Law Council
OF AUSTRALIA

Telecommunications Amendment (Get a Warrant) Bill 2013

Senate Legal and Constitutional Affairs Committee

31 July 2013

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

Introduction

1. The Law Council of Australia is pleased to provide some brief comments to the Senate Committee on Legal and Constitutional Affairs (the Committee) as part of its inquiry into the provisions of the *Telecommunications Amendment (Get a Warrant) Bill 2013* (Cth) (the Bill).

2. The Bill was introduced by Australian Greens Senator Scott Ludlam on 18 June 2013 and seeks to amend the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) by inserting new provisions that require the Australian Security and Intelligence Organisation (ASIO) and certain enforcement agencies to obtain a warrant in order to access or disclose existing and prospective telecommunications data, and makes a number of related changes to the TIA Act.

3. The Law Council generally supports the objects of the Bill, which aim to introduce a greater level of oversight and accountability into the existing regime for authorising access to and disclosure of telecommunications data by certain enforcement and intelligence agencies. Many features of the Bill align with past recommendations of the Law Council, including recommendations to replace the system of authorisations for accessing and disclosing prospective telecommunications data with a warrant based system.

4. However, the Law Council is also of the view that the Bill does not address the full range of the Law Council's concerns in this area, such as those relating to:

    - the need to ensure robust and consistent protections against unjustifiable or disproportionate intrusion into personal privacy across the TIA Act regime;
    - ensuring that key terms are appropriately and clearly defined; and
    - ensuring that there are appropriate limits on secondary disclosure and use of telecommunications data.

5. As the Bill seeks to extend existing interception and stored communication warrant regimes to cover access to and disclosure of telecommunications data, a number of questions arise that the Law Council considers warrant careful consideration by the Committee. These include questions relating to whether the proposed changes:

    - provide adequate protection against unjustified intrusion into person privacy;
    - will ensure that appropriate detail is provided in applications for warrants to access or disclose telecommunications data in as part of warrants for other purposes;
    - will prescribe appropriate maximum time limits on accessing telecommunications data; and
    - will have implications for recording keeping, reporting and inspection obligations and powers.

The current interception and access regime under the TIA Act

6. As noted above, this Bill seeks to amend the TIA Act by inserting new provisions that require ASIO and certain enforcement agencies to obtain a warrant in order to access or disclose existing and prospective telecommunications data and makes a number of related changes to the TIA Act.

7. The current regime for seeking authorisation for accessing or disclosing telecommunications data is contained in Chapter 4 of the TIA Act which establishes processes to enable access to telecommunications data[1] 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.[2] Access to telecommunications data is otherwise prohibited under the *Telecommunications Act 1997* (Cth) (Telecommunications Act).[3]

8. 'Telecommunications data' is not defined in the TIA Act 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.[4] Both Chapter 4 of the TIA Act and the amendments proposed in the Bill refer to 'telecommunications data' as 'information or documents'.[5]

9. Chapter 4 of the TIA Act forms part of a broader regime designed to specify the circumstances in which it is lawful to intercept and access communications or authorise the disclosure of telecommunications data.[6] This includes:

    - Chapter 2, which prohibits the listening to or recording of communications[7] and establishes a warrant scheme to enable interception of or access to telecommunications to assist in the investigation of serious offences and serious contraventions or to assist in the performance of ASIO's functions.[8] Interception is defined in the TIA Act 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'.[9]

    - Chapter 3 which prohibits access to stored communications[10] (such as voice mail, e-mails and SMS messages) and establishes a warrant scheme to

[1] 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.
[2] TIA Act Chapter 4.
[3] See for example Telecommunications Act ss276, 277, 278.
[4] *Telecommunications (Interception and Access) Act 1979* (the TIA Act) s171.
[5] See for example TIA Act s171; *Telecommunications Amendment (Get a Warrant) Bill 2013* (Cth) clause 109A.
[6] 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.
[7] TIA Act s7.
[8] TIA Act Chapters 2 and 3.
[9] TIA Act s6.
[10] Section 108 of the TIA Act prohibits access to stored communications. Stored communications are: (a) communications which have passed over the telecommunications system, and are accessed with the assistance of a telecommunications carrier without the knowledge of one of the parties to the communication. Section 6AA provides that 'accessing' a stored communication means listening to, reading or recording it, by means of equipment operated by a carrier, without the knowledge of its intended recipient.

enable interception of or access to stored communications to assist in the investigation of serious offences and serious contraventions or to assist in the performance of ASIO's functions.[11]

10. These Chapters of the TIA Act also contain a detailed regime that governs what can be done with any information accessed or communication intercepted under these provisions.[12]

11. For example, under Part 2-6 of the TIA Act there is a general prohibition on dealing in intercepted information or interception warrant information[13] which is accompanied by a range of prescribed circumstances where communicating, recording or making use of lawfully intercepted information is permitted. For example, there are exceptions for dealing with this information for other purposes under Chapter 2, such as making an application for a subsequent interception warrant.[14] Certain persons are also permitted to communicate, make use of or record lawfully intercepted information in connection with the performance by ASIO 'of its functions, or otherwise for purposes of security'.[15]

12. Certain officers of enforcement agencies are also permitted to communicate lawfully intercepted information to other enforcement agencies, including State and Territory agencies, if the information relates, or appears to relate, to the commission of a relevant offence and meets other prescribed criteria.[16] Prescribed exceptions also exist for communicating lawfully intercepted information to foreign authorities in certain circumstances.[17]

13. These Chapters also contain provisions that outline the circumstances in which an employee of a carrier may, in the performance of his or her duties as such an employee, communicate or make use of intercepted information.[18]

14. Similar but not identical provisions exist in Part 3.4 of the TIA Act related to dealing with accessed stored communication information.

Access to and disclosure of telecommunications data under the TIA Act

15. Chapter 4 of the TIA Act contains a general prohibition on disclosure of telecommunications data.[19] It also includes a system of authorisations that enable certain enforcement agencies[20] and approved ASIO officers to access and disclose existing and prospective telecommunications data without needing to obtain a warrant.

[11] TIA Act Chapters 2 and 3.
[12] Part 2.6 of the TIA Act relates to dealing with intercepted communications, Part 3.4 relates to dealing with accessed stored communication information.
[13] TIA Act s63.
[14] TIA Act s63AA.
[15] TIA Act s34.
[16] TIA Act s68.
[17] TIA Act s68A.
[18] TIA Act s63B.
[19] Section 172 of the TIA Act contains a general prohibition on disclosure..
[20] "Enforcement agency" is defined in section 5 of the TIA Act and includes the Australian Federal Policy, the Australian Commission on Law Enforcement and Integrity, the Australian Crime Commission, 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 Australian Tax Office (ATO).

16. 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 a relevant enforcement agency.[21] This includes the disclosure of historical[22] or existing data when it is considered reasonably necessary for the enforcement of a criminal law, a law imposing a pecuniary penalty, or for the protection of the public revenue. It also includes the disclosure of prospective data[23] when it is considered reasonably necessary for the investigation of an offence with a maximum penalty of at least three years imprisonment.[24] Authorisations for such disclosure must include the information outlined in sections 180 to 183 of the TIA Act, which includes: details of the information or documents to be disclosed; 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 and a statement that the officer had regard to the impact on privacy.

17. Section 175 of the TIA Act empowers the Director-General or Deputy Director-General of Security or an approved ASIO officer to authorise the disclosure of existing telecommunications data if he or she is satisfied that the disclosure would be in connection with the performance by ASIO of its functions. Authorisations can also be made under section 176 of the TIA Act allowing ASIO access to prospective telecommunications data. However, the senior ASIO officer must not authorise the disclosure unless he or she is satisfied that it would be in connection with the performance by ASIO of its functions and is for a period of not more than 90 days.[25]

18. In addition to setting out when government agencies can authorise the disclosure of telecommunications data, Chapter 4 of the TIA Act also outlines circumstances 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). For example, under Chapter 4 of the TIA Act:

    - a person may voluntarily disclose telecommunications data to ASIO if the disclosure is in connection with the performance by ASIO of its functions;[26] and

    - a person may voluntarily disclose telecommunications data to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law;[27] and

    - 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.[28]

[21] 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.
[22] 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.
[23] TIA Act s180. Prospective data is data that comes into existence during the period the authorisation is in force.
[24] 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 Australian Customs and Border Protection Service (ACBPS) was the only body prescribed.
[25] TIA Act s176.
[26] TIA Act s174(1).
[27] TIA Act s177(1).
[28] TIA Act s177(2).

Amendments proposed in the Bill

19. The Bill seeks to repeal many of the key provisions in Part 4.1[29] and replace the existing authorisations system with a requirement for enforcement agencies and ASIO officers to obtain a warrant before accessing or disclosing existing or prospective telecommunications data. The proposed warrant system in the Bill seeks to build upon the existing warrant processes contained in Part 2.2 (relating to telecommunications interception) and section 116 (relating to stored communications) of the TIA Act.

20. In relation to access to telecommunications data by ASIO officers, the provisions proposed in the Bill would mean that, in addition to authorising interception of the content of telecommunications, a telecommunications interception warrant obtained under Part 2-2 of the TIA Act would also authorise an approved ASIO officer to access or disclose existing or prospective telecommunications data if it would or would be likely to assist ASIO in the carrying our its function of obtaining intelligence relating to the security matters mentioned in the Part 2-2 warrant.[30]

21. These changes would be made to reflect existing section 109 of the TIA Act which provides that in addition to authorising interception of telecommunications, a Part 2-2 warrant also authorises an approved ASIO officer to access a stored communication if the warrant would have authorised interception of the communication if it were still passing over a telecommunications system.

22. In relation to enforcement agencies accessing telecommunications data, the Bill proposes changes to sections 116 and 117 of the TIA Act. These provisions currently govern the issue and scope of stored communications warrants which can be obtained by an enforcement agency. The changes proposed in the Bill would expand the application of stored communication warrants to include access to existing or prospective telecommunications data. The new form of warrant would be a 'stored and other communications warrant'.

23. Currently, a stored communications warrant issued[31] under section 116 authorises covert access to stored communications in connection with the investigation of a 'serious contravention'.[32] 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.[33] Before issuing a stored communications warrant to an enforcement agency, an issuing authority must have regard to similar considerations to those in relation to telecommunications interception warrants, such as considerations relating to privacy effects, the seriousness of the contravention, the

[29] Item 12 of the Bill repeals Division 3 Part 4 of the TIA Act relating to authorisations for ASIO to access telecommunications data, and Items 12-14 repeal provisions in Division 4 of the TIA Act relating to authorisations for enforcement agencies to access telecommunications data. It is noted that the Bill will retain those provisions in Division 4 Part 4 relating to authorisations for access to existing information or documents for the purpose of locating missing persons.
[30] See *Telecommunications Amendment (Get a Warrant) Bill 2013* clauses 109A and 109B.
[31] 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 Administrative Appeals Tribunal (AAT) members or any person who has been appointed by the Attorney-General for this purpose.
[32] 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.
[33] TIA Act s112.

assistance that will be provided through the warrant and possible alternative methods of obtaining the relevant information. [34]

24. The Bill also makes a number of related changes to the TIA Act, such as replacing the word "stored" throughout the Act with "stored and other" (or "stored or other" in some cases). These amendments reflect the expansion of the kind of information that a stored communication warrant can be required for.

Law Council's Support for the Objects of the Bill

25. The purpose of this Bill is to "require normal warrant authorisation procedures for law enforcement and intelligence agencies that wish to access telecommunications data."[35]

26. As noted above, the Bill would do this by expanding certain warrant processes already contained in the TIA Act, such as those contained in sections 116 and 117 (relating to stored communications) or Part 2-2 (relating to telecommunications interception) of the TIA Act, to include access or disclosure of telecommunications data.

27. The existing provisions require the issuing authority to be satisfied of certain matters before authorising the interception of telecommunications or access to stored communications. For example, before issuing a named person warrant to an ASIO officer under Part 2-2, the Attorney-General must be satisfied that:

    - 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;[36]

    - the interception by ASIO of communications made to or from telecommunications services used by the person; or communications made by means of a particular telecommunications device or particular telecommunications devices used by the person will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relating to security; [37]

    - relying on a telecommunications service warrant to obtain the intelligence would be ineffective and there are no other practicable methods available to ASIO to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued. [38]

28. These requirements are considerably more onerous and detailed than those currently required to be met under the telecommunications data authorisation process in Division 3 Part 4 of the TIA Act.

29. Similarly, the requirements for the issue of a stored communications warrant to an enforcement agency under 116 are more onerous than those required to be satisfied before such an agency is authorised to access or disclose telecommunications data under the current provisions of the TIA Act. The requirements for issuing authorities include consideration of how much the privacy of any person or persons would be

[34] TIA Act s116.
[35] *Telecommunications Amendment (Get a Warrant) Bill 2013* Explanatory Memorandum p. 1
[36] TIA Act s9A(1).
[37] TIA Act s9A(1).
[38] TIA Act s9A(1) and (3)

likely to be interfered with by accessing stored communications under a stored communications warrant.

30. The changes proposed by the Bill will amend sections 116 and 117 of the TIA Act to include access to telecommunications data through a stored and other communications warrant and , and as a result, require issuing authorities to have regard to these types of matters before authorising access to or disclosure of telecommunications data.

31. The Law Council generally supports the objects of this Bill and those amendments that would replace the current authorisation process for accessing telecommunications data in Part 4 of the TIA Act with a warrant based system.

32. For many years, the Law Council has raised concerns with the broad scope and intrusive nature of the existing powers available to enforcement and intelligence agencies under the TIA Act and in particular with those provisions that authorise the disclosure of existing and prospective telecommunications data. [39]

33. Of particular concern to the Law Council has been section 176 of the TIA Act, which allows an eligible person within ASIO to authorise the disclosure of prospective telecommunications data to ASIO, on a near real-time, ongoing basis for a period of 90 days., Also of concern has been section 180 which allows an authorised officer within a criminal law enforcement agency to authorise the disclosure of prospective telecommunications data to that agency, on a near real-time, ongoing basis for a period of 45 days.

34. These provisions are significant because, in the case of mobile phones, telecommunications data includes information not only about who the user has communicated with, when and for how long; it also includes accurate information about the user's location. As result, the effect of sections 176 and section 180 can be akin to granting ASIO and certain enforcement agencies the ability to use a person's mobile phone to effectively track him or her.

35. Although section 180F requires that before an authorisation is issued under section 180, the authorising officer "must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure", the Law Council is concerned that this subsection has little value as it is not clear what it means to "have regard to" a person's privacy.[40]

[39] See for example Law Council of Australia Submission to the Senate Standing Committee on Legal and Constitutional Affairs on the *Telecommunications (Interception and Access) Bill 2007* (March 2007); Law Council of Australia submission to the Senate Legal and Constitutional Affairs Committee *Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008* (4 April 2008); Law Council of Australia submission to the Australian Law Reform Commission, Discussion Paper 72, *Review of Australian Privacy Law* (20 December 2007).

[40] The Law Council has previously submitted that this is evident from experience with the *Surveillance Devices Act* which contains a similar provision. Subsection 16(2)(c) of *Surveillance Devices Act* states that in determining whether to issue a surveillance device warrant, the issuing officer must have regard to the extent to which the privacy of any person is likely to be affected. However the Commonwealth Ombudsman's 2007 report on compliance with the *Surveillance Devices Act* reveals that in practice there is little evidence to suggest due consideration is given to privacy in the application and authorisation process relating to surveillance devices. Commonwealth Ombudsman, *Report to the Attorney-General on the results of inspections of records under s 55 of the Surveillance Devices Act 2004*, February 2007, p. 5. Subsequent reports by the Ombudsman continue to identify a tendency by agencies to provide insufficient information to establish a link between persons named in a warrant and the premises where the surveillance device/s were installed, which in turn continues to dilute the effectiveness of the privacy tests and other safeguards contained in that legislation. See for example September 2011-Report to the Attorney-General on the results

36. These concerns have led the Law Council to recommend that section 176 should be amended to require that, in order to obtain access to prospective telecommunications data, ASIO must obtain a warrant from the Minister, which the Minister must only issue if satisfied that:

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

    - the disclosure of the prospective telecommunications data will, or is likely to, assist ASIO in carrying out its function of obtaining intelligence relevant to security.

37. The Law Council supports the provisions of this Bill that align with these recommendations, including those that repeal sections 176 and 180 of the TIA Act. However, for the reasons outlined below, the Law Council suggests that the Committee give further consideration to certain components of the approach proposed in the Bill, which seeks to extend existing warrant processes rather than introducing a separate telecommunications data warrant regime.

Outstanding Law Council Concerns

38. In addition to the concerns described above, the Law Council has also expressed a range of other concerns in respect of the current provisions governing access to and disclosure of telecommunications data under the TIA Act. These include concerns that:[41]

    - the key term 'telecommunications data' is not defined;

    - the threshold test for when telecommunications data can be voluntarily disclosed to ASIO is unclear and difficult for people outside the agency to understand;

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

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

    - 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".

39. The changes proposed in the Bill would go some way to meeting the Law Council's concerns with the existing regime for authorising access to and disclosure of existing

---

of inspections of records under s 55 of the Surveillance Devices Act 2004 available at http://www.ombudsman.gov.au/reports/inspection/

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

and prospective telecommunications data. For example, the proposed amendments would:

- improve existing levels of oversight by requiring that enforcement agencies seek a warrant from an issuing authority such as a judge, and that intelligence agencies seek a warrant from the Attorney-General;

- require that certain matters be considered by the issuing authority, such as the nexus between the telecommunications data sought to be accessed or disclosed and a particular criminal offence being investigated or the particular intelligence function; and

- repeal the voluntary disclosure provisions that contain difficult and confusing tests; and

- repeal sections 176 and 180 of the TIA Act, which currently authorise the disclosure of prospective telecommunications data to certain intelligence and criminal law enforcement officers on a near real time basis.

40. However, the Law Council also notes that this Bill does not address the entirety of the Law Council's concerns in this area. For example the Bill does not seek to address the meaning of the term 'enforcement agency' or otherwise limit the scope of agencies that have access to telecommunications data under the amended provisions.

41. The Bill also fails to address the Law Council's concerns relating to inadequacy of the warrants regime contained in Parts 2-2 (relating to telecommunications interception) and section 116 (relating to stored communications) of the TIA Act. These warrants can apply for periods of up to six months and can be obtained urgently in the case of emergencies. The information obtained during the exercise of powers under these warrants can also be shared with other agencies, subject to limitations, and the type of information that can be obtained in the exercise of these powers can be highly sensitive, such as conversations that might otherwise be considered confidential (for example those between lawyer and client) or personal (for example those between husband and wife). The Law Council has previously expressed concern at the breadth of these powers and the lack of appropriate safeguards within the warrant process to protect against unjustified intrusions into personal privacy.[42]

42. Of particular concern is the fact that while the Bill increases scrutiny for the access and disclosure of telecommunication data by certain agencies, it fails to satisfactorily strengthen the existing protections in the TIA Act against unjustified intrusion into personal privacy.

43. As the Law Council has previously submitted, in order to protect against unjustified intrusion into personal privacy, the TIA Act should contain a single, consistent privacy impact test to ensure that privacy considerations are always taken into account before a warrant to intercept or access a telecommunication is granted or access to telecommunications data is authorised.

44. In its previous submissions, the Law Council has noted that privacy considerations are currently taken into account in the issuing of certain TIA Act warrants, but not all. The

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

Law Council has recommended that a consistent privacy test be applied in all warrant applications and in all authorisations to intercept, access or disclose telecommunications data.

45. The key features of the test proposed by the Law Council can be summarised as follows:

> *Before authorising 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.*

46. 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.[43] In that context, the Law Council recommended that the following clause be introduced:

> *"Before making 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."*

47. The Law Council suggests that a similar provision be included in the Bill that would apply to the proposed new warrant regime for accessing and disclosing telecommunications data.

48. Although privacy impacts are listed as one of a range of considerations within the warrant processes proposed in the Bill, a single, consistent "reasonable grounds" privacy test remains critical to ensure that the issue of privacy is more fully considered in this process.

49. The Law Council has most recently expressed these and many other concerns relating to the TIA Act to the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) as part of its inquiry into a number of potential reforms to Australia's national

[43] Law Council of Australia submission to Joint Select Committee on Cyber-Safety *Inquiry into the Cybercrime Legislation Amendment Bill 2011* (14 July 2011) available at http://www.lawcouncil.asn.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=69459E2B-C846-30EE-C1FD-17B77D7122E9&siteName=lca (the 2011 Cyber Crime Submission). The Law Council notes that subsequently section 180F has been inserted into the TIA Act which provides that: "Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters: a) the likely relevance and usefulness of the information or documents; (b) the reason why the disclosure or use concerned is proposed to be authorised. "

security legislation.[44] This Committee issued its report in May 2013 and made a number of recommendations for reform of the TIA Act, including reforms to the warrant regime in Part 2-2 (relating to telecommunications interception) and the system of authorisation of telecommunications data sought to be amended by this Bill. [45]

50. The Law Council notes that the PJCIS recommended that the Attorney-General's Department undertake an examination of the proportionality tests (such as those contained within Part 2-2 and section 116) within the TIA Act, having regard to the privacy impacts of proposed investigative activity; the public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and the availability and effectiveness of less privacy intrusive investigative techniques.[46] The PJCIS further recommended 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.

51. The PJCIS also recommended that the Attorney-General's Department review the threshold for access to telecommunications data, with a 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.[47]

52. The Law Council urges this Committee to have close regard to the report and recommendations of the PJCIS, in particular Recommendations 2 to 8, which have a particular bearing on the provisions of the TIA Act that are subject to amendment in this Bill.

Issues for Further Consideration

53. While the Law Council supports the general objects of the Bill and many of the amendments it proposes, the Law Council notes that the Bill seeks to make a number of important changes to a complex legislative regime without providing a detailed Explanatory Memorandum that outlines the full impact of these changes on other aspects of the regime.

54. For this reason, the Law Council suggests the Committee seek further information about the impact the changes will have on matters such as:

- Whether the proposed changes provide adequate protection against unjustified intrusion into person privacy. As discussed above, the Law Council considers that further amendments should be made to the TIA Act to introduce a single consistent privacy test.

[44] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security on Potential Reforms to National Security Legislation, 20 August 2012 available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

[45] Report of the Inquiry into Potential Reforms of Australia's National Security Legislation Parliamentary Joint Committee on Intelligence and Security (May 2013) Canberra (the PJCIS Report) available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm

[46] PJCIS Report Recommendation 2.

[47] PJCIS Recommendation 5.

- Whether the changes proposed in the Bill will ensure that appropriate detail is provided in applications relating to access to or disclosure of telecommunications data which are included in applications for warrants under Part 2-2 (relating to telecommunications interception) and section 116 (relating to stored communications). For example, Part 2-2 currently prescribes a range of matters that must be included in an application for an interception warrant that relate to telecommunication services and/or certain named persons. While the Bill seeks to extend this regime to accessing and disclosing telecommunications data, further adjustments may be needed to Parts 2-2 to ensure that applications for warrants to access or disclose telecommunication data contain adequate detail to ensure that the issuing authority can apply the test prescribed in proposed sections 109A and 109B. Similar issues may arise in the context of extending the stored communications warrant regime in section 116 to apply to telecommunications data;

- The maximum duration that an agency can access telecommunications data under the changes proposed in the Bill. For example Part 2-2 warrants can be obtained for a period of six months, whereas under section 176 authorisations for access to telecommunications data currently have a maximum duration of 90 days. This can be contrasted with stored communications warrants under section 116 which generally apply for a maximum of 5 days;

- The procedures for applying for Part 2-2 or section 116 warrants in cases of emergency, and whether these procedures are appropriate for the inclusion of access to or disclosure of telecommunications data;

- The impact of the changes on the continued existence of certain authorisation provisions in Part 4-1 of the TIA Act. For example, the Bill does not repeal section 178A (relating to authorisations for access to existing information or documents for the purpose of locating missing persons) or section 179 (relating to authorisations for access to existing information or documents for the purpose of enforcement of a law imposing a pecuniary penalty or protection of the public revenue);

- The implications of the changes for recording keeping, reporting and inspection obligations and powers. For example, currently section 186 outlines the information that must be provided to the Minister in relation to authorisations to access or disclose telecommunications data. This is a different regime to that contained in Part 2-8 of the TIA Act relating to Part 2-2 warrants and may require further legislative or administrative adaptation in light of the changes proposed in the Bill.

Conclusion

55. The Law Council has a long standing interest in the content and operation of Australia's telecommunications interception and access regime. It has previously raised concerns relating to the necessity and effectiveness of certain components of the TIA Act; whether it contains adequate safeguards to ensure appropriate transparency and accountability for those agencies exercising these intrusive powers; and whether it contains appropriate protections against unjustifiable or disproportionate intrusions into personal privacy.

56. .

57. These concerns have led the Law Council to make a number of recommendations designed to improve the level of accountability and oversight in Chapter 4, including recommending that a warrant process be introduced in order for ASIO to obtain access to prospective telecommunications data. The Law Council has also recommended that a single consistent privacy test be incorporated into the TIA Act to ensure that the impact of the proposed inception or access activity on the privacy of and individuals concerned is given adequate consideration in any warrant or authorisation process.

58. The Law Council supports the provisions of this Bill that align with these recommendations, including those that repeal sections 176 and 180 of the TIA Act.

59. However, this Bill seeks to address these concerns by extending existing warrant processes that have been designed to authorise access to intercepted communications or stored communications rather than introducing a separate telecommunications data warrant regime. As a result, careful consideration must be given to what impact the proposed changes will have on these existing processes. It is critical that those features of the existing regime that are designed to enhanced accountably and transparency and provide protection against unjustifiable or disproportionate intrusions into personal privacy are not diluted as a result of the amendments proposed in the Bill.

Attachment A: Profile of the Law Council of Australia

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

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

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

- Australian Capital 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.