and access, is needed and desirable.

In addition to these comments, the Law Council is also of the view that certain critical reforms of the TIA Act are urgently needed and should not be dependent upon the completion of a broader review process.

In particular, the Law Council considers that there is a need for immediate legislative amendments to the TIA Act to:

- introduce defined limits on the issue of B-party warrants and the derivative use of material collected by a B-party warrant;
- amend the threshold for access to telecommunications data with a view to reducing the number of agencies able to access such data;
- increase the penalty thresholds for stored communications warrants to apply only to criminal offences; and
- increase the threshold for sharing stored communications to that prescribed in sections 110 and 139 of the TIA Act.

[1] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era Issues Paper 43*, October 2013, p 47.

Introduction

1. The Law Council of Australia is grateful for the opportunity to provide the following submission to the Senate Legal and Constitutional Affairs Committee ('the Committee') in response to its comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* ('the TIA Act').

2. The Law Council notes that the Committee's review will consider the recommendations of the Australian Law Reform Commission ('ALRC') *For Your Information: Australian Privacy Law and Practice* report ('the ALRC Report'), dated May 2008, particularly recommendation 71-2, and recommendations relating to the TIA Act from the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') *Inquiry into the Potential Reforms of Australia's National Security Legislation* report ('the PJCIS Report'), dated May 2013.

3. The Law Council has a history of advocacy in relation to Commonwealth telecommunications interception and access and disclosure of telecommunications data. In particular, the Law Council has submitted that where a State seeks to restrict human rights, such as the right to privacy, for legitimate and defined purposes, for example in the context of telecommunications access and interception, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective.[2]

4. In the context of telecommunications access and interception, this involves balancing the intrusiveness of the interference, against operational needs. Interception of or access to communications will not be proportionate if it is excessive in the circumstances or if the information sought could reasonably be obtained by other means.[3]

5. In light of these principles, the Law Council has previously provided submissions to the PJCIS and the ALRC supporting a greater recognition of privacy interests in law enforcement, intelligence and telecommunications activities, while acknowledging the competing public policy interests involved in such activities.[4]

6. The Law Council's PJCIS submission included an overview of the TIA Act regime (Attachment A) regarding telecommunications interception and access to communications.[5] The Law Council's current submission to the Committee does not provide detailed comments on the telecommunication interception and access to communications framework, but instead focuses on the inquiry's particular Terms of Reference and addresses many of the recommendations relating to the TIA Act from the ALRC and PJCIS Reports. It also raises a general concern, not addressed by these recommendations, regarding the impact of B-party warrants on the privacy rights of individuals.

---

[2] United Nations 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].

[3] See United Kingdom Home Office, *Interception of Communications Code of Practice* Pursuant to Section 71 of the *Regulation o f Investigatory Powers Act 2000*, at http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/interception-comms-code-practice?view=Binary.

[4] See Law Council of Australia, *Submission to the Parliamentary Joint Committee on Intelligence and Security on National Security Legislation Reform*, 20 August 2012, at www.lawcouncil.asn.au ; Law Council of Australia, *Submission to the Australian Law Reform Commission on Privacy Law*, 20 December2007, at www.lawcouncil.asn.au.

[5] Law Council of Australia, *Submission to the Parliamentary Joint Committee on Intelligence and Security on National Security Legislation Reform*, 20 August 2012, pp 8-14, at www.lawcouncil.asn.au.

7. In line with its past advocacy in this area, the Law Council notes that there is a need for concrete reform proposals to be outlined, exposure draft legislation circulated for public consultation, and evidence provided that reform is necessary and proportionate to assist in the prevention and prosecution of criminal activity and to respond to threats to national security.

Preliminary Comments

8. The Law Council supports the need for a comprehensive review of the TIA Act that considers: how this legislation fits within the broader surveillance and interception legislative regime; whether the TIA Act can and should respond to emerging technological developments; and what safeguards and other provisions should be included in the TIA Act to ensure that it does not unduly burden individual rights, including the right to privacy.

9. The ALRC has observed that legislation dealing with surveillance in general, is not uniform throughout Australia.[6] Telecommunications interception and access under the TIA Act is only a part of a broader surveillance regime within Australia that invests state and federal law enforcement and intelligence agencies, and many other agencies, with intrusive powers to covertly access or intercept their communications and/or monitor their movements. Many of the Law Council's Constituent Bodies have raised concerns with these laws at the State level, and in particular, noted the lack of safeguards or other limitations to prevent against unjustified intrusion into the right to privacy.[7] Similarly, the Law Council has raised concerns with this regime as it operates at the federal level.

10. Further, the Law Council is of the view that there is a need for a fundamental restructure of the TIA Act to avoid its current unnecessary complexity. Such a restructure should involve the production of specific reform proposals, through a White Paper process or exposure draft legislation circulated for public consultation.

11. Any proposed restructure should also consider whether the TIA Act should be amended to provide a clear legislative basis for law enforcement and intelligence agencies to intercept or access telecommunications information from entities over whom they do not typically have jurisdiction, for example, from foreign satellite based services, social networking sites and foreign cloud providers. The Law Council considers that this type of reform should not be pursued in the absence of clear evidence demonstrating the need for law enforcement and intelligence agencies to utilise these powers as part of their statutory functions and in light of their existing powers. It must also be demonstrated that such powers can be effectively applied in practice and that they are necessary and proportionate to assist in the prevention and prosecution of criminal activity and to respond to threats to national security. Past proposals of this nature, including those outlined in the PJCIS Inquiry, lacked sufficient detail for the Law Council and others to evaluate whether reforms designed to respond to emerging technologies were needed, were likely to work in practice or would be accompanied by appropriate safeguards to protect against unjustified intrusion into the right to privacy.

[6] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era Issues Paper 43*, October 2013, p 47.
[7] For example, the Law Society of South Australia has made submissions in respect of the *Surveillance Devices Bill 2012* (SA), at http://www.lawsocietysa.asn.au/other/submissions_made.asp.

12. In making these general recommendations, the Law Council notes that a number of agencies, including the Australian Security and Intelligence Organisation ('ASIO'), are generally excluded from the operative provisions of the *Privacy Act 1988* (Cth) ('the Privacy Act') including the Information Privacy Principles.[8] Despite this, the Office of the Australian Information Commissioner ('the OAIC') has developed a useful proposed framework ('the 4A framework') for assessing and implementing new law enforcement and national security powers. The aim of the OAIC's 4A framework is to 'bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy'.[9] It includes a four stage process of: 'analysis' which determines whether there is a problem and whether the solution to the problem is proportionate, the least privacy invasive solution and in line with community expectations; 'authority' which provides for the circumstances an organisation will be able to exercise its powers and clear guidance as to who will authorise their use; 'accountability' that implements a range of safeguards including in relation to auditing the system and reporting mechanisms; and 'appraisal' which determines whether there are built in review mechanisms and periodic review to determine whether the measure delivered what it promised and at what cost and benefit. The Law Council would support such a framework applying in relation to the powers exercised under the TIA Act.[10]

13. The Law Council further notes that the need to evaluate national security legislation in light of its impacts on the right to privacy has also been recently acknowledged by the United Nations General Assembly and the United Nations High Commissioner for Human Rights. On 24 February 2014, the United Nations High Commissioner for Human Rights made public comments on the impact on the right to privacy of laws which authorise surveillance of an individual's electronic communication.[11] The High Commissioner referred to a resolution adopted by the General Assembly expressing their deep concern at the negative impact that surveillance and interception of communications may have on human rights.[12] The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to privacy in digital communication.[13] The General Assembly resolution further called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data. It emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law. The Law Council encourages this Committee to turn its mind to the relevant international law principles, in particular the right to privacy as protected by Article 17 of the *International Covenant on Civil and Political Rights* ('the ICCPR'), when undertaking this review of the TIA Act.

14. The Law Council also notes that the ALRC is currently conducting a review of Commonwealth Laws for consistency with traditional rights and freedoms. In this

[8] The Law Council notes that as a result of privacy law reform which commenced on 12 March 2014 the Information Privacy Principles have been replaced by Australian Privacy Principles.
[9] Office of the Australian Information Commissioner, *Privacy Fact Sheet 3: 4A Framework – A Tool for Assessing and Implementing New Law Enforcement and National Security Powers*, July 2011, at http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/law-enforcement/privacy-fact-sheet-3-4a-framework-a-tool-for-assessing-and-implementing-new-law-enforcement-and-national-security-powers.
[10] Ibid.
[11] Ms Navi Pillay, United Nations High Commissioner for Human Rights, *Opening Remarks to the Expert Seminar: The right to Privacy in the Digital Age*, 24 February 2014, Palais des Nations, Geneva, at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E
[12] Ibid.
[13] The United Nations General Assembly resolution that the United Nations High Commissioner for Human Rights refers to is Resolution A/RES/68/167: *The right to privacy in the digital age*, 18 December 2013, at http://www.un.org/depts/dhl/resguide/r68_en.shtml.

context, the Law Council considers that such a review should include a review of national security legislation, anti-terrorism and law enforcement generally, including the TIA Act, which may encroach upon traditional rights, freedoms and privileges. If the ALRC's review does include a consideration of the TIA Act, the Law Council suggests that any recommendations made by the ALRC in this area be considered as part of any future reviews of surveillance regulation and the TIA Act.

15. Before proceeding to address the Terms of Reference for the present PJCIS inquiry, this submission reiterates the Law Council's concern regarding the use and disclosure of information obtained by a B-Party interception warrant under the TIA Act. The Law Council understands that it is beyond the mandate of the current PJCIS inquiry to examine issues concerning the use and disclosure of information obtained under B-party warrants or to review whether the B-Party warrant system represents a necessary incursion into the privacy rights of non-suspects. Nonetheless, the Law Council is of the view that there are serious privacy concerns surrounding B-party warrants which require immediate Australian Government consideration of implementing appropriate and necessary restrictions to apply to the use and disclosure of information obtained under such a warrant.

16. These concerns extend to what appears to be a concerning trend towards the use of interception and access powers to target media outlets for the purpose of investigating criminal activity.

B-Party Interception Warrant

17. One of the most concerning developments in the area of telecommunications interception is the introduction of the B-Party warrant system. The current 'B-Party' warrant system was introduced into the TIA Act in 2006 and is contained in Parts 2.2 and 2.5 of the TIA Act.[14]

18. B-Party warrants effectively 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.

19. Under a B-Party warrant telecommunication interception can be authorised where a third party (a 'B-Party') is believed to be in communication with another person and that other person is engaged in, or is reasonably suspected of being engaged in, activities prejudicial to national security or involved in the commission of a serious criminal offence.[15]

20. The introduction of B-Party warrants represents the first time in Australia's history that law enforcement agencies have been given power to intercept telecommunications made or received by people who are not suspects.

21. In the view of the Law Council, the B-Party warrant system is a disproportionate response to the need to investigate threats to national security and serious criminal offences and is contrary to Australia's obligations under Article 17 of the ICCPR which provides that:

[14] B-Party warrants were introduced by the *Telecommunications (Interception) Amendment Act 2006* (Cth).
[15] See *Telecommunications (Interception and Access) Act 1979* (Cth) subparagraphs 9(1)(a)(i)(ia), 46(1)(d)(ii).

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.

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

22. In the case of criminal law enforcement agencies, B-Party warrants are available in circumstances where police are unable to identify and intercept the telecommunications services used by the suspect him or herself to make or receive communications, but where police believe, on reasonable grounds, that the suspect may contact a third party whose telecommunications services can be identified and intercepted. The third party may be anyone from the suspect's family members to his or her lawyer or even a media provider. Both the latter third parties may be targeted where for instance ASIO seeks to obtain information regarding a whistle-blower. As noted by Simon Bronitt and James Stellios:

    …the B-Party might be the suspected person's legal representative with the result that the interception may lawfully capture otherwise privileged communications. It is also wide enough to capture the privileged communications between the legal representative and other clients, as well as collateral intimate communications between the legal representative and spouse, which have no bearing on the investigation.[16]

23. In order to be issued a B-party warrant, police must be able to demonstrate that the information that would be obtained by the interception is likely to assist with the investigation. B-Party warrants are only available for the investigation of an offence punishable by a period of imprisonment of 7 years.

24. B-Party warrants received much attention during the Senate Legal and Constitutional Affairs Legislation Committee's *Inquiry into the Telecommunications (Interception) Amendment Bill 2006* ('the 2006 Bill'). The Committee noted that 'a principal problem with the B-party warrant is the potential for collecting a great deal of information which may be incidental to, or not even associated with, the investigation for which the warrant was issued'.[17]

25. The Senate Committee made a number of recommendations concerning B-party interceptions, including that the 2006 Bill be amended to introduce defined limits on the issue of B-Party warrants and the derivative use of material collected by a B-Party warrant. The Australian Government did not accept these two recommendations.

26. The ALRC has expressed concern that there is potential to collect a large amount of information about non-suspect persons under a B-party warrant, compared with other types of warrant.[18] The Law Council shares the ALRC's concerns regarding the impact of B-party warrants on the privacy rights of individuals.

27. The Law Council continues to maintain that innocent third parties should not be subject to covert surveillance and believes that the provisions in the TIA Act relating to B-Party warrants should be repealed.

[16] Simon Bronitt and James Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?', *Prometheus* (2006) 24:4, p 417.
[17] Senate Legal and Constitutional Affairs Legislation Committee, 'Provisions of the Telecommunications (Interception) Amendment Bill 2006', Parliament of Australia, Canberra, 2006, p 38.
[18] Australian Law Reform Commission, *Discussion Paper 72: Review of Australian Privacy Law*, September 2007, p 1056.

28. The intended purpose of a B-Party warrant is to ensure that where it is not possible to intercept a suspect's communications directly, an alternative option is available to obtain information relevant to the investigation by intercepting the 'B-Party's' communications with the suspect. In light of this purpose, the Law Council believes that the TIA Act should specifically limit the type of information obtained under a B-Party warrant that can be used or disclosed for any purpose to intercepted communications between the suspect and the B-Party.

29. Except in cases of emergency or imminent threat, there should be a clear prohibition on the use or disclosure of any information derived from intercepting a communication between the B-Party and a person other than the suspect. Although such a prohibition may deny agencies the benefits of valuable information unexpectedly obtained using a B-Party warrant, it is a necessary safeguard against the misuse of personal information.

30. In addition to this prohibition on use and disclosure, the Law Council also believes that, as long as there are no statutory limitations on the range or types of B-parties able to be monitored, the TIA Act should impose strict procedures for identifying and protecting otherwise privileged communication which might be obtained, for example, by intercepting communications between doctor and patient and lawyer and client.

ALRC Recommendation

31. The ALRC Report inquired into the extent to which the Privacy Act and related laws continued to provide an effective framework for the protection of privacy in Australia. Part J of the ALRC Report examined telecommunications privacy issues, including the interaction between the Privacy Act and the TIA Act, and made approximately 34 recommendations seeking to improve the telecommunications interception and access framework. The Law Council provided a submission to the ALRC inquiry and also attended one of the consultation meetings with the Department of Prime Minister and Cabinet to discuss the recommendations contained in the final report.

32. A number of telecommunications issues were raised during the ALRC inquiry that extended beyond the inquiry's Terms of Reference, including whether the TIA Act continues to be effective in light of technological developments, changes in the structure of communication industries and in community perceptions and expectations about communication technologies. The ALRC recommended (see Recommendation 71-2 below) that the Australian Government should initiate a review specifically to consider these issues. To date, the Australian Government is yet to respond to the ALRC's recommendations relating to telecommunications privacy issues.

ALRC Recommendation 71–2

> *The Australian Government should initiate a review to consider whether the Telecommunications Act 1997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider: (a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services; (b) how these two Acts interact with each other and with other legislation; (c) the extent to which the activities regulated under the Acts should be regulated*

under general communications legislation or other legislation; (d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and (e) whether the Telecommunications (Interception and Access) Act should be amended to provide for the role of a public interest monitor.

Law Council Position

33. As noted above, the Law Council is of the view that urgent amendments are needed to the TIA Act to prevent disproportionate intrusions on privacy. Notwithstanding the pressing need for these particular amendments, the Law Council supports a broad review of the TIA Act, provided that such a review focuses on the operation of the TIA Act in the context of its impact on the right to privacy, its compliance with rule of law principles, and the extent to which warrant and authorisations processes currently include sufficient safeguards and oversight mechanisms. These issues are outlined in further detail in relation to the PJCIS recommendations.

34. Over the last decade, numerous amendments have been made to the Crimes Act 1914 (Cth), the Australian Security and Intelligence Organisation Act 1979 ('the ASIO Act'), the Surveillance Devices Act 2004 ('the SD Act') , the Australian Crime Commission Act 2002 and the TIA Act which have adversely impacted on the privacy of Australians.

35. As recommended in the Law Council's submission to the ALRC Report, the Law Council believes that a broad review of the TIA Act is required to the extent to which the right to privacy has been increasingly compromised in Australia in response to an asserted, but largely unsubstantiated, need for increased law enforcement and intelligence gathering powers.[19]

36. In particular, the Law Council has expressed concern that:

    (a) the key term 'telecommunications data' is not defined;

    (b) the threshold test for when telecommunications data can be voluntarily disclosed to ASIO is unclear and difficult for people outside the agency to apply;

    (c) enforcement agencies are not limited to authorising the disclosure of telecommunications data for a purpose relevant to the performance of their functions;

    (d) the prohibitions on secondary disclosure and use do not extend to cover telecommunications data disclosed to ASIO;

    (e) there is unnecessary power to make regulations adding further agencies to the list of 'criminal enforcement agencies' on whom special powers are conferred; and

[19] Law Council of Australia, *Submission to the Australian Law Reform Commission on Privacy Law*, 20 December 2007, pp 43-53, at www.lawcouncil.asn.au.

(f) it is unclear why the definition of 'enforcement agency' needs to include either 'a body or organisation responsible *to the Ministerial Council for Police and Emergency Management – Police*' and '*the CrimTrac Agency*'.

37. In addition, the Law Council has raised concerns in relation to the power conferred on both ASIO and criminal law enforcement agencies to authorise the disclosure of prospective telecommunications data on a near real-time, ongoing basis for a period of 90 and 45 days respectively.

38. The Law Council also considers that the interception of and access to communications under the TIA Act requires additional oversight, such as the establishment of a Public Interest Monitor (PIM).[20]

39. All of the current oversight mechanisms are directed at reviewing interception and access powers *after* they have been exercised. For example, the following bodies have oversight of agency powers to intercept and access communications under the TIA Act:

(a) the Inspector General of Intelligence and Security ('IGIS') – over ASIO warrants issued by the Attorney-General;

(b) the Commonwealth Ombudsman – over law enforcement bodies such as the Australian Federal Police ('AFP') that access and intercept telecommunications (this includes specific powers to respond to complaints and enter premises occupied by agencies to obtain relevant information, inspect records and prepare report); and

(c) the Minister and the Parliament – over both ASIO and law enforcement bodies' use of powers under the TIA Act.

40. These mechanisms could be enhanced by the introduction of a PIM, which could invest the authorisation process with a more adversarial character, and provide a degree of transparency that is currently absent from the issuing process. The Law Council also notes that a member of the National Human Rights Committee has indicated that there is a benefit to having independent (as opposed to in-house) lawyers acting for the agency seeking the warrant.

41. The 'up-front' review role is performed by judges or Administrative Appeal Tribunal ('AAT') members who are tasked with issuing interception and access warrants and who must consider, in the context of each application, whether it is lawful, necessary and appropriate for an enforcement agency to be authorised to use such powers.

42. In carrying out this task, judges and AAT members are required to have regard to the following matters:

(a) how much the privacy of any person or persons would be likely to be interfered with by intercepting or accessing communications pursuant to the warrant;

(b) the gravity of the conduct constituting the offence or contravention being investigated;

[20] The Law Council first supported the establishment of a PIM in its *Submission to the Australian Law Reform Commission on Privacy Law*, 20 December 2007, pp 63-65, at www.lawcouncil.asn.au. The information provided in relation to the PIM in the current submission is an extract from the Law Council's 2007 Submission to the ALRC.

(c) how much the information obtained under the warrant would be likely to assist in connection with the investigation by the agency of the offence or offences;

(d) the extent to which methods of investigating the offence or contraventions that do not involve intercepting or covertly accessing communications have been used by, or are available to, the agency seeking the warrant;

(e) the extent to which the use of such alternative methods would be likely to assist in connection with the agency's investigation;

(f) the extent to which the use of such alternative methods would be likely to prejudice the agency's investigation, whether because of delay or for any other reason.

43. The secretive, *ex parte* nature of warrant applications under the TIA Act means that the judge or AAT member is required to consider all the above matters and reach a view purely on the basis of the uncontested assertions of the agency seeking the warrant. Often the agency's application will be prepared using a template document and even the supporting affidavit will rely on standardised paragraphs and phrases.

44. While the use of a PIM and legal representative involvement in this environment would not result in the introduction of new and, possibly conflicting evidence for the judge or AAT member to consider, it may assist in creating an adversarial environment in which a greater degree of scrutiny is brought to bear on the grounds advanced for seeking the warrant and for claiming that it is a necessary and justified intrusion into the privacy of those likely to be affected.

45. The Law Council should emphasise that if a PIM were to be involved in the application process, this would not relieve the judicial officer or AAT member from having to satisfy him or herself personally, based on the evidence presented, of each of the matters set out in section 46 and section 116 of the TIA Act.

46. For example, if a PIM appears in a warrant application or is consulted by police prior to making an application and, having reviewed the available material, he or she opts not to ask any questions or make any submissions in relation to the application, this should not encourage the judge or AAT member to then simply issue the warrant without personally engaging in the review and balancing process envisaged by the legislation.

47. Likewise, if the PIM singles out only one issue in the warrant application for comment and submission, this ought not relieve the judge or AAT member from turning his or her mind to each of the other warrant criteria and matters for consideration.

48. The introduction of a PIM is valuable only if it assists the judge or AAT member to review the information contained in warrant application more thoroughly and from more than one perspective. There is little value in introducing a PIM into the warrant application process if the result, in practice, is simply the transfer of responsibility for reviewing and interrogating the warrant application from the ultimate issuer of the warrant to the PIM. The judge or AAT member must still scrutinise the information at hand. Similarly, it is important that the role of the PIM carries proper weight and does not become a 'rubber stamp' process.

49. In relation to the proposal that a PIM be introduced for the purpose of assuming an information gathering and reporting role, the Law Council's preliminary view is that this would only be valuable if the PIM was able to offer a different and greater degree of scrutiny and oversight than the Commonwealth Ombudsman is able to provide.

50. The Law Council believes that the important question is not so much whether there ought to be more or different oversight bodies to monitor compliance with the TIA Act, but whether the bodies currently performing that role have the requisite resources and capacity to complete the task, particularly given the volume of warrant applications.

51. The ALRC did not recommend the establishment of a PIM because it considered that many of the functions of a PIM are adequately provided by other bodies.[21] It acknowledged, however, that most of these functions occur after a warrant has been issued or the interception or access of communications and recommended that the establishment of a PIM should be considered as part of a broader review of the TIA Act.[22] The Law Council supports this ALRC recommendation and notes that a PIM has been appointed in Victoria and has been successful in strengthening oversight for independently testing the evidence used by crime fighting and integrity bodies to apply for surveillance device warrants and telecommunications interception warrants.

PJCIS Recommendations

52. The PJCIS Report inquired into potential reforms of national security legislation. The PJCIS considered a wide range of proposed reforms to certain national security laws comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform. In July 2012, the Attorney-General's Department issued a Discussion Paper ('the Discussion Paper') which described the reform proposals. As noted, the Law Council made a submission to the Discussion Paper and also appeared at a public hearing on 14 September 2012 to give evidence before the PJCIS.

53. The Discussion Paper included a package of reform proposals, which comprised of telecommunications interception reform, telecommunications sector security reform and Australian intelligence community reform that the Australian Government intended to pursue. Many of these proposals were only outlined in broad terms, without a clear justification for why they were considered necessary and without detailed information relating to the types of safeguards or other accompanying provisions. In its submission to the PJCIS, the Law Council submitted that the broad scope of the potential reforms of national security legislation and the varying levels of detail in the Discussion Paper made it quite difficult to provide comprehensive comments that could effectively evaluate telecommunications privacy issues and also some of the very technical aspects that relate to proposed legislative reforms.

54. The Law Council supported some of the proposed reforms – such as those that were designed to strengthen protections against individual privacy in the TIA Act – but in many instances the Law Council was of the view that the proposed reforms had not been shown to be necessary in light of the already expansive powers available to agencies. Further, many of the proposed reforms did not appear to be accompanied by the types of safeguards and oversight requirements that would be needed to ensure that they do not authorise an unjustified intrusion into the rights and freedoms of individuals.

55. In raising these concerns, the Law Council recognised 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

[21] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, May 2008, p 2394, at http://www.alrc.gov.au/publications/report-108.
[22] Ibid.

in the community. It is clear that the types of devices and services that are used to communicate and the frequency and volume of those communications have changed dramatically since the first legislation on 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.

56. Notwithstanding this, it should 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 those challenges. In many cases, these requests have been granted, generally without a corresponding enhancement of safeguards and accountability provisions. As a 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 telecommunications data.

57. This is the background against which the current review must take place.

58. The two inquiries included in the reviews' Terms of Reference calls for further review of many of the key features of the TIA Act. The Law Council supports this process, however, it urges this Committee to exercise caution before supporting any proposals that would have the effect of expanding the scope of the interception and access powers under the TIA Act.

59. The recommendations made by the PJCIS followed an inquiry into reform proposals that were insufficiently detailed to enable a robust assessment as to whether they would constitute a necessary and proportionate response to an identified operational need. In addition, there has been a lack of Government response to the PJCIS recommendations, making it difficult to determine which, if any, reform proposals are likely to be pursued by the Government.

60. Until concrete reform proposals are outlined and accompanied by clear evidence that each particular reform is necessary and proportionate, the Law Council strongly opposes any recommendation that would broaden the scope of these already intrusive and expansive powers.

61. This does not preclude the Law Council responding to many of the PJCIS recommendations that seek to improve the operation of the TIA Act, and strengthen those features of the Act designed to limit the impact of such powers on the individual privacy or enhance existing safeguards or oversight mechanisms.

62. The Law Council's response to these recommendations is outlined below. The Law Council does not hold the appropriate expertise to evaluate PJCIS recommendations 11, 12, 14, 15 and considers that other interested stakeholders, such as those in the telecommunications industry with direct experience or those with technical expertise, are better equipped to answer these questions. However, the Law Council suggests that before amendments are made in line with those suggested in the recommendations, evidence would need to be provided to justify this claim.

PJCIS Recommendation 1

> *The Committee recommends the inclusion of an objectives clause within the Telecommunications (Interception and Access) Act 1979, which: expresses the dual objectives of the legislation – to protect the privacy of communications; to enable interception and access to communications in order to investigate serious crime and threats to national security; and accords with the privacy principles contained in the Privacy Act 1988.*

63. 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 ICCPR (as noted above).

64. Article 8 of the *European Convention on Human Rights* ('the 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.*

65. 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* released for discussion by the Department of Families, Housing, Community Services and Indigenous Affairs.[23] The exposure draft of the *Homelessness Bill* contained 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*.[24]

66. It also contained a provision that recognised 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.*[25]

67. 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.*

68. 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,[26] 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.

---

[23] 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 .
[24] Exposure Draft *Homelessness Bill 2012* Clause 3.
[25] Ibid, Clause 12.
[26] For example, Article 17 of the *International Covenant on Civil and Political Rights*.

69. 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.

70. 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.

71. The Law Council notes that a privacy based objects 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 – for example, in a manner which ensures that any 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 . 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. Specific, enforceable protections should be incorporated into the TIA Act to ensure that individual privacy is adequately protected through, for example, a privacy impact test and appropriate safeguards in the various warrant processes. Further, a privacy impact test and issues of proportionality must be supported by a requirement that compels a decision-maker issuing a warrant under the TIA Act to turn his or her mind to privacy considerations.

72. The Law Council notes that its support for a privacy protection objective in the TIA Act was shared by a number of other submission makers to the PJCIS inquiry, including the OAIC who suggested that the Privacy Act, 'as the privacy oversight instrument the public is most familiar with, reflects existing community expectations' and that:

> *Accordingly, incorporating the core principles and values that underpin the Privacy Act into the other privacy accountability frameworks will help ensure that they remain consistent with community values and expectations.*[27]

73. In its report, the PJCIS also stated that it recognised:

> *…the dual objectives of the TIA Act: to protect the privacy of communications by prohibiting unlawful interception, while enabling limited interception access for the investigation of serious crime and threats to national security.*[28]

74. Accordingly, the PJCIS recommended that:

> *Express recognition of these objectives within the legislation would provide clarity of the purposes of the legislation and some interpretive guidance.*[29]

PJCIS Recommendation 2

> *The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the Telecommunications*

[27] See the Office of the Australian Information Commissioner, *Submission No. 183,* pp 1-2 referred to in the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 12, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[28] Ibid, p 13.
[29] Ibid.

(Interception and Access) Act 1979 (TIA Act). Factors to be considered in the proportionality tests include the: privacy impacts of proposed investigative activity; public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and availability and effectiveness of less privacy intrusive investigative techniques.

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

75. The Law Council supports PJCIS Recommendation 2 that the Attorney-General's Department undertake an examination of the proportionality tests within the TIA Act. It considers that one way to strengthen the protections within the TIA Act against unjustified intrusion into privacy is to ensure that a consistent privacy impact test is applied before a warrant to intercept or access a telecommunication, or access to telecommunication data, is granted.

76. 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.

77. 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. Further, as noted a privacy impact test and proportionality tests must be supported by a requirement that compels a decision-maker issuing a warrant under the TIA Act to turn his or her mind to privacy considerations.

78. The Law Council's proposed test can be summarised as follows:

Before authorizing the use of an interception, access or disclosure power under the TIA Act the authorising officer must:

- *consider whether the exercise of the interception, access or disclosure power would be likely to deliver a benefit to the investigation or inquiry; and*
- *consider the extent to which the interception, access or disclosure is likely to interfere with the privacy of any person or persons; and*
- *be satisfied on reasonable grounds that the benefit likely to be delivered to the investigation or inquiry substantially outweighs the extent to which the interception, access or disclosure is likely to interfere with the privacy of any person or persons.*

79. 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.[30] In that context, the Law Council recommended that the following clause be introduced:

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

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.

80. 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.

81. 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.

82. The Law Council notes that a range of other submissions, including the AFP's, expressed support for strengthening the proportionality test for telecommunications interception warrants, noting that the current provisions has become 'increasingly out of balance to the changes in the way people communicate, the technology available to communicate and the use of that technology to commit crime'.[31] As a result, the AFP saw:

…benefit in strengthening the existing proportionality test to include consideration of the overall community good served by the investigation for which the interception is sought.[32]

83. The Law Council supports the useful discussion of proportionality tests provided by the Human Rights Law Centre in its submission to the 2012 PJCIS Inquiry:

Put broadly, general provisions setting out a proportionality analysis require that any limitation of rights be reasonable and demonstrably justified in a free and democratic society. The proportionality test is a two stage process.

First, the purpose of the limitation on the right must be of sufficient importance to a free and democratic society to justify limiting the right. This might also be described as requiring a 'pressing and substantial' objective, reflecting a need to balance the interests of society with those of individuals and groups. Examples of purposes for limitations that might accord with a free and democratic society include protection of public security, public order, public safety or public health.

Secondly, the means used by the State to limit rights must be proportionate to the purpose of the limitation.[33]

[31] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 15, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[32] Ibid.
[33] Human Rights Law Centre, *Submission No. 140 to the Parliamentary Joint Committee on Intelligence and Security, Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 2-3, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/subs.htm

PJCIS Recommendation 3

> *The Committee recommends that the Attorney-General's Department examine the Telecommunications (Interception and Access) Act 1979 with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.*

84. The Law Council notes that the TIA Act contains a number of reporting requirements in relation to telecommunications interception, as well as requirements to destroy records of intercepted information. The TIA Act also contains a number of mechanisms designed to provide independent oversight of the telecommunication regime. Under the TIA Act certain records must also be kept in relation to stored communications. The current information sharing and reporting requirements under the TIA Act are outlined in further detail at Attachment A.

85. The Law Council supports PJCIS Recommendation 3 that the Attorney-General's Department examine the TIA Act with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether privacy intrusion was proportionate to the public outcome sought. However, it does not support proposals that would remove any current restrictions on the communication, use or disclosure of information obtained under a TIA Act warrant or authorisation.

86. 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.

87. 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.

88. 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.

89. 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 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 necessary, and to protect against the potential for misuse or overuse of this information.

90. 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.

91. For example, the sharing of intercepted information is appropriately limited to law enforcement agencies and does not include other 'enforcement agencies' such as the

Australian Communications Media Authority. Currently, a broader range of agencies is 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 in its submission to the PJCIS Discussion Paper, 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.

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. Accordingly, the Law Council is of the view that the Attorney-General's Department should examine the TIA Act with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether privacy intrusion was proportionate to the public outcome sought in a manner which strengthens and clarifies 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

98. The Law Council notes that the proposal in the Discussion Paper to simplify reporting requirements appeared 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.[34] It is on this basis that the Law Council provided the following comments.

[34] See Discussion Paper footnote 27, p. 26.

99. 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.

100. 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.[35] 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.

101. 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.

102. The Discussion Paper noted 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.

103. It suggested that this contrasts to the reporting requirements currently contained in 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.[36] Under subsection 6(1) of the SD Act, the term 'law enforcement agency' includes the ACC, the AFP, the ACLEI, police forces of each State and Territory and other specified State and Territory law enforcement agencies.

104. 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:[37]

[35] TIA Act s 81A.
[36] *Surveillance Devices Act 2004* (Cth) (the SD Act) ss 48, 49.
[37] SD Act s44.

- 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:[38]
  - 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:[39]
  - 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.
- 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.[40]

[38] SD Act s45.
[39] SD Act s47.
[40] SD Act s48.

- 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.[41]

- 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?

105. 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.

106. 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.

107. For example, it may be necessary to retain section 36 of the TIA Act which allows States to legislate to specifically require State Ministers 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.

108. 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 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.[42]

109. 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

[41] SD Act s 49.
[42] Law Council of Australia, *Submission to the Senate Legal and Constitutional Affairs Committee's Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008*, 4 April 2008.

powers under the TIA Act.[43] Some of these mechanisms have also been supported by the 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.[44]

- consideration of the establishment of a 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 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.[45]

    - 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.

110. 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

[43] Law Council of Australia, *Submission to the Australian Law Reform Commission's Discussion Paper 72: Review of Australian Privacy Law*, 20 December 2007.
[44] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108), Recommendation 73-6, 12 August 2008, at http://www.alrc.gov.au/publications/report-108,
[45] Ibid, paragraphs 73.1332- 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.

(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.

111. 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.

112. 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.*[46]

PJCIS Recommendation 4

> *The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the Telecommunications (Interception and Access) Act 1979.*
>
> *Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.*
>
> *The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.*

113. The Law Council supports PJCIS Recommendation 4. The type of oversight obligations the Law Council supports are noted above in relation to PJCIS Recommendation 3, including the establishment of the PIM.

114. In particular, as noted, the Law Council reiterates its support for consideration of a model similar to the SD Act model (as set out under PJCIS Recommendation 3 above) whereby the Commonwealth Ombudsman would be the sole oversight body for law enforcement agency's under the TIA Act.

115. The PJCIS was not convinced that the SD Act model is appropriate, but was convinced of the need for the TIA Act oversight regime to be reviewed and improved to ensure the application of consistent standards of accountability and the adoption of a single perspective on best practice.[47]

116. Similarly, Telstra noted in its submission to the 2012 PJCIS Inquiry a desire for consistency of oversight arrangements:

[46] Discussion Paper p. 26.
[47] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 21, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.[48]

117. The Office of the Australian Information Commissioner ('the OAIC') also noted that existing oversight arrangements are fragmented and that this:

…can make it difficult for the public to discern which oversight body is responsible for overseeing the access and interception activities of a particular law enforcement agency. The OAIC is mindful that the nature of the activities undertaken by law enforcement agencies may mean that, in certain circumstances, it is not appropriate for these activities to be made public. In these circumstances, it is particularly important that effective oversight arrangements exist to ensure that these agencies are not exceeding their lawful authority and to give the public confidence that their personal information is being handled in accordance with contemporary community expectations. The OAIC suggests that providing the public with clear information about which oversight bodies are responsible for overseeing the access and interception activities of specific law enforcement agencies would provide a more appropriate level of transparency.[49]

118. Notwithstanding the PJCIS's view of the SD Act model, the Law Council submits that the Attorney-General's Department should consider such a model as an aid to providing the public with clear information about which oversight body is responsible for overseeing the access and interception activities. The SD Act model clearly identifies the responsible oversight body and explains the criteria applied to assess compliance.

PJCIS Recommendation 5

The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

119. The Law Council supports efforts to reduce the number of agencies eligible to access stored communications information under the TIA Act and considers that urgent legislative amendment to the TIA Act is necessary to prevent disproportionate privacy intrusion.[50]

120. Subsection 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.

[48] Ibid, p 20.
[49] Ibid, p 21.
[50] 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.

121. The current provisions regulating covert access to stored communications and introducing an expansive definition of 'enforcement agency' were introduced and passed in 2006.[51] The 2006 amendments sought to clarify the position surrounding access to stored communications which had previously been under dispute.

122. The 2006 amendments were subject to an inquiry by the Senate Committee on Legal and Constitutional Affairs.[52] During this Inquiry, many submissions argued that the range of agencies 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.[53]

123. 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.*[54]

124. 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. [55]

125. However, this recommendation was not reflected in the amendments as passed.[56] 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 PJCIS Recommendation 5.

126. As the Law Council has previously submitted,[57] 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.

127. The Law Council notes that this view that lawful access by agencies to telecommunications data ought to be restricted to protect the privacy rights of

---

[51] See *Telecommunications (Interception) Amendment Act 2006*.
[52] Senate Committee on Legal and Constitutional Affairs, *Report on Inquiry into Provisions of the Telecommunications (Interception) Amendment Bill 2006,* 27 March 2006, at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/ti/report/index.htm.
[53] For example, see Australian Privacy Foundation, *Submission to the Senate Legal & Constitutional Committee's Inquiry into the Telecommunications (Interception) Amendment Bill 2006*, March 2006, at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/ti/submissions/sublist.htm.
[54] 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.
[55] Ibid, Recommendation 2.
[56] 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
[57] Law Council of Australia, *Submission to the Senate Legal and Constitutional Affairs Committee's Inquiry into Telecommunications (Interception and Access) Bill 2007,* July 2007.

individuals was shared by many submissions to the 2012 PJCIS Inquiry, including those made by Liberty Victoria.[58]

128. An alternative approach was submitted by the Australian Mobile Telecommunications Association and Communications Alliance in their joint submission to the 2012 PJCIS Inquiry:

> *The Associations believe that rather than looking to defined the number of agencies that are eligible to access communications information (that being content and transactional data), a preferred approach should be to reserve access to communications information solely for purposes of addressing instances of serious crime or threats to national security. The nature of the crime/threat in each instance would then determine they type of information required, and the agency/agencies who are eligible to obtain access. If this approach is taken it will be important to be clear about what constitutes 'serious crime'.*

129. The PJCIS also considered that the appropriate mechanism to justify access to telecommunications data is the threshold at which access is granted and was satisfied that access to telecommunications data for serious crime and threats to security is justified.[59]

PJCIS Recommendation 6

> *The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the: privacy impact of the threshold; proportionality of the investigative need and the privacy intrusion; gravity of the conduct to be investigated by these investigative means; scope of the offences included and excluded by a particular threshold; and impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.*

130. The Law Council supports efforts to review the current offence thresholds that apply to obtaining a warrant to access or share a stored communication, however, it notes that urgent legislative amendments are needed in this area to prevent undue privacy invasion. In particular, legislative amendments are needed to:

(a) increase the penalty thresholds for stored communications warrants to apply only to criminal offences; and

(b) increase the threshold for sharing stored communications to that prescribed in sections 110 and 139 of the TIA Act.

---

[58] See Liberty Victoria, *Submission No. 143*, p6. See also Mr Bernard Keane, *Submission No. 117*, pp 3-4; Senator Scott Ludlam, *Submission No. 146*, p 3; Mr Ian Quick, *Submission No. 95*, p 5. Submissions made to the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 24-25, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

[59] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 25, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

131. Currently, two penalty thresholds must be met in relation to accessing and using stored communications:

(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.

132. In relation to the initial penalty threshold, paragraph 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 subsection 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.

133. 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;[60] 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).

[60] As defined in s5D of the TIA Act.

134. 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:

(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.

135. 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[61] 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'.[62]

136. 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.*[63]

---

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

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

[63] Australian Privacy Foundation, *Submission to the Senate Legal & Constitutional Committee's Inquiry into the Telecommunications (Interception) Amendment Bill 2006*, March 2006, at http://www.privacy.org.au/Papers/index.html.

137. Many submissions also raised concerns about the lower secondary threshold for sharing stored communication information which allows such information to be shared for the purpose of proceedings into offences carrying a punishment of 12 months imprisonment or 60 penalty units, for example.[64]

138. The Senate Committee recommended that the penalty thresholds in relation to the issue of stored communications warrants be raised to include only criminal offences.[65] However this recommendation was not adopted in the amendments as passed.

139. 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.*[66]

140. 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.

141. 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'.[67]

142. The Law Council also notes that the Inspector-General of Intelligence and Security has previously submitted to the PJCIS that 'proposals to standardise security warrant tests and thresholds must take into account the nature of each of these warrants and the level of intrusiveness'.

143. The PJCIS in its 2013 Report into National Security Legislation reform also noted that the:

---

[64] 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*, at https://www.efa.org.au/Issues/Privacy/tia-bill2006.html .

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

[66] Discussion Paper p. 24.

[67] 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, at http://www.lawcouncil.asn.au/shadom.x/apps/fms/fmsdownload.cfm?file_uuid=5FEEEFAE-1E4F-17FA-D2E6-8084811EA9AC&siteName=lca.

…appropriate threshold for access to telecommunications and access to stored communications (whether they be combined under a single test) requires careful consideration of the:

- *proportionality of the investigative need and the privacy intrusion;*
- *gravity of the conduct to be investigated by these investigative means;*
- *scope of the offences included and excluded by a particular threshold;*
- *impact on law enforcement agencies investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences; and*
- *privacy impact.*[68]

144. The Law Council agrees with the PJCIS view that 'there is very little difference in the privacy impact carried out if communications are accessed live via interception or after the communication takes place when accessed with a stored communications warrant'.[69] However, in the Law Council's view this lack of difference justifies increasing the lower threshold for sharing stored communications not decreasing it.

PJCIS Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes: the ability for the issuing authority to set parameters around the variation of attributes for interception; the ability for interception agencies to vary the attributes for interception; and reporting on the attributes added for interception by an authorised officer within an interception agency.

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures: attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated; oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.

145. The Law Council does not support Recommendation 7 on the basis that 'attribute based interception' has not been sufficiently defined in order to assess the true privacy implications associated with the implementation of such a model. In particular, the Law Council is concerned that an attributes based interception model may allow for an extremely broad 'catch-all' warrant that potentially allows for a disproportionately wide

[68] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 28-29, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[69] Ibid, p 29.

collection of information. The Law Council is also concerned that in the case of warrants issued to ASIO a power to allow the Attorney-General to vary a warrant, or ASIO itself, risks a lack of independent evidence to indicate whether particular attribute variation is necessary and proportionate.

146. The Law Council recognises the challenges that 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 this 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.

147. 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.

148. 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.

149. 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.

150. The Discussion Paper provided 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.[70]

151. 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.

152. The Law Council notes that a number of submissions to the 2012 PJCIS Inquiry expressed in principle support that interception be conducted on the basis of specific attributes of communications subject to appropriate oversight and accountability arrangements. The IGIS, for example, raised a range of issues for consideration should this proposal be adopted:

> *A key issue to be considered in this proposal is whether the warrants would be limited to interception based on the 'characteristics' described in the initial warrant (similar to a service warrant) or whether ASIO would itself be able to vary the warrant to add or remove 'characteristics' (similar to a named person warrant). If the proposal is for the latter then there needs to be certainty as to the parameters within which 'characteristics' can be added.*
>
> *…*

[70] Discussion Paper p. 21.

A further issue is the technological capacity to actually undertake this type of 'characteristic' – based interception – including whether the carriers should be responsible for collecting, processing and delivering the communications of interest or whether the agencies should be permitted to collect and retain large amounts of information in order to find the communications of interest. It is outside my area of focus to comment on the technology, cost or burden sharing aspects of the proposal. However, I would expect to see any regime include appropriate measures to ensure that the content of communications which were not the specific target of the warrant were not retained longer than necessary for 'sorting' and to ensure that such information is kept secure.

One of the important accountability and oversight requirements of the current regime is the requirement that ASIO provide a report to the Attorney-General after the expiration or revocation of each warrant. The report must include details of the telecommunications service to or from each intercepted communication was made as well as the extent to which the warrant has assisted ASIO in carrying out its functions. This measure would be particularly important in maintaining oversight and accountability of any discretion to add new characteristics for interception.[71]

153. The PJCIS noted the 'potential for attribute based interception to assist in arresting the decline of interception capability, while also adopting additional privacy protections'.[72]

154. The Law Council agrees with the PJCIS suggested possible attributes which may be used in these warrants to include:

- time of communication;
- location of a communication; and
- an identifier or address that uniquely identifies a service or account.[73]

155. However, as noted, the Law Council considers that the specific attributes needs further consideration and refinement to be further refined to ensure in order to assess the true privacy implications associated with the implementation of such a model.

PJCIS Recommendation 8

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the Telecommunications (Interception and Access) Act 1979 to ensure: protection of the security and privacy of intercepted information; and sharing of information where necessary to facilitate investigation of serious crime or threats to national security.

[71] Inspector-General of Intelligence and Security, *Submission No. 185*, pp 11-12 referred to in the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 34, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[72] Ibid.
[73] Ibid.

156. The Law Council supports PJCIS Recommendation 8 for the reasons outlined in relation to PJCIS Recommendation 3. It notes that a greater commitment to information sharing between intelligence and law enforcement agencies across jurisdictions is inevitable and desirable. However, it must be matched by a similar shared commitment to handling personal information in a manner which complies with agreed privacy principles.

157. The Law Council submits that it is appropriate for information obtained under the TIA Act to be subject to more rigorous legislative protections than other forms of information in a law enforcement agency's possession because of the particularly sensitive nature and the intrusive impact on a person's rights and privacy. Reforms should aim to strengthen and clarify existing provisions while recognising that different restrictions may be appropriate in light of the nature of the information obtained, and depending on what types of agencies have primary access to such information.

158. The Law Council supports the PJCIS view (as expressed in the PJCIS Report) that law enforcement and security agencies need to be able to share information to 'ensure that serious crimes and threats to national security can be investigated in a timely and thorough manner'.[74] However, the Law Council also shares the PJCIS concern about the 'proliferation of institutions that gather and share information, and the absence of consistent guidelines and sufficient oversight'.[75] Accordingly, the Law Council is of the view that that any amendments to the information sharing provisions provide appropriate privacy protections.

PJCIS Recommendation 9

> *The Committee recommends that the Telecommunications (Interception and Access) Act 1979 be amended to remove legislative duplication.*

159. The Law Council is of the view that the TIA Act should be amended to remove legislative duplication which can create unnecessary ambiguity, but caution must be exercised so that current privacy safeguards are not diluted.

160. For example, the Law Council would not support removal of legislative duplication where this would 'streamline' the existing warrant authorisation processes. 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 the particular safeguards that currently apply to the use of each specific power.

161. As the Law Council pointed out in its submissions to the *Telecommunications (Interception and Access) Bill 2006* and *Telecommunications (Interception and Access) Bill 2008*, 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.[76]

[74] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 41, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[75] Ibid.
[76] See for example Law Council of Australia, *Submission to the Senate Legal and Constitutional Affairs Committee's Inquiry into Telecommunications (Interception and Access) Bill 2006,* 13 March 2006; Law

162. 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 people, 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.

163. 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.

164. 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
- 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.

165. 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

Council of Australia, *Submission to the Senate Legal and Constitutional Affairs Committee's Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008*, 4 April 2008.

the relevant criminal penalty threshold that might apply. Consideration must be given as to how to address these differences.

166. 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.

167. 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.

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

169. The Law Council notes that the Attorney-General's Department considers that multiple types of warrant are no longer appropriate in a modern communications environment:

> *Key areas of duplication relate to the different types of warrants, including the distinction made between intercepted and stored communications.*[77]

170. The Department has observed that the duplicated nature of warrants leads to other forms of unnecessary legislative duplication, including oversight, record keeping and reporting provisions. For example:

- dual oversight of State and Territory agencies by both the Commonwealth Ombudsman and the relevant State or Territory oversight agency;
- three separate annual report requirements for telecommunications interception warrants, stored communication warrants and access to telecommunications data; and
- in the case of interception warrants there are separate annual reporting requirements for Commonwealth agencies and State prescribed authorities.[78]

171. The PJCIS was of the view that removing legislative duplication 'would help to make the interception regime easier for the general public, legal practitioners, law enforcement and the justice system to understand and apply'.[79]

172. The Law Council supports the removal of legislative duplication but not where this involves a single warrant regime which would make it difficult for issuing authorities to adequately assess the privacy impacts of the powers under the warrant. Given the

[77] Attorney-General's Department, *Submission No. 236,* p 18, referred to in the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 42, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[78] Ibid.
[79] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 42, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

particularly intrusive nature of telecommunications interception, legislative clarity must not be achieved to the detriment of privacy principles.

PJCIS Recommendation 10

The Committee recommends that the telecommunications interception warrant provisions in the Telecommunications (Interception and Access) Act 1979 be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features: a single threshold for law enforcement agencies to access communications based on serious criminal offences; removal of the concept of stored communications to provide uniform protection to the content of communications; and maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures: interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated; rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security; reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and Parliamentary oversight of the use of interception.

173. The Law Council holds concerns with the imposition of a single warrant process that could result in the dilution of specific safeguards. These concerns are outlined above under PJCIS Recommendation 9 and include, for example, that it would be extremely difficult for issuing authorities to adequately assess the privacy impacts of the powers under a single warrant which could apply to suspects and third parties, contain multiple interception powers, multiple targets, multiple people, multiple telecommunication devices and multiple telecommunication services.

174. If a proposal of this nature were pursued (which the Law Council opposes), the Law Council supports the safeguards recommended by the PJCIS. Further, the Law Council would recommend the Committee to adopt the Law Council's prescribed minimum matters that an issuing authority or authorising officer should be satisfied of before issuing a warrant, as outlined above under PJCIS Recommendation 7.

175. The Law Council notes that interception agencies are of the view that the proposal for a single telecommunications interception warrant would 'significantly increase administrative efficiency without diminishing accountability'.[80] Further that:

The relevant thresholds and privacy intrusions are essentially the same where communications are accessed via service device be they stored communications or intercepted in transit.[81]

[80] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 45, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

[81] Western Australia Corruption and Crime Commission, *Submission No. 156*, p 8, referred to in the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 45, at

176. However, the Law Council is of the view that privacy intrusions differ depending on the information to be obtained and the method of obtaining that information. Consequently, the Law Council continues to have concerns that a single warrant proposal has the potential to diminish accountability.

177. The Law Council notes that other submissions to the 2012 PJCIS inquiry also noted the need to ensure that any proposals for a single telecommunications interception warrant not diminish current privacy and accountability thresholds. The IGIS and the Gilbert + Tobin Centre for Public Law, for example, noted that that any proposal for a single warrant regime must incorporate issues of proportionality, necessity and appropriate levels of authorisation.[82] The Gilbert + Tobin Centre also raised the concern that:

> *…merging of named person warrants and telecommunications service warrants into a single category of warrant would result in law enforcement agencies using all the powers that are available to them (regardless of whether these powers are strictly necessary to investigate the criminal activity).*[83]

178. The PJCIS was of the view that a single warrant regime 'can deliver administrative efficiencies to interception agencies without removing the appropriate accountability and safeguards'.[84]

179. The Law Council acknowledges that administrative efficiencies may be gained through the adoption of a single warrant regime. However, such efficiencies must not be achieved at the expense of privacy concerns, and should only be adopted where appropriate accountability and safeguards exist.

180. On this basis, the Law Council recommends that if single warrant regime is introduced, it must be accompanied by an overarching safeguard that requires the decision maker to specifically address the impacts of the proposed warrant on the privacy rights of every individual affected by the warrant, and consider whether the use of such a warrant is necessary and proportionate in light of those privacy impacts. The outcome of these privacy considerations and the factors taken into account to arrive at the outcome, should be expressed recorded as part of the warrant process.

---

http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

[82] Inspector General of Intelligence and Security, *Submission No. 185*, pp 9-10; Gilbert + Tobin Centre for Public Law, *Submission No. 36*, p 9 referred to in the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 46, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

[83] Gilbert + Tobin Centre for Public Law, *Submission No. 36*, p 9 referred to in the Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 46, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

[84] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 47, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

PJCIS Recommendation 13

> *The Committee recommends that the Telecommunications (Interception and Access) Act 1979 be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.*

181. The Law Council supports PJCIS Recommendation 13 on the basis that the current TIA Act provides:

- insufficient guidance about when voluntary disclosure is permitted;
- agencies to authorise disclosure for purposes unrelated to their functions; and
- the lack of positive obligations on enforcement agencies to destroy in a timely manner material containing personal information which is irrelevant to the agency or no longer needed by the agency.

182. These reasons are further discussed below.

Insufficient guidance about when voluntary disclosure is permitted

183. In addition to setting out when government agencies can authorise the disclosure of telecommunications data, the 2007 amendment Act also introduced provisions into the TIA Act which set out when an employee of a carrier or carriage service provider can *voluntarily* disclose telecommunications data (that is, in the absence of a formal disclosure authorisation from an enforcement agency).

184. Specifically, Chapter 4 of the TIA Act now provides that:

a. a person may voluntarily disclose telecommunications data to ASIO if the disclosure is in connection with the performance by ASIO of its functions (section 174); and

b. a person may voluntarily disclose telecommunications data to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law (subsection 177(1)); and

c. a person may voluntarily disclose telecommunications data to an enforcement agency if the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (subsection 177(2)).

185. These provisions are similar to the voluntary disclosure exemption provisions previously contained in sections 283 and 131 of the *Telecommunications Act 1997* (Cth).

186. The Law Council believes that these provisions, particularly section 174, require further refinement if they are to effectively guide employees of carrier or carriage service providers about when they may lawfully, voluntarily and in an unsolicited manner disclose telecommunications data to ASIO.

187. Under section 174 of the TIA Act, voluntary disclosure of telecommunications data to ASIO is permissible if it is 'in connection with the performance by the organisation of its functions'.

188. Those functions are listed in section 17 of the ASIO Act and comprise a long and complex list. As a result, the Law Council believes that the threshold test applied by section 174 (that is, that the disclosure must be 'in connection with the performance by ASIO of is functions') is a very difficult test for a person outside of ASIO to apply.

189. In order to provide appropriate and clear guidance and parameters, the Law Council believes that section 174 should be amended to state more explicitly the circumstances in which voluntary disclosure of telecommunication data to ASIO is not prohibited. For example it may be necessary to specify that voluntary disclosure is permissible if it will assist ASIO in obtaining intelligence that is directly relevant to:

(i) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;
(ii) sabotage;
(iii) politically motivated violence;
(iv) promotion of communal violence;
(v) attacks on Australia's defence system; or
(vi) acts of foreign interference; whether directed from, or committed within, Australia or not; and

(ii) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a).

190. The Law Council believes that setting out the threshold test for voluntary disclosure in this more detailed way may reduce the risk that personal information will be disclosed to ASIO for an unauthorised purpose.

<u>Agencies permitted to authorise disclosure for purposes unrelated to their functions</u>

191. Following the 2007 amendments, sections 178 and 179 of the TIA Act permit all agencies defined as 'enforcement agencies' under the TIA Act to authorise (regardless of their particular function) the disclosure of telecommunications data for one of the following three purposes:

d. when it is reasonably necessary for the enforcement of the criminal law;

e. when it is reasonably necessary for the enforcement of a law imposing a pecuniary penalty; and

f. when it is reasonably necessary for the protection of the public revenue.

192. The Law Council believes that the TIA Act should not allow agencies to authorise the disclosure of information for a purpose which is beyond their mandate. The Law Council questions how an agency could be satisfied that a disclosure is 'reasonably necessary' if it is for a purpose unrelated to the agency's functions.

193. The Law Council believes that subsections 178(3) and 179(3) of the TIA Act should be amended to specifically state that an agency may not authorise the disclosure of telecommunications data unless it is reasonably necessary for one of the

three purposes listed above and unless it is reasonably necessary for the agency's performance of its functions. Without this additional limitation, there is an increased risk that agencies will gather extraneous personal information which they do not require and which is unrelated to the performance of their duties.

Destruction of non-material information

194. One of the issues raised directly in the ALRC Discussion Paper was whether the 2007 amendment Act (now Chapter 4 of the TIA Act) should include positive obligations on enforcement agencies to destroy in a timely manner material containing personal information which is irrelevant to the agency or no longer needed by the agency.

195. The Law Council strongly supports the inclusion of provisions which establish positive obligations of this kind and makes two specific observations with reference to Chapter 4 of the TIA Act.

(a) while telecommunications data does not include the content and substance of a *person's* private communications, it nonetheless reveals information about crucial matters such as their associations and their whereabouts. 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.

(b) chapter 4 allows for the employees of telecommunications carriers or carriage service providers to voluntarily and without solicitation disclose otherwise private information to ASIO and government enforcement agencies. To do so, they must form the view that the disclosure is reasonably necessary for one of a number of purposes, (such as the enforcement of the criminal law), about which they are unlikely to be expert. This may lead to the *ad* hoc, random disclosure of information unrelated to a particular case or investigation. It may also lead to an agency obtaining personal information which, on review, is not relevant to the performance of the agency's functions. In these circumstances it is particularly important that there is a statutory obligation to review the information disclosed in a timely manner, to make an immediate assessment as to its relevance and to destroy it if it is not relevant.

196. The Law Council notes that the Australian Mobile Telecommunications Association, iiNet and the Western Australia Corruption and Crime Commission also expressed support for the potential benefits to be derived from clear, straightforward and reasonable obligations.[85] The Western Australia Corruption and Crime Commission endorsed the inclusion of administrative requirements as part of the industry interception requirements.[86] The PJCIS also saw:

> *…benefit in providing detailed guidance on the obligations imposed on the telecommunications industry to ensure telecommunications providers and interception agencies alike understand the extent of those obligations.*[87]

[85] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 53, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.
[86] Ibid.
[87] Ibid, p 54.

PJCIS Recommendation 16

> *The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.*

197. The Law Council does not oppose mechanisms to assist agencies to reconstruct or decrypt the content of communications to which access has been authorised, however it queries the necessity for a criminal offence to address any identified needs in this area.

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

199. It is not clear 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.

200. 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*.[88] 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?

[88] 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.

- 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?

- 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?

201. The Law Council notes that the PJCIS shared the Law Council's concerns regarding the lack of clarity and detail in respect to this proposal. The Law Council understands the proposal is for an offence to apply where a telecommunications provider does not provide assistance to decrypt communications where those communications have been encrypted by that telecommunications provider. The Law Council shares the PJCIS' view, however, that 'there remains a lack of specify regarding the scope of the offence and the circumstances in which it may apply'.[89]

PJCIS Recommendation 17

The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority.

The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.

202. While the Law Council supports PJCIS Recommendation 17, it encourages the Government to develop timelines for telecommunications industry assistance for law enforcement and national security agencies in broad consultation that extends beyond investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. Other interested stakeholders, including privacy advocates and practitioners, oversight bodies should also be consulted.

PJCIS Recommendation 18

The Committee recommends that the Telecommunications (Interception and Access) Act 1979 (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following: clear protection for the privacy of communications; provisions which are technology neutral; maintenance of investigative capabilities, supported by provisions for

[89] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, p 64, at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

appropriate use of intercepted information for lawful purposes; clearly articulated and enforceable industry obligations; and robust oversight and accountability which supports administrative efficiency.

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the: Independent National Security Legislation Monitor; Australian Information Commissioner; ombudsmen and the Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

203. The Law Council supports PJCIS Recommendation 18. In addition, as noted above under the overview to the PJCIS Recommendations, the Law Council considers there to be a need for specific legislative reforms to be developed and justified by evidential information and subject to public consultation. The previous Discussion Paper (prepared for the PJCIS Inquiry) contained insufficient detail and insufficient justifying information to support the reforms proposed.

Recommendation 19

The Committee recommends that the Government amend the Telecommunications Act 1997 to create a telecommunications security framework that will provide: a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference; a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and powers of direction and a penalty regime to encourage compliance.

The Committee further recommends that the Government, through a Regulation Impact Statement, address: the interaction of the proposed regime with existing legal obligations imposed upon corporations; the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia; consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and impacts on competition in the market-place, including: the potential for proposed requirements to create a barrier to entry for lower cost providers; the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and any other relevant effects.

204. The Law Council supports the development of a regulation impact statement as contained in PJCIS Recommendation 19, but considers that this should be accompanied by an appropriate justice impact assessment.

205. As noted in the Law Council's Policy Statement on Justice Impact Assessments[90], a justice impact assessment would require Commonwealth Government Departments and Agencies to consider the potential impacts that a proposed legislative or regulatory change may have on the justice system. This includes impacts on:

- the nature and extent of legal inquiries and disputes;
- access to legal assistance services;
- the resources or workload of the federal courts and tribunals; and
- the cost of or access to criminal or civil justice system as a whole.

206. Justice impact assessments would extend the existing Regulatory Impact Assessment process to analysis of costs and impacts on the justice system.

207. The Law Council is concerned that the existing RIA process is focused on productivity and compliance costs for business. While agencies which draft and advance legislation or regulation are encouraged to give consideration to social and compliance impacts there is no requirement to consider the broader social impacts of a proposed regulatory change, including impacts on the Australian justice system.

208. In the absence of specific consideration of these impacts, there is a risk that there will be costs for the justice system and broader society which are unanticipated and not able to be assessed by Parliament and the broader community.

209. Impacts can, for example, be expected to arise in relation to increasing policy activity and criminal sanctions.

210. The Law Council support the introduction of a specific justice impact assessment component within the broader regulatory impact assessment framework.

211. Ideally, regulatory proposals impacting on the justice system should entail genuine consultation with key stakeholders, including courts and tribunals, legal assistance sector providers and legal professional peak bodies, at all stages of the regulatory cycle.

212. The Law Council notes that the robust approach to regulatory impact assessments adopted in the United Kingdom, Canada, the European Commission and the United State of Virginia all incorporate a justice impact assessment. The Law Council recommends the adoption of a justice impact assessment process in Australia, similar to the Justice Impact Test adopted in the United Kingdom.

213. Examples of matters a justice impact assessment process might consider under this model include potential impacts of new legislative or regulatory initiatives on:

- the volume, length and cost of legal inquiries and disputes;
- the workloads of courts and tribunals;
- access to, demand for and resourcing of publicly funded legal assistance services;

[90] Law Council of Australia, *Policy Statement on Justice Impact Assessments*, September 2013. The discussion of justice impact assessments as contained in this submission is based on excerpts from the Law Council's Policy Statement on Justice Impact Assessments.

- the cost of and demand for private legal services;
- access to, demand for, resourcing of and the workload of federal courts and tribunals and the ancillary impacts to state and territory courts and tribunals when exercising concurrent jurisdiction; and
- the criminal and civil justice system as a whole.

214. Accordingly, the Law Council recommends that any Regulation Impact Statement that is issued by the Government regarding a telecommunication security framework include such a justice impact assessment.

Summary of the Law Council's Position in response to the Terms of Reference

215. The Law Council has focused its comments on those recommendations made in the ALRC and PJCIS Reports in respect to which the Law Council has previously expressed views. On this basis the Law Council supports:

- greater recognition of privacy interests in law enforcement, intelligence and telecommunications activities, while acknowledging the competing public policy interests involved in such activities;
- a broad review of the TIA Act, provided that such a review focuses on the operation of the TIA Act in the context of its impact on the right to privacy, its compliance with rule of law principles, and the extent to which warrant and authorisation processes currently include sufficient safeguards and oversight mechanisms;
- the inclusion of an objectives clause within the TIA Act which contains a privacy focus and is supported by a privacy impact test and appropriate safeguards in the various warrant processes;
- an examination of the proportionality tests within the TIA Act by the Attorney-General's Department that considers for instance the privacy impacts of proposed investigative activity;
- 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;
- an examination of the reporting requirements in the TIA Act by the Attorney-General's Department to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought;
- a review of the oversight arrangements in the TIA Act by the Attorney-General's Department to consider the appropriate organisation or agency to ensure effective accountability under the Act, including a consideration of a role for a Public Interest Monitor;
- a review of the threshold for access to telecommunications data by the Attorney-General's Department. The Law Council recommends that unless a compelling case can be made for why the agencies referred to in section 5 of the TIA Act

should remain within the definition of an enforcement agency, they should be removed;

- a review of the offence threshold for stored communication warrants. The Law Council recommends raising the threshold to apply only to criminal offences, and possibly only 'serious offences';
- efforts to develop a warrant regime that focuses on better targeting the characteristics of the particular communication to be accessed or intercepted and enables it to be isolated from communications that are not of interest. In supporting the objects of this reform, the Law Council emphasises that any changes to the existing warrant regime must 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;
- a review of the information sharing provisions in the TIA Act by the Attorney-General's Department to ensure protection of the security and privacy of intercepted information and sharing of information where necessary to facilitate investigation of serious crime or threats to national security;
- amending the TIA Act to remove legislative duplication in a way that does not dilute particular safeguards that currently apply to the use of each specific telecommunication interception power;
- amending the TIA Act to include provisions which clearly express the scope of obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data;
- the Government to develop timelines for telecommunications industry assistance for law enforcement and national security agencies in broad consultation that extends beyond investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. Other interested stakeholders, including privacy advocates, practitioners and oversight bodies should also be consulted; and
- the accompaniment of a justice impact assessment on any Regulation Impact Statement that is issued by the Government regarding a telecommunication security framework.

216. The Law Council also holds concerns with a number of the issues raised in the recommendations made by the ALRC and the PJCIS. In particular, the Law Council holds concerns with the imposition of a single warrant process in so far is it may compromise specific privacy safeguards. The Law Council recommends that if a single warrant regime is introduced, it must be accompanied by an overarching safeguard that requires the decision maker to specifically address the impacts of the proposed warrant on the privacy rights of every individual affected by the warrant, and consider whether the use of such a warrant is necessary and proportionate in light of those privacy impacts. The outcome of these privacy considerations and the factors taken into account to arrive at the outcome, should be expressly recorded as part of the warrant process.

217. The Law Council also queries the necessity for a criminal offence for failure to assist in decrypting communications and calls upon law enforcement and intelligence gathering agencies to demonstrate identified needs in this area.

Conclusion

218. The Law Council recognises that the TIA Act reflects the telecommunications industry as it existed in 1979 when the Act was made. The rapid development of information and telecommunications technology in Australia since that time opens the door for new challenges for law enforcement and intelligence agencies. In the twenty-first century, the Australian community has become increasingly reliant on electronic devices as a basic tool of communication and a means for conducting business and personal affairs. These advances have created an environment in which it is clear that the current TIA Act needs amending to fully respond to modern communications in the prevention and prosecution of criminal activity and threats to national security.

219. The developing technology landscape, including in regards to social media, smart phones and GPS navigation systems, also poses associated privacy concerns. Many technologies involve the collection, use and transfer of personal information and therefore have the potential to impact on our privacy. Telecommunications interception, access and disclosure by law enforcement and intelligence agencies is a particularly intrusive interference and should occur only when it is necessary and proportionate to operational needs.

220. Care must be taken to ensure that any changes to the TIA Act do not come at the cost of diluting the safeguards and accountability provisions that have been included in the existing legislative regimes. The Law Council notes that there have been a number of reviews of the TIA Act, including the ALRC and PJCIS inquiries. Any future revision of the TIA Act must include detailed concrete legislative proposals with adequate time for public consultation so that the Australian Government, privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies can ensure that appropriate safeguards and accountability measures remain.

Attachment A: Overview of the TIA Act

The following attachment is an extract from the Law Council's Submission to the PJCIS on National Security Legislation reform (2012) and provides an overview of the TIA Act legislative framework.

Current Legislative Framework for Intercepting or Accessing Telecommunications

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.[91]

The TIA Act seeks to achieve these outcomes by:

- prohibiting the listening to or recording of communications; [92]
- prohibiting access to stored communications; [93]
- 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;[94] and
- establishing processes to enable access to telecommunications data[95] 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. [96]

Access to telecommunications data is otherwise prohibited under the Telecommunications Act. [97]

[91] 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.
[92] 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.
[93] Section 108 of the TIA Act prohibits access to stored communications. Stored communications are 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.
[94] TIA Act Chapters 2 and 3.
[95] 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.
[96] TIA Act Chapter 4.
[97] See for example Telecommunications Act ss276, 277, 278.

Telecommunication Interception Warrants

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 ACC), Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Federal Police (AFP) and certain declared State and Territory agencies.[98]

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.

The TIA Act provides that an 'eligible Judge'[99] or 'nominated Administrative Appeals Tribunal (AAT)[100] member' may issue a telecommunications interception warrant on application by an agency. This can be a telecommunications service warrant or a named person warrant.[101]

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

[98] 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/Telecommunications(InterceptionandAccess)Act1979AnnualReportfortheyearendingJune2011.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.

[99] 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.

[100] 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.

[101] TIA Act ss46, 46A.

regarding any previous warrants obtained in relation to the same matter.[102] In urgent circumstances, applications may be made by telephone. The warrant takes effect only when completed and signed by the Judge or nominated AAT member. [103]

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.[104]

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.

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.

In respect of telecommunication service warrants, the Attorney-General must be satisfied that:[105]

(h) 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

[102] TIA Act s49.
[103] 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.
[104] TIA Act ss46, 46A.
[105] TIA Act s9.

(i) 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.

When issuing a named person warrant, the Attorney-General must be satisfied that:[106]

(j) 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

(k) 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;

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

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

The maximum duration for these warrants is six months

ASIO can also apply for a telecommunications service warrant or a named person warrant for collection of foreign intelligence.[107] There is also provision for emergency warrants to be issued by the Director-General.[108]

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. [109]

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.[110] 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.

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.[111]

The TIA Act also contains a number of mechanisms designed to provide independent oversight of the telecommunication interception regime. For example, the ACC, ACLEI

[106] TIA Act s9A.
[107] TIA Act ss11A, 11B.
[108] TIA Act s10.
[109] TIA Act s12.
[110] 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.
[111] See TIA Act, ss 11C, 14.

and the AFP are required to maintain records relating to interceptions and the use, dissemination and destruction of intercepted information.[112] 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.[113]

Stored communications warrants

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.[114]

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.

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.

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.[115] In urgent circumstances, applications may be made by telephone.[116] In either case, the warrant takes effect only when completed and signed by the issuing authority.

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. [117]

[112] See TIA Act Part 2.7.
[113] 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).
[114] See TIA Act Part 2.7.
[115] TIA Act s112.
[116] 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.
[117] TIA Act s116.

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

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.

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.

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.[118] 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.[119]

Telecommunications data authorisations

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.

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.[120] For example:

- the disclosure of historical[121] or existing data may be authorised by an enforcement agency when it is considered reasonably necessary for the

[118] TIA Act Part 3.5 Division 2.
[119] TIA Act s161 and 164.
[120] 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.
[121] 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.

enforcement of a criminal law, a law imposing a pecuniary penalty, or for the protection of the public revenue.

- the disclosure of prospective data[122] 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.[123]

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.

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.

The TIA Act also allows senior ASIO officers to authorise access to historical telecommunications data and prospective data in certain circumstances.[124]

Current Information Sharing and Reporting Requirements

Information obtained from Telecommunication Interception Warrants

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;[125]
- 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.[126]

[122] TIA Act s180. Prospective data is data that comes into existence during the period the authorisation is in force.
[123] 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.
[124] TIA Act ss175-176.
[125] 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.

- the Secretary of the Attorney-General's Department must maintain a General Register which includes particulars of all telecommunications interception warrants[127] and this must be delivered to the Attorney-General for inspection every three months.[128]

- 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.[129]

- agencies must destroy restricted records which are original records.[130] 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.

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.[131]

- the Australian Crime Commission ('ACC'), the Australian Commission for Law Enforcement Integrity ('ACLEI') and the AFP are required to maintain records relating to interceptions and the use, dissemination and destruction of intercepted information.[132] 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. [133]

- parallel requirements are imposed by State and Territory legislation on State and Territory interception agencies. [134]

As is noted in the Discussion Paper, while the Commonwealth Ombudsman is responsible for inspecting the records of the ACC, the ACLEI and the AFP, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies.[135] The reports of the inspections of the declared State and Territory agencies

[126] 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.
[127] TIA Act s81A.
[128] 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.
[129] TIA Act s81C. The Special Register is delivered to the Attorney-General for inspection together with the General Register.
[130] 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.
[131] TIA Act s99, 104.
[132] TIA Act s80.
[133] TIA Act ss83-86.
[134] TIA Act ss34, 35, 92A.
[135] 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.*

are given to the responsible State or Territory Minister who must provide a copy to the Commonwealth Attorney-General.[136]

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:

(n) 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;[137]

(o) 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;[138]

(p) 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).[139]

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

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.

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. [140] 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.[141]

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.[142] The Act then outlines certain exceptions to this general rule, for example:

[136] TIA Act s35.
[137] TIA Act s65A.
[138] TIA Act s64.
[139] TIA Act s68.
[140] TIA Act s153.
[141] TIA Act s161 and 164.
[142] TIA Act s133.

(q) 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;[143]

(r) 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; [144]

(s) 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[145]

(t) the Director-General of Security can, in accordance with the relevant provisions of the ASIO Act,[146] 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;[147]

(u) 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 Australian Communications Media Authority ('ACMA') in the performance of its functions under the *Spam Act 2003;*[148] and

(v) 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.* [149]

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

[143] TIA Act s135.
[144] TIA Act s136.
[145] TIA Act s136.
[146] ASIO Act ss 18(3) or (4A), or s19A(4).
[147] TIA Act s137.
[148] TIA Act s138.
[149] TIA Act s139 .

Attachment B: 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 Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian 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 60,000 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 2013 Executive are:

- Mr Michael Colbran QC, President
- Mr Duncan McConnel President-Elect
- Ms Leanne Topfer, Treasurer
- Ms Fiona McLeod SC, Executive Member
- Mr Justin Dowd, Executive Member
- Dr Christopher Kendall, Executive Member

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