20 January 2015

Law Council
OF AUSTRALIA

Mr James Nelson
Inquiry Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box Parliament House
CANBERRA ACT 2600

By email: **pjcis@aph.gov.au**

Dear Mr Nelson

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Please find attached the Law Council of Australia's submission to the Parliamentary Joint Committee on Intelligence and Security regarding its inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

The Law Council appreciates the opportunity to make this submission.

Yours faithfully

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

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Parliamentary Joint Committee on Intelligence and Security

20 January 2015

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 acknowledges the assistance of its Media and Communications Law Committee and the Privacy Law Committee of the Business Law Section, National Criminal Law Committee, National Human Rights Committee and Client Legal Privilege Committee and the Law Institute of Victoria in the preparation of this submission.

The Law Council agrees with the Law Institute of Victoria's recommendations regarding the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, which accord with key Law Council recommendations in this submission.

Executive Summary

1. The Law Council of Australia is grateful for the opportunity to provide comments to the Parliamentary Joint Committee on Intelligence and Security (the Committee) Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill).

2. The Australian Parliament and Government have a responsibility to ensure the security of Australia and its people. Our security and law enforcement agencies require appropriate powers to detect, prevent, and prosecute terrorist and major criminal activities. Such powers must also be a necessary and proportionate response to potential threats and not unduly impinge on the values and freedoms on which our democracy is founded.

3. The Law Council acknowledges that the Bill seeks to pursue the legitimate objective of addressing and preventing serious crime and terrorism.[1] However, the Law Council does not support the mandatory data retention scheme, as currently proposed, because:

    - the urgency for implementation of this legislation has not been demonstrated;
    - the scheme is not sufficiently defined to allow people to know the extent of the restrictions on their rights and freedoms and for service providers to know their legal obligations;
    - there are concerns about the proportionality of the data retention regime, privacy, security of the retained data, client legal privilege, feasibility and cost;
    - blanket mandatory data retention in respect of all citizens, residents and visitors has not been demonstrated as reasonable, necessary or proportionate;
    - the nature and scope of the telecommunications data to be retained, the service providers captured and the agencies that will be permitted access to such data is uncertain and subject to change by the Executive through regulation, rather than by the Parliament; and
    - it does not provide sufficient safeguards or restrictions for civil proceedings, non-law enforcement purposes or third-party access.

4. Consequently the Law Council recommends the Bill not be passed and that it be withdrawn, amended and released as exposure draft legislation for public consultation. This would accord with a previous recommendation by the Committee that a mandatory data retention scheme, if proposed, should be released first as an exposure draft.[2]

5. If this is not accepted by the Committee, the Law Council encourages the Committee to carefully consider how the Bill may be amended to address four key issues.

    - accessibility and legislative precision;
    - privacy and proportionality;

[1] The Law Council notes that the recent judgement of the Court of Justice of the European Union (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) *and Kärntner Landesregierung* (C 594/12) [2014] ECR*)* accepted that the objective of the EU Data Retention Directive, namely to assist in the fight against serious crime and terrorism in order to ensure public security, was a legitimate objective – see [42]-[51].

[2] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) 192 , recommendation 42.

- security of retained telecommunications data; and
- privileged and confidential communications**.**

6. Access to telecommunications data must be governed by a robust legislative regime to ensure access is only permitted when the public interest in detecting and addressing serious criminal activity outweighs the public interest in ensuring Australians can conduct their lives free from tracking and surveillance.

7. If a mandatory data retention scheme is introduced, the following provides a summary of some of the Law Council's key recommendations:

   (a) the data set must be clearly defined in the primary legislation;

   (b) the agencies which can access stored communications and telecommunications data should be exhaustively listed in the primary legislation;

   (c) access to telecommunications data should be limited to agencies required to investigate serious indictable offences or specific threats to national security;

   (d) access to telecommunications data should ordinarily be issued by an independent tribunal warrant. In an emergency, a Ministerial warrant may suffice;

   (e) specific protections for privileged and confidential information should be included in the scheme, for example, where agencies seeking access must demonstrate how such information will be protected before a warrant can be issued;

   (f) minimum standards for protecting the security of the data are needed;

   (g) a privacy impact assessment (PIA) of the scheme should be conducted by the Office of the Australian Information Commissioner (OAIC) prior to the Bill's enactment; and

   (h) the data retention period should be reduced to no longer than the minimal period required by law enforcement and security agencies.

What is the balance to be achieved?

8. The Law Council has identified the fundamental tenets of the rule of law in its Rule of Law Principles[3]. These principles require that the law must be both readily known, available, and certain and clear.

9. In assessing whether the Bill is sufficiently defined by law,[4] reasonable, necessary and proportionate to achieving a legitimate objective, its potential impact upon the rights of Australians needs to be balanced against the legitimate purpose of detecting criminal conduct and threats to national security and apprehending criminals.

10. The Law Council supports the previous views of this Committee that:

> *A mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed*.[5]

11. In the current Bill, this balance is uniquely difficult to achieve for several reasons.

12. As noted by the Court of Justice of the European Union (CJEU) in its ruling *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) *and Kärntner Landesregierung* (C 594/12) [2014] ECR, blanket retention of telecommunications data:

> *…taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*.[6]

13. Within the last few years, mass pervasive tracking and surveillance has become possible because of the advent of smart phones and other personal internet devices carried by individuals. Smartphone penetration in Australia is now over 75%.[7] Over one in three Australians access mobile content as the first thing they do in the morning and last thing at night. There are approximately 25 billion devices connected to the internet. By 2020, estimates put that number at 50 billion: that is an average of between 6 and 7 connected devices per person on the planet.[8]

14. The impact on privacy of the data retention scheme should be assessed in light of the growing proliferation of new technologies. It is reasonable to assume that the next ten

---

[3] Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011, Principle 1.
[4] Laws which seek to limit human rights must be prescribed by law. That is, they must be accessible and precise enough so that people know the legal consequences of their actions or the circumstances under which authorities may restrict the exercise of their rights – see Parliamentary Joint Committee on Human Rights, *Guidance Note 1: Drafting statements of compatibility*, December 2014, p. 1.
[5] Joint Parliamentary Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, (2013)190.
[6] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) *and Kärntner Landesregierung* (C 594/12) [2014] ECR 27.
[7] Alistair Leathwood, 'Connecting Consumers, Connecting Brands, Connecting Life' (Paper presented at Digital Next Australia 2014 Conference, <http://www.tnsaustralia.com/events/digitalnextaustralia/2014/presentations/alistair-leathwood-tns.html>, Sydney, July 2014) 8.
[8] Dave Evans 'The Internet of Things – How the Next Evolution of the Internet is Changing Everything' (White Paper, CISCO, April 2011 < http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>) 3.

years will see the development of new ways of monitoring individuals through advanced personal communications devices and other new technologies. This Bill should be assessed applying that assumption.

Scheme's necessity not sufficiently demonstrated

15. The Law Council understands that the context put forward by the Government for the Bill is as follows:

    - terrorism and other serious crimes are increasingly planned or otherwise facilitated through use of electronic communications;
    - data about electronic communications is increasingly useful in identifying potential criminal acts, actual and potential criminals and proving criminality; and
    - providers of telecommunications services do not have commercial incentives to retain data about communications for a sufficient period to enable law enforcement agencies to identify criminals and prove criminality.[9]

16. The Explanatory Memorandum to the Bill, sets out the rationale for the mandatory data retention scheme to be:

    … [the] protection of national security, public safety, addressing crime, and protecting the rights and freedoms of by [sic] requiring the retention of a basic set of communications data required to support relevant investigations.[10]

17. The Statement of Compatibility with Human Rights, contained in the Explanatory Memorandum to the Bill, argues that the scheme is justified due to the 'pressing social need' for enforcement agencies to effectively prosecute crime*:*

    Access to historical data and analysis of inter-linkages with other data sources is vital to both reactive investigations into serious crime and the development of proactive intelligence on organised criminal activity and matters affecting national security. In 2012 the Queensland Crime and Misconduct Commission (now the Crime and Corruption Commission) stated that more than one-fifth of all of their investigations were being undermined by telecommunications data not being kept. In 2014 the Australian Federal Police (AFP) revealed that it could not identify more than one-third of all suspects in a current, major child exploitation investigation, because the telecommunications data is not available.[11]

18. The Law Council considers that the 'pressing social need' and urgency for implementation of this legislation has not been demonstrated, particularly given that:

[9] See the Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) ; Commonwealth, Parliamentary Debates, House of Representatives, 30 October 2014, 12560 – 12562 (Malcolm Turnbull) ; Attorney-General and Minister for Communications, 'Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014' (Joint Media Release, 30 October 2014) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2014/FourthQuarter/30October2014-TelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill2014.aspx>.

[10] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 10.

[11] Ibid 6.

- certain features of the Bill will not commence until 6 months after the Act receives Royal Assent; and

- the scheme will not be fully functional until at least two years after commencement.[12]

19. The Law Council considers that the case for the mandatory data retention has not been made out because:

    - the ability of access to telecommunications data is not limited to national security or serious crime;

    - there is little evidence from comparable jurisdictions that have previously had mandatory data retention schemes to suggest that such schemes actually assist in reducing the crime rate, for example in Germany, research indicates that a mandatory data retention scheme led to an increase in the number of convictions by only 0.006%;[13];

    - there is a lack of Australian statistical quantitative and qualitative data to indicate:

        - the necessity of telecommunications data in securing convictions;[14] or

        - the cases where requests for telecommunications data could not be met because data had not been retained and its effect on an investigation.

20. The Law Council considers that any proposal to introduce a mandatory telecommunications data retention scheme should be preceded by rigorous and comprehensive review of the alleged deficiencies in current processes and unavailability of data needed for investigatory purposes. This should be undertaken by an appropriate body such as the Committee.

21. If the proposed scheme is to be progressed, it is vital that statistical reporting clearly indicates to the Australian community the times when access to retained data has resulted in a conviction, whether it has assisted in detecting serious criminal activity or assisted security agencies against threats to Australia's national security. Further, such reporting should explain where such success or assistance would be impeded because some providers may not be retaining the data in question. Statistics should

[12] See Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) cl2; Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 18.

[13] A 2011 study conducted by the Legal Services of the German parliament which concluded that the mandatory data retention scheme in Germany led to an increase in the number of convictions by only 0.006%. The study was in the context of arrests and charges by the German Federal Criminal Police (Bundeskriminalamt, BKA). The Law Council notes, however, that the study did not assess the impact the scheme had on protecting German security interests. That is, in terms of activities by the Bundesnachrichtendienst (BND) or the Federal Office for the Protection of the Constitution (Bundesamt fuer Verfassungsschutz – BfV). See Legal Services of the German Bundestag available at http://www.vorratsdatenspeicherung.de/images/rechtsgutachten_grundrechtecharta.pdf

[14] The TIA Act currently requires annual reporting of the effectiveness of information obtained under an interception and stored communications warrant in terms of the number of arrests, prosecutions and convictions. However, it does not require the effectiveness of authorisations for access to telecommunications data in terms of the number of arrests, prosecutions and convictions to be reported. On this basis, it is difficult to determine the true value of telecommunications data in terms of securing convictions and reducing crime. See also Paul Farrell, 'Metadata: most Australian police forces can't say how many times it has been used to prevent crime', *The Guardian* (online) , 29 December 2014 <http://www.theguardian.com/world/2014/dec/29/metadata-most-australian-police-forces-cant-say-how-many-times-it-has-been-used-to-prevent?CMP=share_btn_link>.

also be published on the specific type of data requested and the age of the data requested to demonstrate the necessity for a 2 year retention period.

22. While the Inspector-General of Intelligence and Security (IGIS) includes a summary of inspection activity in her annual report, including references to the Australian Security and Intelligence Organisation's (ASIO's) compliance with the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), the Office of the IGIS does not receive periodic reporting of the volume of ASIO's requests for telecommunications data.[15] Nor is such information required to be regularly reported publicly. The Law Council considers that the Act should include such requirements.

23. Recommendations:

- **The Committee should evaluate the necessity of such a scheme in view of the clear privacy risks and the risks to the integrity and public confidence in enforcement and security agencies in the case of unauthorised publication.**
- **The Committee should be satisfied that the categories of data in the draft data set such as category 5 (c) have a clear link to law enforcement purposes.**
- **The TIA Act should be amended to require the Attorney-General to report annually on the times when access to retained telecommunications data has resulted in an arrest, prosecution or conviction.**
- **ASIO or the IGIS's annual reports should be required to indicate the number of times when retained telecommunications data has been accessed and the instances in which such access has substantially assisted in investigating or addressing threats to Australia's national security.**
- **Enforcement, security and oversight agencies should be required to report on the type of data requested, the age of the data requested and the use made of that data.**

Accessibility and legislative precision

24. The Law Council considers that the proposed scheme is not sufficiently defined by the Bill to allow people to know the extent of the restrictions on their rights and freedoms and for service providers to know their legal obligations. The Law Council's Rule of Law Principles require that the law must be readily known, available, certain and clear.[16]

Scheme's application to a wide and indeterminate range of telecommunications service providers

25. The retention obligation of the Bill would be imposed on most providers of communications carriage services provided to the public between points within Australia or points within Australia and outside Australia (e.g. international services touching Australia). That is, it would apply to Australian telecommunications carriers,

[15] Senate Finance and Public Administration Legislation Committee, Parliament of Australia, *Supplementary Budget Estimates 2013-14*, (2014)138.
[16] Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011, Principle 1. See also Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Guidance Note 1: Drafting statements of compatibility* (2014) 1.

internet service providers (ISPs) and carriage service providers (CSPs), but only if they own or operate in Australia infrastructure that enables the provision of any of the provider's relevant services.[17]

26. The Bill does not define what 'infrastructure' is. This creates uncertainty about the application of the Bill to certain CSPs.

27. The Bill gives the Attorney-General power to make regulations to address such matters, including expanding the category of services that will be subject to data retention obligations (subparagraph 187(3)(b)(iii)). The Explanatory Memorandum claims this power to expand the application of obligations though delegated legislation is required to ensure:

> *…the data retention regime is able to remain up-to-date with rapid changes to communications technologies, business practices, and law enforcement and national security threat environments*.[18]

28. The Law Council considers that subparagraph 187(3)(b)(iii) is an inappropriate delegation of legislative power. Given the intrusive nature of the scheme and the obligations it imposes on service providers (which include significant economic cost), it is appropriate for Parliament to determine the range of services and range of service providers that will be captured. The Law Council agrees with the conclusion of the Senate Standing Committee for the Scrutiny of Bills (the Scrutiny of Bills Committee) that:

> *…how this scheme – which is highly intrusive of individual privacy – should be applied in a new technological context is a matter which will raise significant questions of policy that are not appropriately delegated by the Parliament to the executive government*.[19]

29. Recommendations:

- **The Bill should provide that the category of services and service providers that will be subject to data retention obligations should only be determined by the primary legislation rather than permitting expansion of obligations by delegated legislation.**
- **The Bill should define what is meant by a service provider which owns or operates in Australia 'infrastructure' that enables the provision of any of the provider's relevant services.**

<u>Implementation plans and exemptions from data retention obligations (clauses 187F and 187G)</u>

30. It is not clear why the proposed scheme draws certain distinctions in permitting exemptions from data retention obligations.[20] The decision of the Communications

[17] Peter Leonard, *Internet Data Retention in Australia – A Quick (but Deep) Dive into the new Bill*, (Gilbert and Tobin Lawyers, November 2014) 1.
[18] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 43.
[19] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, Alert *Digest*, No 16 of 2014, 26 November 2014, 4.
[20] Division 2 of Part 5-1A of the TIA Act establishes a data retention implementation plan scheme, providing industry with the ability to seek endorsement of a strategy to achieve compliance with the mandatory telecommunications data retention scheme. The CAC would be empowered to amend or accept an implementation plan – see proposed section 187F of the TIA Act. ACMA would have the power to review any

Access Co-ordinator (CAC) may be expressed broadly and may specify service providers in any way, for example by reference to a class of service providers. For example, the CAC may specify that any service provider that provides Internet Protocol Television (IPTV) services is not required to retain any data in relation to its IPTV service.

31. The legislative frameworks for the TIA Act and the Bill are to adopt a technology-neutral approach,[21] yet the Bill immediately makes provision for exemption on the basis of specific media without adequate explanation. The Law Council encourages the Committee to further investigate the justifications for such distinctions.

32. It is also unclear whether the Australian Communications Media Authority (ACMA) will have the power to review a decision by the CAC to grant an exemption or variation. As currently drafted, it appears that ACMA only has the power to review implementation plans. It is unclear whether an exemption or variation will constitute part of a service provider's implementation plan or be a separate process not subject to ACMA review. The Law Council considers amendment is required to the Bill and Explanatory Memorandum to ensure ACMA is empowered to review the exemption and variation scheme.

33. The Explanatory Memorandum to the Bill does not explain why merits review by an independent body such as the Administrative Appeals Tribunal is unavailable for decisions made by the ACMA in relation to implementation plans and CAC to grant an exemption or variation.

34. The Law Council notes that a number of ACMA's other decisions which affect service providers are subject to AAT review.[22]

35. The Attorney-General's Department's 'Australian Administrative Law Policy Guide' (2012) states that:

> *As a matter of policy, an administrative decision that will, or is likely to, adversely affect the interests of a person should be reviewed on the merits, unless there are factors justifying the exclusion of merits review*.[23]

36. Unless there are valid reasons for its exclusion, an administrative decision not to exempt or vary a particular telecommunications service provider's telecommunications data retention obligations is likely to adversely affect the interests of that provider – for example, in terms of the implementation and maintenance costs of storing the data securely – and should therefore be subject to merits review. This is particularly pertinent given that judicial review under the *Administrative Decisions (Judicial*

---

dispute over a request to amend a data retention plan (proposed subsections 187G(4) and (5) of the TIA Act). The proposed exemption regime in new Division 3 of new Part 5-1A would provide the CAC with a discretion to exempt or vary a service provider from the mandatory data retention obligations (proposed section 187K of the TIA Act). The CAC may grant this exemption or variation on his or her own volition or on application by a service provider. The Law Council notes that the exemption and variation scheme would allow exemptions or variations to be granted where telecommunications data relating to the relevant service is likely to be of little or no relevance to law enforcement or national security investigations, or where the cost of complying, either in full or in part, with data retention obligations in relation to the relevant service would be disproportionately high - Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 35.

[21] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 36.

[22] See for example decisions made under the *Radiocommunications Act 1992* (Cth) s285.

[23] Attorney-General's Department, 'Australian Administrative Law Policy Guide', (2012) 13 citing Administrative Review Council, *What decisions should be subject to merits review?* (1999).

Review) Act 1977 will not be available.[24] No valid reason for exclusion of such decisions from merits review has been identified by the Government.

37. Recommendations:

- **The Explanatory Memorandum to the Bill should be amended to:**
  - **more clearly explain why the scheme proposes to apply to certain forms of media and not others;**
  - **provide for merits review for decisions made by the ACMA in relation to implementation plans and by the CAC to grant an exemption or variation or explain why merits review is not available.**
  - **make it clear that a service provider would be able to make a complaint to the Commonwealth Ombudsman in relation to a decision by ACMA or the CAC.**
- **The Bill should be amended to require the CAC to report through the TIA Act annual reports or through ACMA annual reports the number of instances where exemptions or variations have been granted or refused.**

Wide and indeterminate range of telecommunications data to be retained

38. The Law Council's Rule of Law Principles require that the law must be readily known, available, certain and clear.[25] The current lack of definition to the scope of data to be retained in the Bill is inconsistent with this requirement.

39. Proposed subsection 187A(1) would require telecommunications service providers to retain certain categories of data as '(a) information of a kind prescribed by the regulations' or '(b) documents containing information of that kind' relating to any communication carried by means of the service. Proposed subsection 187(2) seeks to limit the range of data that may be prescribed for the purposes of paragraph 187A(1)(a) to specified categories, including information relating to the:

    - subscriber, accounts, telecommunication devices and other relevant services of a relevant service;[26]
    - source of a communication;[27]
    - destination of a communication;[28]
    - date, time and duration of a communication, or of its connection to a relevant service;[29]

[24] As decisions under the *Telecommunications (Interception and Access) Act 1979* (Cth) are not decisions to which the *Administrative Decisions (Judicial Review) Act 1977* (Cth) applies – see the *Administrative Decisions (Judicial Review) Act 1977* (Cth) sch 1 para (d)
[25] Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011, Principle 1. See also Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Guidance Note 1: Drafting statements of compatibility* (2014) 1.
[26] Proposed paragraph 187A(2)(a) of the TIA Act.
[27] Proposed paragraph 187A(2)(b) of the TIA Act.
[28] Proposed paragraph 187A(2)(c) of the TIA Act.
[29] Proposed paragraph 187A(2)(d) of the TIA Act.

- type of communication, or a type of relevant service used in connection with a communication;[30] and

- location of equipment, or a line, used in connection with a communication.[31]

40. Proposed subsection 187A(4) seeks to limit the telecommunications data to be retained by specifying that service providers cannot be required to keep information that is:

    - the 'content or substance of a communication',

    - an address to which a communication was sent on the internet from a telecommunications device, or

    - an address from which a communication was sent on the internet by a telecommunications device, using an internet access service.

41. However, if the service provider obtains a destination internet address identifier in the course of providing another service (e.g. an email service), the provider would be required to keep records of identifiers such as an IP address, port number or URL.

42. The scope of the telecommunications data set to be retained is indeterminate as what constitutes the 'content and substance of a communication' is not defined in the Bill.

43. Consequently, there is uncertainty about whether some types of telecommunications data would be considered 'content' (and thus excluded from collection). For example, it is not clear whether meta-tags would be captured. The Explanatory Memorandum to the Bill recognises that 'text messages and e-mails stored on a phone or other communications device are more akin to content than data,'[32] however, it does not explain how this is so.

44. While the prescribed data set is limited by sub-clauses 187A(2) and (4) of the Bill and does not include the 'content and substance' of a person's private communications, the categories of telecommunications data which may be prescribed are nonetheless broadly defined and may provide information about crucial matters such as their associations and their whereabouts. For example, the following information could be revealed about a person from the subset of telecommunications data proposed to be captured: medical connections, use of mental health services, use of suicide hotlines, use of domestic violence crisis support, use of child abuse support, use of alcohol, drug or gambling addiction support, use of support for rape victims, family associations, friendship groups, financial connections, legal connections, religious associations, political affiliations, professional affiliations, sexual associations, escort services, commercial preferences (for example, frequently accessed online shopping websites), location and movement.

45. The scope of the telecommunications data set to be retained is also complex as the Bill requires creation of data where the service provider is not currently capturing data that falls within the data set.[33] Some of the examples in the draft data set also reveal

[30] Proposed paragraph 187A(2)(e) of the TIA Act.
[31] Proposed paragraph 187A(2)(f) of the TIA Act.
[32] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 4.
[33] Stephen Dalby and Leanne O'Donnell, 'iiNet's response to Industry Consultation Paper – Telecommunications data retention – statement of requirements September 2014', (Response Paper,

the complexity of the data sought to be captured by this Bill. For example, category 5(c) 'the features of the relevant service that were, or would have been, used by or enabled for the communication'.

46. The method for separating or filtering the content and substance from the non-content of communications by service providers in the course of meeting their data retention obligations is also unclear. In practical terms, it is not clear, for example, whether service providers will retain both in order to meet their obligations under the scheme.

Inappropriate delegation of the data set to regulations

47. The Law Council's Rule of Law Principles require that where legislation allows for the Executive to issue subordinate legislation in the form of regulations, the scope of that delegated authority should be carefully confined and remain subject to Parliamentary supervision.[34] Such a requirement ensures that Executive powers are defined by law, such that it is not left to the Executive to determine for itself what powers it has and when and how they may be used.[35]

48. As a matter of good legislative practice, significant matters should be specified in primary legislation which generally undergoes extensive consultation, not potentially subject to change by Ministerial decision and regulation.[36] The categories of information which should be captured by the scheme will raise significant questions of policy and have very substantial financial, as well as privacy, implications.[37]

49. The 'kinds of information' (within defined categories) that might be required to be captured and kept are uncertain. Although the Government has provided an initial proposal (in the form of a draft Regulation) the data set is still in draft form and can be changed at any time. Given that service providers can be subjected to civil penalties for failing to comply with obligations under the scheme (see for example section 187M) and the impact of the scheme on individuals, the Law Council considers that it is inappropriate for the kind of telecommunications data to be prescribed by regulations. Both the categories of the data to be retained and the specific data set should be set out in the Bill itself.

50. The Law Council notes the Scrutiny of Bill Committee also considered paragraph 187A(1)(a) to inappropriately delegate legislative power. An indeterminate data set also fails to allow for a full consideration of the necessity and proportionality of the scheme.

51. Clauses 187(1)(2) enable the Minister to define the data that must be collected, stored and released to an authorised agency, subject to the stated limitations. The ability to prescribe by regulation the telecommunications data that must be retained may dilute Parliamentary scrutiny, and limit opportunity for meaningful discussion about whether capturing such data is appropriate in the circumstances. The key concern arises, as follows:

<http://www.iinet.net.au/about/mediacentre/papers-and-presentations/industry-consultation-paper-data-retention.pdf>, iiNet, 8 October 2014) 3.

[34] Ibid, Principle 6(a).

[35] Ibid, Principle 6.

[36] Senate Standing Committee for the Scrutiny of Bills, *Alert Digest,* No 16 of 2014, 26 November 2014, 3; Peter Leonard, *Internet Data Retention in Australia – A Quick (but Deep) Dive into the new Bill*, (Gilbert and Tobin Lawyers, November 2014) 3.

[37] Ibid.

- the nature of the telecommunications information, the retention and disclosure of which is authorised by the Bill, is a central and fundamental concern for Parliament in deciding whether the Bill should be enacted; and

- clause 187A of the Bill will empower the Minister to effectively vary the content and nature of the telecommunications information that must be retained by telecommunications providers.

52. Accordingly, the Minister may, by delegated legislation, expand the scheme in a way that may create further privacy and security concerns, breach fundamental privileges, and do so in a way that may be contrary to the intention of the Parliament.

53. Such a process may undermine the rule of law without an appropriate Parliamentary process to consider a significant, further diminution of civil rights.

54. Arguably, scrutiny by the Senate Rules and Ordinances Committee and the regulation disallowance process provides a mechanism for addressing these concerns. However, a regulation can have effect from the date of registration and it may be weeks or months before a disallowance motion may be tabled or considered by the Parliament. There is a clear and serious concern about the capacity for the Minister to extend the ambit of the legislation for an uncertain period, without scrutiny and with significant implications for fundamental civil rights or traditional rights and freedoms.

55. Recommendations:

- **The Bill should clearly define the types of telecommunications data and the specific data set to be retained.**
- **The power to prescribe by way of regulation the mandatory data set should be removed from the Bill.**
- **The Bill should define the distinction between the 'content and substance' of a communication (referred to in clause 187(4)(a) of the Bill), as opposed to 'telecommunications data'.**

Inappropriate determination of agencies empowered to access data through regulations

56. The Law Council considers that the Attorney-General's ability to further expand the agencies which can access stored communications or telecommunications data by way of regulation, unacceptably reduces the level of Parliamentary scrutiny of fundamental elements of the Bill. For example, clause 110A(3) enables the Attorney-General to expand the number of agencies which can apply for a stored communications warrant, by declaring, on request, that an agency is a 'criminal law-enforcement agency'. This raises the prospect that agencies required to impose pecuniary penalties or protect public revenue may be given access to stored communications.[38]

[38] Currently, under the TIA Act 'enforcement agencies' can access both stored communications (i.e. the content of emails or SMS messages) and telecommunications data. Access to stored communications requires a warrant[38] whereas access to telecommunications data does not. An 'enforcement agency' is defined to include: the AFP; State and Territory Police; investigative bodies such as the Australian Crime Commission and the Independent Commission against Corruption; CrimTrac; and any body administering a law that imposes a pecuniary penalty or protects public revenue – see *Telecommunications (Interception and Access) Act 1979* (Cth) s5. Clause 110A(1) of the Bill would amend the TIA Act to provide that only a 'criminal

57. Further, under subclauses 176A(1) and (3) the Attorney-General can expand the 'enforcement agencies' that may access telecommunications data by way of regulation. The Minister may declare *any* authority or body an enforcement agency where the Minister considers it may be relevant.[39] This could include, for example, local councils, organisations responsible for enforcing copyright infringement and gambling authorities.

58. Expanding the number of agencies that may have access to stored communications and telecommunications data raises similar concerns to those outlined above. Vesting such a power in the Minister, notwithstanding disallowance procedures available to parliament, may significantly increase the ambit of the legislation and frustrate the intention of the Parliament. Even if a regulation was in force for a short period of time, this would be sufficient for any number of agencies, not previously authorised by the Parliament, to obtain stored communications data or telecommunications data.

59. Identification of the enforcement agencies which are permitted to access telecommunications data and the conditions on which such access is allowed should remain the prerogative of Parliament, not the Executive, to ensure adequate scrutiny of the necessity and potential consequences of expanding such access.

60. The Law Council submits that the agencies permitted access to stored communications and telecommunications data should be declared by way of a list scheduled to the TIA Act.

61. **Recommendations:**

The Bill should be amended so that the **agencies that may have access to:**

- **stored communications warrants are by way of a list scheduled to the legislation – not via regulation or other legislative or executive instrument; and**

- **telecommunications data under the scheme are the agencies:**

  - **that may have access to telecommunications data warrants; and**

  - **listed in a schedule to the legislation – not in regulation or other legislative or executive instrument.**

Proportionality

62. Limitations on law enforcement and national security agencies' powers are necessary to ensure the scheme is proportionate. A scheme which applies to all Australians and imposes high-cost obligations, and civil penalties on service providers, argues for appropriate limits.

law enforcement agency' may apply for a warrant to access stored communications. A 'criminal law enforcement agency' will be defined to include agencies such as the AFP, State Police forces, and anti-corruption bodies. Authorities responsible for imposing pecuniary penalties or protecting the public revenue are not included.

[39] Proposed paragraph 176A(4)(f) of the *Telecommunications (Interception and Access) Act 1979 (Cth)*.

Two year retention period

63. The Law Council considers that the two year retention period required under the scheme is unusually long by international standards and has not been satisfactorily justified. Law enforcement and security agencies have advised that a 'data retention period of two years is appropriate to support critical investigative capabilities.'[40] The Explanatory Memorandum notes that, despite telecommunications data being accessed by agencies under other data retention regimes frequently being less than six months old 'there was a higher requirement for data up to two years old for national security and complex criminal offences.'[41] However, law enforcement and security agencies have been unable to approximate with any degree of certainty how many criminal actions, including terrorist offences, have been averted as a direct result of the use of telecommunications data which is up to two years old.[42]

64. The Law Council notes that a 2011 report from the European Commission revealed that 90 per cent of data accessed under data retention regimes in European countries was six months old or less. Around 73 per cent of data accessed was three months old or less.[43] In the joint submission from Communications Alliance and AMTA to the Committee's inquiry, it was relevantly noted that 'CSPs report that the vast majority of warrantless requests they receive from Australian agencies relate to data that is 6 months old or younger'.[44]

65. The vast majority of EU countries which have mandatory data retention schemes in place only require the data to be retained for 6 months to 1 year.[45] Only Poland appears to have a similar two-year retention period as set out in this Bill.[46] There are also currently no equivalents in the United States or the United Kingdom (other than voluntary data retention.

66. Accordingly, in the absence of any other evidence, the data retention period should be reduced to the minimal period reasonably required, in view of the experience of investigations requiring access to telecommunications data, the comparative experience in other jurisdictions and the need for proportionality and protection of privacy and evidence provided to the Committee's 2013 inquiry relating to data retention relating to the estimated cost of a 2 year mandatory data retention regime.

67. Recommendations:

[40] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 19.
[41] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 19.
[42] See Paul Farrell, ' Metadata: most Australian police forces can't say how many times it has been used to prevent crime', *The Guardian* (online), 29 December 2014<http://www.theguardian.com/world/2014/dec/29/metadata-most-australian-police-forces-cant-say-how-many-times-it-has-been-used-to-prevent?CMP=share_btn_link>.
[43] European Commission, Report from the Commission to the Council and European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM (2011) 225 Final 15.
[44] Communications Alliance/AMTA, Submission No 6 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 12 December 2014, 8.
[45] Chris Jones and Ben Hayes, 'The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy' (Project, Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness, November 2013 <http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf>) 35 – 50.
[46] See http://ec.europa.eu/archives/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf page 13-14.

- **The data retention period should be reduced to no longer than the minimal period required by law enforcement and security agencies.**

Agencies and access to data should be limited

68. To ensure the scheme is proportionate, the Law Council considers it is necessary to limit both the agencies that can access stored communications and telecommunications data and the situations in which those agencies can access such data to only address threats to national security or serious criminal activity.

69. To provide greater clarity and to limit access to stored communications in line with the Bill's intended purpose, the Law Council considers that the TIA Act should be amended to only permit ASIO and criminal law enforcement agencies involved in investigating 'serious contraventions'[47] to have access to stored communication warrants.

70. The Law Council also considers that for the regime to be consistent with its stated purpose of protecting national security, public safety and addressing crime[48] access to telecommunications data should only be granted to criminal law enforcement and security agencies that investigate specific serious crimes such as serious indictable offences or specific serious threats to national security (as defined by section 4 of the *Australian Security and Intelligence Organisation Act 1979* (Cth) – the ASIO Act). A serious indictable offence could be defined in similar terms to section 15GE of the *Crimes Act 1914* (Cth) as one that involves a range of matters (including for example espionage, sabotage or threats to national security, violence, firearms, importation and exportation of prohibited imports, theft, fraud, money laundering, harbouring criminals, forgery) and is punishable by at least three years' imprisonment.

71. The proposed scheme covers all persons using relevant electronic communications services. It applies indiscriminately including persons for whom there is no evidence of any connection with serious crime or a threat to national security. The scheme in this regard is similar to the EU Directive which the CJEU found invalid, partly on the basis of its indiscriminate application. Indeed, the proposed data set is expressly stated to be 'based closely' on the EU Data Retention Directive. While this decision was made in the context of the EU's human rights framework, it is nonetheless instructive as the Court applied the same concepts of proportionality and necessity which the Law Council considers should inform the development of legislation in the Australian context.

72. Recommendations:

The Bill should be amended so that the agencies that have access to:

- **Stored communications warrants are limited to those required to investigate 'serious contraventions' as defined in section 5E of the TIA Act;**

- **Telecommunications data are limited to those agencies required to investigate serious indictable offences (similar to section 15GE of the Crimes Act 1914) or specific threats to national security (as defined by section 4 of the ASIO Act). Access to retained data that is older than 6**

[47] As defined in section 5E of the *Telecommunications (Interception and Access) Act 1979 (Cth)*.
[48] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 10.

months should be limited to the investigation of significant threats to national security and complex criminal offences.

Independent and Ministerial warrant process necessary

73. All of the current and proposed oversight mechanisms in the TIA Act are directed at reviewing telecommunications data access powers *after* they have been exercised. For example, the following have or will have oversight of agency powers to access retained telecommunications data under the scheme:

    - IGIS – over ASIO's access to telecommunications data. While there is the potential for the IGIS to act independently to initiate inspections to monitor ASIO's access to telecommunications data under the TIA Act, there is no legislative requirement that he or she does so prior to an access request being issued.

    - Commonwealth Ombudsman – over law enforcement agencies such as the AFP, ACC and anti-corruption bodies;

    - OAIC – existing statutory obligations under the Privacy Act in relation to privacy protections and accountability standards for service providers (where covered by the Act) in relation to customers' personal information, consistent with contemporary community expectations;

    - Parliament – over both ASIO and law enforcement bodies' use of powers under the TIA Act and the Committee would be required to review the scheme three years after its commencement.[49]

74. The Law Council considers that these are necessary oversight mechanisms, but that they are not sufficient and should be enhanced by the introduction of a warrant process, which would provide prior review by a court or independent administrative body to determine the necessity of the request for the purposes of preventing or detecting serious crime.

75. A warrant is required because under the proposed data retention regime, vastly more telecommunications data will be available – both in terms of volume and potentially the quality of the data retained – than is currently the case. This change heightens the risk of an encroachment on rights of privacy.

76. There is also greater potential for a breach of confidentiality of lawyer/client, journalist/source, doctor/patient, communications in circumstances when telecommunications data can be obtained about when, where and how often a client/source/patient seeks advice.

77. It is likely the richness of available telecommunications data will also grow permitting more sophisticated and powerful searches by law enforcement and security agencies over time. Further, the technology to handle and deal with telecommunications data is different than in 1979 when the TIA Act was introduced. In the 1970s, agencies received paper bills that they had to process manually. These factors combine to make it preferable for judicial oversight of access to telecommunications data.

78. Requiring a warrant for access would more readily accord with the process required for accessing telecommunications data in a number of EU countries where law

[49] Proposed section 187N of the TIA Act.

enforcement agencies are not permitted to authorise their own access. The tables in **Attachment B** set out such EU countries and also those where law enforcement agencies may authorise their own access to telecommunications data.

79. .The benefits of a warrant-based process by an independent body include independent assessment of:

    - whether it is strictly necessary and proportionate for an enforcement agency to be authorised to have access to telecommunications data;
    - whether client legal privilege or confidentiality of journalists' sources may be adversely affected by the issue of the warrant;
    - the gravity of the conduct constituting the offence or contravention being investigated;
    - how much the information obtained under the warrant would be likely to assist the investigation by the agency of the offence/s or threat to national security;
    - the extent to which conventional methods of investigating the offence or contraventions that do not involve accessing intrusive telecommunications data have been used by, or are available to, the agency seeking the warrant;
    - the extent to which the use of such alternative methods would be likely to assist the agency's investigation; and
    - 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.[50]

80. The CJEU found that the EU Data Retention Directive was invalid, partly on the basis that it lacked any requirement of prior review by a court or independent administrative body.[51]

81. The Law Council notes that there are existing warrant processes in place for interception and access of stored communications that would be 'likely to assist' with an investigation of a serious offence.[52]. These existing processes could be extended and applied to the proposed access to retained telecommunications data for investigation of threats to national security or serious criminal activity.

82. The issue of delay can be allayed by requiring a prompt-approval process as is currently the case for emergency warrants issued under the TIA Act.[53] In an emergency, where there is a real and reasonable belief that there is a serious and immediate risk to public safety or health, access may be authorised through a non-delegable Ministerial warrant.[54] In such circumstances, the Minister should be

[50] The Law Council notes that similar factors are currently required to be considered by judges and AAT members tasked with issuing interception and access warrants.
[51] Court of Justice of the European Union *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) *and Kärntner Landesregierung* (C 594/12) [2014] ECR [62].
[52] *Telecommunications (Interception and Access) Act 1979* (Cth) s110, s116.
[53] See for example section 10 of the TIA Act.
[54] The Law Council is confident of the integrity and professionalism of our law enforcement and security agencies. However, the Law Council considers that it is not appropriate for agencies to be permitted to empower themselves to conduct intrusive activities, even in emergency situations. Imposing clear limitations on the exercise of Executive power – particularly when that power can have pronounced impacts on members of the community, which has little recourse to the criminal or civil law in respect of contraventions of such

required to consider the range of factors noted above in relation to the benefits of a warrant process. Such an exemption would also help ensure that urgent operational activity would not be unduly impeded.

83. A warrant-based system would not amount to 'a *de facto* requirement for judicial authorisation to investigate certain crimes – crimes that Parliament has already endorsed agencies to investigate'[55] as it would not prohibit an agency utilising and pursuing other methods of investigation.

84. The Law Council understands that there are concerns that a warrant-based system would limit the ability of law enforcement and national security agencies to employ what is often the lowest risk, least resource-intensive and least intrusive investigative tool.[56] The Law Council does not agree that the method of access to retained communications should be the paramount consideration. Rather, protection and oversight of rights of privacy should be paramount.

85. Without such a prior review mechanism there is no ability of an independent body to assess whether it is lawful, necessary and appropriate for an enforcement agency to be authorised to have access to telecommunications data in the particular circumstances of a case.

86. The Law Council acknowledges that a warrant-based system for access to telecommunications data would increase the number of warrant applications. However, it would serve as an important deterrent for agencies to only apply for access when an interference with privacy is considered necessary.

87. The Law Council rejects the argument that, even if accompanied by increased resourcing, a warrant regime would distort the ability of issuing authorities to perform their day-to-day functions as members of the judiciary or AAT.[57] This is an issue of adequate resourcing of the Courts and the AAT. The government has a responsibility to sufficiently resource those bodies charged with supervision of such activities to ensure that rights of privacy are not unnecessarily infringed upon.

88. **Recommendations:**

- **Access to retained telecommunications data should be authorised by an independent tribunal.**

- **In an emergency, where there is a real and reasonable belief that there is a serious and immediate risk to public safety or health, access may be authorised through a non-delegable Ministerial warrant. In such circumstances, the Minister should be required to consider a range of factors set down in the legislation.**

power – is a key component of the rule of law and reflected in the Law Council's Rule of Law Principles – Law Council of Australia, *Policy Statement: Rule of Law Principles*, March 2011.

[55] Attorney-General's Department, Submission No 26 to the Senate Legal and Constitutional Affairs Reference Committee, *Inquiry into a Comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, 22.

[56] Ibid.

[57] Ibid.

Availability of retained telecommunications data for civil and non-law enforcement purposes

89. The Bill does not limit in any way disclosures of data required to be retained where those disclosures are mandated by laws other than the Bill. The *Privacy Act 1988* (Cth) exempts certain disclosures in permitted general situations as described in section 16A of that Act, including if that disclosure is 'reasonably necessary for the establishment, exercise or defence of a legal or equitable claim'.

90. Disclosure is also permitted where the disclosure 'is required or authorised by or under Australian law or a court/tribunal order' (APP 6.2(b)).

91. A variety of Federal, State and Territory Acts empower particular agencies to compel disclosure. For example, section 29 of the *Crime Commission Act 2012* (NSW) provides that an executive officer with special legal qualifications may, by notice in writing served on a person require the person to appear before the Commission at a particular time and place and produce to that officer a document or thing specified in the notice, being a document or thing that is relevant to an investigation.

92. Subpoenas are frequently already issued to third parties by courts, including ISPs, to produce records. Further, parties to prospective or current litigation might seek such retained data as part of the discovery.

93. In the absence of any restriction upon access to telecommunications data under other Federal, State or Territory laws or court process requiring disclosure of information or documents, there are obvious concerns about the privacy and security of telecommunications data held by authorised collecting agencies. Significant risks include attempting to determine journalists' sources, cases involving alleged infringement of online copyright, family law proceedings, civil claims involving use of machinery or motor vehicles, class actions or other legal proceedings.

94. The Law Council recommends that access authorised by other Federal, State, or Territory laws, or pursuant to court process should be precluded to ensure that the impact of the Bill is clear and limited to achieving its stated purpose.

Individual access exception

95. An exception should be provided for individuals seeking to access their own telecommunications data. This may be essential, for example, in a criminal trial where an individual believes that telecommunications data may establish their innocence. If government agencies are able to access the telecommunications data of individuals to establish a prosecution, the Law Council considers that it is also appropriate for individual's to access such data to be able to establish a defence, or to understand the evidence and charges against them.

96. Recommendations:

- **The Bill should be amended to preclude access to retained telecommunications data under other Federal, State, or Territory laws, or pursuant to court process.**
- **An exception should be provided for individuals seeking to access their own telecommunications data.**

Client legal privilege and confidentiality

97. Client legal privilege is a right for a client of a lawyer not to have their communications associated with legal advice or impending litigation disclosed without their consent. The benefit is for the client, not the lawyer. The Law Council regards client legal privilege as a fundamental civil right and a pillar of the Australian legal system. It ensures full and frank discussions between legal advisers and their clients, which promotes the administration of justice and encourages compliance with the law.[58]

98. The Law Council's Client Legal Privilege Committee has noted that although telecommunications data alone may not reveal the content or substance of lawyer/client communications, it would, at the very least, be able to provide an indication of whether:

    - a lawyer has been contacted;
    - the identity and location of the lawyer;
    - the identity and location of witnesses;
    - the number of communications and type of communications between a lawyer and a client, witnesses and the duration of these communications.

99. The Law Council notes that client legal privilege does not attach to legal advice which furthers the commission of a crime.[59] Therefore, it may be possible to respect client legal privilege and permit investigations. The issue involves one of determining the purpose of obtaining the information. That is, if the purpose is to prevent the commission of an offence which is about to occur, then client legal privilege will not attach to such a communication. If information is sought to investigate an offence already committed, then client legal privilege may apply. The Law Council also notes that the TIA Act does not expressly or impliedly abrogate the right to claim client legal privilege.[60]

100. Accordingly, where access to retained data is sought relating to a lawyer's communications, it is essential that agencies seeking access demonstrate how privileged and confidential communications will be protected before a warrant can be issued and that sanctions for non-compliance be included.

101. The scheme's application to other relationships whose communications are subject to the obligation of professional confidentiality, such as the communications of a journalist and source, a doctor and patient, a priest and penitent, or communications relating to public interest immunity needs to be reconsidered. These relationships invariably involve a public interest in maintaining confidentiality not only for the content of communications but for information about the communication. We have seen

[58] Law Council Submission to the Australian Law Reform Commission, *Inquiry into Client Legal Privilege and Federal Investigatory Bodies*, November 2007, 5, 9.
[59] *AWB Limited v Honourable Terence Rhoderic Hudson Cole* (No 5) [2006] FCA 1234 at [210]-[212], [229]; *Commissioner of Australian Federal Police v Propend Finance Pty Ltd* (1997) 188 CLR 501, per Brennan CJ at [514], Dawson J at [522], Gaudron J at [545] and Gummow J at [564]; *Carter v Northmore Hale Davy & Leake (1995)* 183 CLR 121 at [163] per McHugh J.
[60] Under the common law, the right to claim client legal privilege will only be taken to be abrogated if the legislation clearly indicates: *Daniels Corp International Pty Ltd v Australian Competition and Consumer Commn* (2002) 213 CLR 543; *Valantine v Technical and Further Education Commn* (2007) 97 ALD 447 at 454.

instances where access to telecommunications data has led to the disclosure of the identity of a journalist's source in the United Kingdom.[61]

102. It has recently been reported that the UK government will reform the *Regulation of Investigatory Powers Act 2000* (UK) to require a judicial warrant for access to journalistic telecommunications data in the wake of growing concern at the misuse of powers to discover journalistic sources.[62]

103. Advance notice would afford lawyers an opportunity to claim client legal privilege on certain communications where relevant and allow an opportunity for review of any warrant issued, and provide a similar opportunity with respect to protection of journalists' sources.

104. The Law Council considers that there should be a legislative presumption that will ensure notice to lawyers and journalists in all but the most exceptional cases. That is, the presumption of advance notice should be overcome only if it would pose a clear and substantial threat to the investigation, risk grave harm to national security, or present an imminent risk to public safety or health. The possibility that notice, and potential judicial review, may delay the investigation should not, on its own, be considered a compelling reason to overcome the presumption.

105. In the United States, the Department of Justice also considered that a presumption regarding advance notice to news media should apply whenever access to their records related to newsgathering activities is sought, in all but the most exceptional cases, along the lines suggested above.[63]

106. The Law Council considers that the legislation should include provisions to:

- require an agency seeking access to retained data to consider the prospect of the data revealing confidential or privileged communications and in those circumstances, to provide advance notice of any intended access and/or to apply for a warrant before accessing the data; and

- prohibit the use of any data obtained without a warrant – even inadvertently – that breaches confidentiality or privilege.

Recommendation:

- **Where access to retained data is sought for persons with legal obligations of professional confidentiality, there should be a requirement for agencies seeking access to demonstrate how privileged and confidential communications will be protected before a warrant can be issued.**

- **The TIA Act should include a legislative presumption that will ensure notice to lawyers and journalists in all but the most exceptional cases where access to retained telecommunications data is sought.**

[61] Lisa O'Carroll, 'MPs to investigate police use of RIPA powers to snoop on journalists' *The Guardian* (online) 6 October 2014 http://www.theguardian.com/uk-news/2014/oct/05/mps-police-ripa-powers-snoop-journalists.
[62] Patrick Wintour, 'British police's use of RIPA powers to snoop on journalists to be reined in', *The Guardian* (online) 12 October 2014 <http://www.theguardian.com/world/2014/oct/12/police-ripa-powers-journalists-surveillance>.
[63] Department of Justice, 'Report on Review of News Media Policies', (12 July 2013), 2 <www.justice.gov/iso/opa/resources/2202013712162851796893.pdf>.

Security of retained data

107. Security of retained data is proposed to be dealt with through the Telecommunications Sector Security Reforms (TSSR)[64] combined with the Privacy Act, and the Bill's proposed changes to the Telecommunications Act to implement remedial directions, formal warnings and pecuniary penalties. However, the Law Council is concerned that there does not appear to be a minimum set of standards for government agencies and service providers to ensure security of retained telecommunications data.

108. Recent experience with the AFP mistakenly publishing sensitive information, including telecommunications data, connected to criminal investigations demonstrates the importance of high levels of data security.[65]

109. The Explanatory Memorandum to the Bill also notes that the implementation plan process is partly intended to 'allow service providers to develop and implement more cost-effective solutions to their data retention obligations'.[66] This could encourage telecommunications service providers to seek the lowest cost solutions, provided that they comply with the TSSR, the Australian Privacy Principles (APPs) and their data retention obligations under the TIA Act. For example, offshore cloud or server storage would appear to be permitted.

110. The Law Council notes that CJEU held the EU Data Directive invalid partly on the basis that it permitted providers to have regard to economic considerations when determining the level of security which they applied and did not require the telecommunications data to be retained within the EU.[67]

111. The Law Council considers that minimum standards of security of retained data should be developed before the legislation is implemented.

112. Entities subject to mandatory data retention requirements under the Bill should be required to demonstrate to ACMA that they have met minimum standards for ensuring the security of retained data.

113. Recommendations:

- **Government agencies that have access to telecommunications data should develop minimum standards and put them forward for consideration and approval of the Committee.**
- **Entities subject to mandatory data retention requirements under the Bill should be required to demonstrate to ACMA that they have met minimum standards for ensuring the security of retained data.**
- **ACMA should develop these minimum standards for approval of the Committee.**

[64] The Telecommunications and Other Legislation Amendment Bill 2014 seeks to implement the TSSR.
[65] Mandie Sami, 'AFP accidentally publish secret, sensitive information' *ABC* (online) 28 August 2014 <http://www.abc.net.au/pm/content/2014/s4076431.htm>.
[66] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 35.
[67] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) *and Kärntner Landesregierung* (C 594/12) [2014] ECR [67] - [68].

Destruction of telecommunications data

114. The Law Council notes that the CJEU found the EU Data Directive invalid partly on the basis that there was a lack of a requirement to ensure the irreversible destruction of the data at the end of the data retention period.[68]

115. In the Law Council's view, it is essential that when the telecommunications data is no longer required, it is de-identified or put beyond use in a timely manner to avoid malicious or inadvertent publication of personal information.

Law enforcement and security agency destruction of telecommunications data

116. The TIA Act includes a number of obligations requiring that information obtained under an interception or stored communication warrant be destroyed.[69] Section 31 of the ASIO Act also requires that certain records obtained under a warrant be destroyed where the Director-General is satisfied that the record or copy is not required for the purposes of ASIO's functions and powers.[70]

117. Chapter 4 of the TIA Act does not require enforcement agencies to destroy in a timely manner telecommunications data containing personal information which is irrelevant to the agency or no longer needed

118. The Law Council strongly supports the inclusion of provisions which establish positive obligations of this kind.

Service provider destruction of telecommunications data

119. Proposed subsection 187C(3) of the Bill notes that a service provider is not prevented from keeping information or a document for a period that is longer than the two year data retention period.

120. The APPs, as set out in Schedule 1 of the Privacy Act, will apply to service providers and their dealings with telecommunications data that is personal information and that is required to be retained under new Part 5-1A of the TIA Act.

121. A service provider that holds personal information, must take steps that are reasonable in the circumstances to protect the information from misuse, interference and loss; and unauthorised access, modification or disclosure (APP 11.1). The service provider must also take such steps as are reasonable in the circumstances to destroy the information and ensure that the information is de-identified if it constitutes personal information and the provider no longer needs it for any purpose under the Privacy Act, or any other Australian law, or a court/tribunal order (APP 11.2).

122. The Explanatory Memorandum to the Bill also notes that the proposed TSSR[71] will, in combination, require service providers to do their best to prevent unauthorised access to and unauthorised interference with retained telecommunications data.

[68] Ibid [67].
[69] See for example sections 14, 31C, 79, 150 of the TIA Act.
[70] Although the Law Council notes that it does not positively require the Director-General to turn his or her mind to whether a record or copy is required.
[71] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 13. The Telecommunications and Other Legislation Amendment Bill 2014 involves introducing a new obligation on C/CSPs to do their best to prevent unauthorised access and unauthorised interference to telecommunications networks and facilities, including where a C/CSP outsources functions.

123. The Law Council considers that the views of the OAIC should be obtained to determine whether the current APPs and the proposed TSSR relating to service providers destruction of telecommunications data is sufficient to safeguard personal information.

124. Recommendations:

- **The Bill should be amended to require law enforcement and security agencies to de-identify or put beyond use in a timely manner telecommunications data containing personal information which is irrelevant to the agency or no longer needed by the agency.**

- **The views of the OAIC should be obtained to determine whether the current APPs and the proposed TSSR relating to destruction of telecommunications data by service providers is sufficient to safeguard personal information, given the very large amount of telecommunications data to be retained.**

Disclosure of telecommunications data

125. The Law Council notes that sections 181A, 181, 181B and 182 of the TIA Act contain offences for unlawful dealing in telecommunications data authorisation information or unlawful secondary disclosure of accessed telecommunications data under Chapter 4, Part 4-1, Division 6 of the TIA Act. As noted in the Explanatory Memorandum to the Bill, the purpose of such provisions is to 'protect the privacy of impact on persons whose information was accessed under the TIA Act'.[72]

126. The Law Council considers it is vital that the disclosure regime in the TIA Act be strengthened if the Bill is to be progressed.[73]

127. The TIA Act allows agencies to authorise the disclosure of information for a purpose unrelated to the purpose for which it was originally granted access.[74] The effect on privacy should be considered in a privacy impact assessment.

Subsequent Disclosure

128. The Bill should include a presumption against subsequent disclosure of information to another agency such as the Australian Taxation Office, Australian Securities and Investments Commission, Australian Competition and Consumer Commission or other regulatory body. This presumption should only be rebutted by express legislative intention to enable an agency to address a serious threat to national security or a serious offence.

[72] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 89.

[73] In a submission to the Senate Legal and Constitutional Affairs Committee regarding its Comprehensive Review of the TIA Act (February 2014), the Law Council previously noted that there is insufficient guidance about when voluntary disclosure is permitted by service providers. The Law Council also raised concerns over agencies being permitted to authorise disclosures for purposes unrelated to their functions.

[74] 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: when it is reasonably necessary for the enforcement of the criminal law; when it is reasonably necessary for the enforcement of a law imposing a pecuniary penalty; and when it is reasonably necessary for the protection of the public revenue. Under the information sharing provisions in the TIA Act and the *Australian Security Intelligence Organisation Act 1979* (section 18), the Australian Secret Intelligence Service may receive information obtained by ASIO under the TIA Act if it is relevant to ASIS's functions.

Voluntary disclosure

129. The Law Council considers that the voluntary disclosure provisions in Chapter 4 of the TIA Act should be repealed.[75] As noted, all information should only be accessed via a judicial or Ministerial warrant. There is a clear inconsistency between a mandatory telecommunications data retention regime, which permits only certain agencies to access data, running parallel to a voluntary disclosure regime.

130. The Law Council believes that prohibiting voluntary disclosure may reduce the risk that personal information will be disclosed for an unauthorised purpose. Accordingly, section 313 of the Telecommunications Act should be amended to make clear that voluntary disclosure is not permitted.[76]

131. Recommendations:

- **The Bill should preclude voluntary disclosure of telecommunications data. All information should only be accessed via a judicial or Ministerial warrant, as outlined above.**
- **Section 313 of the Telecommunications Act should be amended to make clear that voluntary disclosure is not permitted.**
- **The Bill should include a presumption against subsequent disclosure of information to another agency. This presumption should only be rebutted by express legislation to enable an agency to address a serious threat to national security or a serious offence.**

Privacy Impact Assessment

132. The Law Council considers that a PIA of the scheme should be conducted by the OAIC before the Bill is implemented. The PIA should provide a systematic assessment of the Bill before it is enacted that identifies the impact that the scheme might have on the privacy of individuals, and set out recommendations for managing, minimising or eliminating that impact. PIAs are an important tool for assessing privacy risks and developing mitigation strategies. The PIA should form part of the ordinary Regulation Impact Assessment process recommended by the Office of Best Practice Regulation. The PIA should also deal with the possibility of 'function or scope-creep' as a specific privacy risk that the legislation needs to address.

133. **Recommendation:**

- **The Committee should request the OAIC to conduct a privacy impact assessment (PIA) of the scheme to the extent that the information is personal information as defined by the *Privacy Act 1988* (Cth) dealing specifically with the possibility of 'function or scope-creep'.**

[75] Chapter 4 of the TIA Act provides that 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 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 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)).

[76] Section 313 of the Telecommunications Act requires carriers and CSPs to give Commonwealth, State and Territory authorities "such help as is reasonably necessary" for purposes including enforcing the criminal law'..

Notification of access – freedom of expression and the right to an effective remedy

134. The Law Council notes that under the proposed data retention scheme telecommunications data would be retained and could subsequently be used without the user or individual ever being informed.

135. The Parliamentary Joint Committee on Human Rights has stated that this may have a 'chilling' effect on people's freedom and willingness to communicate via telecommunications services because retention and undisclosed use of telecommunications data could lead people to 'self-censor' their views expressed via telecommunication services.[77]

136. The Law Council recommends the Bill be amended to require agencies accessing communications data of an individual under a judicial warrant to notify that individual (unless the judicial officer issuing the warrant is satisfied that such notification would seriously prejudice an investigation into a serious crime). This would allow an individual to be aware of matters affecting their privacy and permit the opportunity for an individual to challenge the lawfulness of the warrant in accordance with the rights to an effective remedy.[78]

137. Recommendation:

- **The Bill should require agencies accessing communications data of an individual under a judicial warrant to take all reasonable steps to notify that individual (unless the judicial officer issuing the warrant is satisfied that such notification would seriously prejudice an investigation into a serious crime). This should be part of the warrant application process.**

Commonwealth Ombudsman oversight arrangements

138. The Law Council welcomes the proposed establishment of Commonwealth Ombudsman oversight of law enforcement agencies' use of powers under the TIA Act.

139. The Law Council notes that the Bill would lead to an increased role for the Commonwealth Ombudsman. Accordingly, additional resources may be required by the Commonwealth Ombudsman's Office for it to continue performing its existing and new roles under the mandatory telecommunications data scheme effectively.

[77] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report of the 44th Parliament*, (2014) [1.70]-[171]. The right to freedom of opinion and expressions is protected by article 19 of the International Covenant on Civil and Political Rights. The right to freedom of opinion is the right to hold opinions without interference and cannot be subject to any exception or restriction. The right to freedom of expression extends to the communication of information or ideas through any medium, including written and oral communications, the media, public protest, broadcasting, artistic works and commercial advertising. Under article 19(3) it may be subject to limitations that are necessary to protect the rights or reputations of others, national security, public order, or public health or morals. Limitations must be prescribed by law, pursue a legitimate objective, be rationally connected to the achievement of that objective and a proportionate means of doing so. See Human Rights Committee, *General Comment No 34 (Article 19: Freedoms of opinion and expression*), CCPR/C/GC/34, (2011) [21]-[36].

[78] Article 2 of the *International Covenant on Civil and Political Rights* requires Australia to ensure access to an effective remedy for violations of human rights. States parties are required to establish appropriate judicial and administrative mechanisms for addressing claims of human rights violations under domestic law.

140. The Law Council also notes that there is an abrogation of privilege against self-incrimination for the proposed criminal offences seeking to ensure compliance with the oversight regime. Generally the Law Council is concerned by the abrogation of existing rights, however abrogation or limitation may be appropriate where exercise of the privilege could seriously undermine the effectiveness of the oversight scheme and prevent collection of evidence. It is also important that the safeguard of use and derivative use immunity applies, which provides some degree of protection for the rights of individuals.

141. There appears to be a typographical error in the Explanatory Memorandum to the Bill at [103]. The second dot point should include a reference to proposed subsection 87(6) rather than '187(6)'.

142. **Recommendation:**

- **The Commonwealth Ombudsman should be given adequate resources to investigate breaches.**

IGIS oversight arrangements

143. As noted above, the Office of the IGIS oversees ASIO's use of TIA powers under the inspection function in the IGIS Act.[79] This includes the power to review warrantless surveillance requests for telecommunications data. The IGIS also has functions in relation to preservation notices given by ASIO.[80]

144. While the Bill seeks to establish an effective obligation of law enforcement agencies to keep records in relation to preservation notices, stored communications and telecommunications data, it does not similarly amend the TIA Act to provide for more effective oversight of ASIO's activities by the IGIS.

145. This diminishes the effectiveness of the oversight mechanism. Clear obligations for ASIO to keep records would allow the IGIS to more effectively determine whether ASIO has used these powers lawfully.

146. Clear record keeping obligations would also increase the IGIS's accountability and provide transparency of the Office's methodologies and activities.

147. Recommendations:

- **ASIO's record keeping procedures in relation to preservation notices, stored communications and telecommunications data, should be brought into line with other enforcement agencies under proposed sections 151 and 186A of the TIA Act; and**

- **IGIS should be required to inspect those records annually in similar terms to proposed subsection 186B(1) of the TIA Act.**

[79] *Inspector-General of Intelligence and Security Act 1986* (Cth) s9A.
[80] TIA Act s158A.

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 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 23 Directors – one from each of the constituent bodies and six elected Executive members. 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 members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2015 Executive are:

- Mr Duncan McConnel, President
- Mr Stuart Clark President-Elect
- Ms Fiona McLeod SC, Treasurer
- Dr Christopher Kendall, Executive Member
- Mr Morry Bailes, Executive Member
- Mr Ian Brown, Executive Member

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

Attachment B: Access to communications data within the EU[81]

The following EU countries require independent oversight to enable government agencies to have access to telecommunications data.

Member State	Role of person authorising access
Belgium	Authorised by magistrate or prosecutor
Bulgaria	Chair person of regional court
Cyprus	Public prosecutor or judge
Denmark	Magistrate/judge
Estonia	Preliminary investigation judge
Finland	Subscriber data may be accessed by all competent authorities without judicial authorisation. Judge's authority for traffic data
France	Senior official in Ministry of Interior
Greece	Member of judiciary
Hungary	Public prosecutor
Italy	Public prosecutor
Lithuania	For access for pre-trial investigations, a member of the judiciary
Luxembourg	Member of the judiciary
Netherlands	Public prosecutor or investigating judge
Portugal	Transmission of data requires judicial authorisation
Romania	Accredited service provider
Slovenia	Member of judiciary

[81] The information provided in this table is a condensed version of tables from (a) a 2011 report by the European Commission which undertook an evaluation of the Data Retention Directive and reported their findings to the European Council and European Parliament – see http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf ; and (b) the Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, 2013 – this project was co-funded by the European Union – see http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf.

Spain	Member of judiciary

The following EU countries permit government agencies to authorise their own access to telecommunications data.

Member State	**Role of person authorising access**
Ireland	No formal authorisation. Requests to be in writing. 'Service provider'
Latvia	'Electronic communications merchant'
Malta	Malta Police Force; Security Service officials ('controller')
Poland	Senior officials of the police, border guards, tax inspectors
Slovakia	Senior official ('controller') of a state administration authority, territorial self-government authority, other public authority body or legal or natural person
UK	'Designated person': individuals holding such offices, ranks or positions with relevant public authorities as are prescribed for the purposes of this legislation by an order made by the Secretary of State