Law Council
OF AUSTRALIA

Access to telecommunications data in civil proceedings

Attorney-General's Department

24 January 2017

Telephone +61 2 6246 3788 •*Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About 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 Law Firms Australia, 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
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 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 2017 Executive as at 1 January 2017 are:

- Ms Fiona McLeod SC, President
- Mr MorryBailes, President-Elect
- Mr Arthur Moses SC, Treasurer
- Ms Pauline Wright, Executive Member
- Mr Konrad de Kerloy, Executive Member
- Mr Geoff Bowyer, Executive Member

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

Acknowledgement

The Law Council acknowledges the assistance of the Media and Communications Law Committee of the Business Law Section, the Privacy Law Committee of the Business Law Section, the National Criminal Law Committee, the National Human Rights Committee, the Family Law Section, the Domestic and Family Violence Taskforce, the Law Society of South Australia (**LSSA**), the Law Institute of Victoria (**LIV**) and Queensland Law Society (**QLS**) in the preparation of this submission.

Executive Summary

1. The Law Council of Australia is grateful for the opportunity to provide comments to the Attorney-General's Department's Inquiry into *Access to Telecommunications Data in Civil Proceedings*.

2. The purpose of the current Inquiry is to determine whether regulations should be made pursuant to section 280 of the *Telecommunications Act 1997* (Cth) (**the Telecommunications Act**) to allow access to telecommunications data retained *solely* for the purposes of the mandatory data retention scheme in civil proceedings.

3. The mandatory data retention scheme must be necessary and proportionate and not unduly impinge on the values and freedoms on which our democracy is founded. It is intrusive of privacy as it requires relevant service providers to collect and retain telecommunications data on every customer in case it might be needed for law enforcement purposes.[1] Mandatory data retention schemes with lesser scope of coverage and shorter retention periods than the Australian scheme have been ruled as unlawful in other comparable jurisdictions on the basis that they are a disproportionate and unwarranted intrusion.[2]

4. The Consultation Paper appears to be designed to solicit suggestions as to a wide range of unspecified possible exceptions to the current section 280 Telecommunications Act. Specification of exceptions would have the effect of expanding the circumstances in which access to telecommunications data retained solely for the purposes of the mandatory data retention regime would be permitted. No specific proposals for exceptions are proposed in the Consultation Paper despite the vast array of possible civil proceedings that might be considered.

5. Detail is required in order for non-government organisations to comment usefully on whether there are particular kinds of civil proceedings and circumstances that would warrant proportionate exceptions. Detail is also needed to demonstrate where a need for expansion, whether operational or otherwise, has been identified. This is particularly so in light of civil litigants already having the ability to access a broad range of telecommunications data where it is retained by relevant telecommunications service providers for a range of purposes, including business and regulatory purposes.

6. Further, the Consultation Paper does not address the broader impact to the community of any expansion of the mandatory data retention scheme in civil proceedings, including in relation to the right to privacy, constitutional considerations, oversight and risk of data insecurity. These impacts – currently not addressed in the Consultation Paper – must also be carefully considered.

7. While expanding availability of telecommunications data for certain civil proceedings such as recovery of proceeds of crime and child abduction may appear worthy goals,

---

[1] See, UN General Assembly Resolution, Right to privacy in the digital age http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167; see also, Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/27/37 (30 June 2014)http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[2] See, e.g. Cases C-203/15 and C-698/15 *Tele2Sverige AB v Post-och telestyrelsen;Secretary of State for the Home Department v Watson & Ors* (European Court of Justice, 21 December 2016).

this must be balanced with the right to privacy, risk of data insecurity and secondary use, and misuse by parties themselves to litigation. Access to telecommunications data held solely for the purpose of the mandatory data retention regime must be governed by robust legislative protections to ensure access is only permitted when the public interest in access outweighs the public interest in ensuring Australians can conduct their lives free from tracking and surveillance.

8. In the absence of specific proposals to demonstrate a need for regulations relating to civil proceedings, the Law Council's preliminary view is to support the recommendation of the Parliamentary Joint Committee on Intelligence and Security (**the PJCIS**) *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, namely that civil litigants generally be prohibited from being able to access telecommunications data held by a service provider *solely* for the purpose of complying with the mandatory data retention regime.[3]

9. The PJCIS considered that as the data retention regime was established specifically for law enforcement and national security purposes, as a general principle it would be inappropriate for data retained under the scheme to be drawn on as a new source of evidence in civil disputes.[4]

10. As a general principle, the Law Council agrees with this assessment. Australia's mandatory data retention legislation is an extraordinary measure enacted by the Australian Parliament to ensure the security of Australia and its people. It was enacted to achieve the objective of addressing and preventing serious crime and terrorism. The two year retention period required under the scheme[5] is unusually long by international standards.[6]

11. The impact upon Australians of this significantly increased level of surveillance and prospective tracking was considered by the Parliament as proportionate to achieve the objective of addressing and preventing serious crime and terrorism: it is an entirely different matter, and in our submission disproportionate, to extend the impact of that tacking and surveillance to an indeterminate range of civil proceedings. Further, the impact of any expansion in civil access to telecommunications data will expand as the range of new devices connected to the internet dramatically increases with take-up of the internet of things, particularly the smart home. Smart thermostats, smart appliances, Internet Protocol/Wi-Fi cameras, smart locks, smart home systems, and smart switches and outlets will enable activity within the home to be retrospectively reviewed and analysed at any time. Telsyte predicts that a number of factors will drive market growth including arrival of new products and services and building of Internet connectivity into many existing products and services. Telsyte estimates that by 2019, the average household will have 24 Internet-connected devices, up from nine in 2015.[7] The adverse privacy impact of the telecommunications data retention requirements

---

[3] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,* Recommendation 23,224.
[4] Ibid [6.115].
[5] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187C(1).
[6] See, e.g. Attorney-General's Department, *Submission Parliamentary Joint Committee on Intelligence and Security Inquiry into the Telecommunications (interception and Access) Amendment (Data Retention) Bill 2014*, Appendix 1.
[7] Telesyte, Australia set for IoT@Home Spending Spree as Connected Devices Market Grows to $4 billion by 2020, (September 2016), available at https://www.telsyte.com.au/announcements/2016/9/1/australia-set-for-iothome-spending-spree-as-connected-devices-market-grows-to-4-billion-by-2020.

will therefore substantially increase within the already foreseeable next few years. Telecommunications data is no longer principally about human-to-human communication: it is now principally individuals using the internet in their private sphere of activities, and with the internet of things will increasingly be an open window into activities of individuals within both public and private spaces.

12. The impact on privacy of the data retention scheme should therefore be assessed in light of the already foreseen proliferation of new technologies and any pending introduction of mandatory breach reporting as it relates to personal information. It is reasonable to assume that the next ten years will see further expansion in the many new ways of monitoring individuals through advanced personal communications devices and other new technologies. Any expansion of the mandatory data retention regime to civil proceedings should be assessed applying that expectation and the related regulatory obligations.

Recommendations

13. Key recommendations of this submission include that prior to the making of regulations under section 280 of the Telecommunications Act:

    - The Attorney-General's Department should release a further Consultation Paper, which clearly:
        - outlines the relevant privacy issues and risks, risk of data insecurity and unauthorised secondary use, and misuse by parties themselves to litigation that might be engaged by the expansion of the mandatory data retention regime to civil proceedings;
        - includes an express and detailed discussion of any specific proposals, to allow a proper assessment of the privacy and security impacts to be made and balanced with other interests and rights in a manner that is proportionate;
        - outlines any relevant constitutional risks that might be engaged by not expanding or expanding the mandatory data retention regime to civil proceedings;
        - outlines and explains the circumstances where parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**the TIA Act**);
        - clearly discusses the basis of the Consultation Paper's second question and describes the possible impact on civil proceedings;
        - outlines specific proposals where it considers that there might be a need to create particular civil proceedings exceptions to section 280 of the Telecommunications Act; and
        - examines options for oversight mechanisms and public reporting obligations for any expansion of the mandatory data retention regime.
    - The public and the Office of the Australian Information Commissioner (**OAIC**) should be consulted on the privacy impact including risks of enabling parties to civil proceedings to access the telecommunications data set as outlined in section 187AA where information or a document is kept by a service provider solely for the purpose of complying with the mandatory data retention obligation. The OAIC's advice should be represented in the additional Consultation Paper and made available for further public consultation.
    - Any expansion of the mandatory data retention regime to civil proceedings should be the subject of assessment in a regulation impact statement or an independent cost benefit analysis.

- Any exceptions to the prohibition in subsection 280(1B) of the Telecommunications Act must be considered in light of Australia's international human rights obligations, including the right to privacy.

- Subsequent to the release of a further Consultation Paper, exposure draft regulations should be released for comment.

- The Commonwealth Ombudsman, Privacy Commissioner and Inspector-General of Intelligence and Security should be consulted on any proposals. They should also be adequately resourced to perform their important oversight functions under the mandatory data retention legislation.

Broader impact of expanding mandatory data retention

14. While expanding the regime for certain civil purposes such as proceeds of crime and child abduction proceedings may appear worthy goals, this must be fairly balanced with the right to privacy, risk of data insecurity and secondary use, and misuse by parties themselves to litigation. Access to telecommunications data held solely for the purpose of the mandatory data retention regime must be governed by a robust legislative regime to ensure access is only permitted when the public interest in access outweighs the public interest in ensuring Australians can conduct their lives free from tracking and surveillance.

15. The particularly lengthy mandatory data retention period and the ability to expand the regime by Ministerial discretion may bring into doubt the proportionality of the regime. Nonetheless, it was designed seeking to ensure the proportionality of the scheme to protect the privacy of individuals and the interests of law enforcement and security agencies in protecting the nation.

16. This was consistent with the objects of the *Privacy Act 1988* (Cth) (**the Privacy Act**), which seek to promote the privacy of individuals including by recognising that the protection of the privacy of individuals must be balanced with the interests of entities in carrying out their functions and activities.[8]

17. These objectives are also consistent with Article 17 of the *International Covenant on Civil and Political Rights* (**ICCPR**),[9] which provides that no-one shall be subjected to arbitrary or unlawful interference with their individual privacy, family, correspondence or home. This right may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary they must seek to achieve a legitimate objective and be reasonable, necessary and proportionate to achieving that objective.[10]

18. The mandatory data retention scheme requires service providers to collect and retain a large volume of personal information for two years and this has the potential to significantly impact on the privacy of individuals.[11] Telecommunications data (that is, information about an individual's communications), such as the time, location and recipient of those communications, has the potential to be used to create a detailed picture of the individual's personal life.[12]

19. For example, the impact of access to telecommunications data by an alleged domestic violence perpetrator in a family law matter needs to be carefully considered. Access might allow greater opportunities to follow, track and stalk victims.

---

[8] *Privacy Act 1988* (Cth) ss 29 and 2A.
[9] Opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
[10] See, e.g. Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014), 23.
[11] Office of the Australian Information Commissioner, *Submission on the Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, (January 2015),9.
[12] Ibid 19.

20. From analysing the data, it is possible to work out where a victim lives, works frequently visits, where they may have sought help, who they might be in contact with, when they are likely to be at home and where they may have sought refuge.

21. In a 2014 submission to the PJCIS, the OAIC explained that:

> *… even where the telecommunications data that service providers are required to collect and retain is not the content or substance of communications, it can still reveal detailed information about an individual and be highly privacy intrusive.*[13]

22. The Law Council commends the OAIC submission to the Attorney-General's Department as it clearly outlines the privacy impacts of collecting, retaining and analysing non-content telecommunications data, including location data associated with Short Message Service messages.

23. The Privacy Act defines personal information broadly, to include any information about an identified individual or an individual who is reasonably identifiable.[14] Whether an individual is reasonably identifiable from particular information depends on, among other things, what other information is held about the individual. This means that telecommunications data about an individual from which an individual is reasonably identifiable is considered personal information for the purposes of the Privacy Act.[15]

24. Organisations within the meaning of the Privacy Act are required to comply with the Australian Privacy Principles (**APPs**) when handling personal information that they collect and retain. This includes personal information collected and retained in compliance with the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (**the Data Retention Act**) by service providers covered by the Privacy Act.

25. Any further exceptions to section 280 of the Telecommunications Act would engage the right to privacy by allowing potentially greater access to personal information for the purposes of the Privacy Act.

26. Accordingly, the broader impact on the Australian community from any expansion of the mandatory data retention regime to civil proceedings should be at the forefront of the Attorney-General's Department's current inquiry.

27. Issues relating to privacy, risk of data insecurity and unauthorised secondary use, and misuse by parties to litigation are currently absent from the Consultation Paper. The document does not ask, for example, what impact there would be on fundamental rights and freedoms if parties to civil proceedings were able to access the telecommunications data retained solely for the purpose of complying with the mandatory data retention obligation.

28. Given the privacy intrusive nature of the mandatory data retention scheme, this question is essential in determining whether access by civil litigants to telecommunications data should be limited to protect the public interest in confining

---

[13] Ibid 12.
[14] *Privacy Act 1988* (Cth) s 6. See further *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 per Kenny and Edelman JJ.
[15] Ibid s 187LA.

the use, disclosure of and access to, telecommunications data, to protect the broader interests of the community.

29. To this end, the Law Council's makes the following recommendations.

Recommendation

- **Prior to the making of regulations under section 280 of the Telecommunications Act:**
    - **The Attorney-General's Department should release a further Consultation Paper, which clearly outlines the relevant privacy issues and risks, risk of data insecurity and unauthorised secondary use, and misuse by parties themselves to litigation that might be engaged by the expansion of the mandatory data retention regime to civil proceedings. The further Consultation Paper should include an express and detailed discussion of any specific proposals to allow a proper assessment of the privacy and security impacts to be made and balanced with other interests and rights in a manner that is proportionate.**
    - **The public and the OAIC should be consulted on the privacy impact including risks of enabling parties to civil proceedings to access the telecommunications data set as outlined in section 187AA where information or a document is kept by a service provider solely for the purpose of complying with the mandatory data retention obligation. The OAIC's advice should be represented in the additional Consultation Paper and made available for further public consultation.**
    - **Subsequent to the release of a further Consultation Paper, exposure draft regulations should be released for comment.**

Constitutional considerations

30. The Law Council also recommends that a further Consultation Paper outline the possible constitutional risks that may arise relating to the separation of powers by limiting the scope of judicial discretion to obtain the information necessary to assist the court in exercising its judicial function. For example, the current prohibition may be seen to limit the circumstances in which a court can issue a subpoena. It is important that the inquiry also addresses any possible constitutional impacts of proposed exceptions.

31. It should also be noted, however, that it is not unusual for the Commonwealth Parliament to create laws that govern court processes in Australian courts (for example, the *Evidence Act 1995* (Cth)).

Recommendation:

- **The Attorney-General's Department should release a further Consultation Paper, which clearly outlines any relevant Constitutional risks that might be engaged by not expanding or expanding the mandatory data retention regime to civil proceedings.**

Access to telecommunications data

32. The Privacy Act exempts certain disclosures of personal information by APP entities, including where disclosure:

    - Is requested by an individual to any personal information that the provider holds about the individual on request, subject to certain exceptions (such as where giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body).[16]

    - 'Is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim';[17] and

    - 'Is required or authorised by or under Australian law or a court/tribunal order'.[18]A large variety of Federal, State and Territory laws fall into this category, empowering particular agencies to compel disclosure. For example, section 29 (Power to obtain documents and things) of the *Crime Commission Act* 2012 (NSW) provides that an executive officer of the NSW Crime Commission with special legal qualifications may, by notice in writing served on a person, require the person to attend 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.

33. However, disclosure by a communications service provider of a broad class of information about an individual's communications which are protected by section 276 of the Telecommunications Act can lead to criminal liability. This is subject to exceptions in Division 3 of Part 13 of the Telecommunications Act and Chapter 4 of the TIA Act. Briefly, the Division 3 of Part 13 of the Telecommunications Act exceptions relate to, for example:

    - Performance of person's duties;[19]

[16] See *Privacy Act 1988 (Cth),* Australian Privacy Principle 12.3. Under APP 12, an organisation may impose a charge on an individual for providing access to their personal information, provided the charge is not excessive.
[17] *Privacy Act 1988 (Cth),* Australian Privacy Principle 6.2(c); s 16A, Item 4 *Privacy Act 1988* (Cth).
[18] Ibid Australian Privacy Principle 6.2(b).
[19] *Telecommunications Act 1977* (Cth) s 279.

- Authorisation by or under law, including where disclosure is: in connection with the operation of an enforcement agency within the meaning of the TIA Act; or required or authorised by or under law.[20]

- Witnesses;[21]

- Assisting the ACMA, the ACCC or the Telecommunications Industry Ombudsman;[22]

- Integrated public number database;[23]

- Data for emergency warnings;[24]

- Calls to emergency service number;[25]

- Threat to person's life or health;[26]

- Communications for maritime purposes;[27]

- Knowledge or consent of person concerned;[28]

- Implicit consent of sender and recipient of communication;[29]

- Business needs of other carriers or service providers;[30]

- Location dependent carriage services;[31] and

- Circumstances prescribed in the regulations.[32]

34. In addition, section 313 of the Telecommunications Act requires carriers and carriage service providers to give Federal and State officers and authorities such help as is reasonably necessary for enforcing the criminal law and laws imposing pecuniary penalties; assisting the enforcement of the criminal laws in force in a foreign country; protecting the public revenue or safeguarding national security.

35. Chapter 4 of the TIA Act exceptions relate to who can access telecommunications data, for what purpose and in what circumstances. For example, a telecommunications carrier may make a disclosure when:

    - It chooses to make a voluntarily disclose information about communications to an enforcement agency if the disclosure was

[20] Ibid s 280.
[21] Ibid s 281.
[22] Ibid s 284.
[23] Ibid s 285.
[24] Ibid s 285A.
[25] Ibid s 286.
[26] Ibid s 287.
[27] Ibid s 289.
[28] Ibid s 289.
[29] Ibid s 290.
[30] Ibid s 291.
[31] Ibid s 291A.
[32] Ibid s 292.

reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of public revenue.[33]

- An authorised officer of an enforcement agency gives a written authorisation to a carrier which mandates provision of information about communications to an authorised officer of that agency, which is purportedly necessary pursuant to enforcement of either the criminal law, a law imposing a pecuniary penalty, or for the protection of public revenue.[34]

36. Section 176A of the TIA Act limits the authorities and bodies that can access telecommunications data to criminal law-enforcement agencies and authorities and bodies declared under section 176A to be an ' enforcement agency'. An 'enforcement agency' can be any authority whose functions include: enforcing the criminal law; administering a law imposing a pecuniary penalty; or administering a law relating to the protection of the public revenue. In prescribing an authority or body as an 'enforcement agency' the Minister must have regard to a range of factors, including whether the authority or body is required to comply with the APPs or other such similar binding privacy obligations to protect personal information.

Access to telecommunications data in civil proceedings

37. This part of the Law Council's submission addresses the first question raised in the Consultation Paper, namely: in what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act (refer to Attachment A)?

38. As noted above, other persons can access retained telecommunications data when the disclosure is:

    - In connection with the operation of an enforcement agency within the meaning of the TIA Act; or

    - Required or authorised by or under law.[35]

39. This allows other organisations or individuals to access telecommunications data of the kind set out in section 187AA of the TIA Act, such as through the exercise of other statutory powers or through court process in civil proceedings such as subpoena or notice to produce or coronial requests.

40. Court orders may involve a civil dispute whereby the telecommunications data is considered to be required to allow the court to adjudicate the matter.

41. Subpoenas are commonly used in civil litigation to require the production of documents and/or to obtain evidence from service providers who are not parties to a lawsuit. A party to a lawsuit may request a subpoena be issued to a carriage service provider.

---

[33] *Telecommunications (Interception and Access) Act 1979* (Cth) s 177.
[34] Ibid s 178.
[35] *Telecommunications Act 1977* (Cth) paras 280(1)(a) and (b).

42. The number of such subpoenas each year is unclear but the Law Council expects the figures to be high. The Chair of the Law Council's Business Law Section's Media and Communications Law Committee and partner of Gilbert + Tobin, Mr Peter Leonard, has previously noted, for example, that:

> *Given that over 550,000 requests for information about communications were made by Australian law enforcement agencies in the last reported year, one might suspect that the number of subpoenas for communications data is already very large. We can also confidently expect (absent any restriction) that this number is likely to substantially grow in response to availability of richer and deeper data sets collected by telecommunications service providers to meet mandatory data retention requirements.*[36]

43. There are a number of different circumstances in which a civil litigant may wish to have access to retained telecommunications data for the purpose of civil proceedings. The Law Council and LSSA consider that the range of circumstances may be unquantifiable given the nature, range and number of civil proceedings.

44. A service provider may be subpoenaed to provide telecommunications data of the kind referred in section 187AA in a variety of civil proceedings, including (but not limited to):

- Proceeds of crime matters;
- Coronial proceedings (e.g. concerning the death of a person);
- Common law proceedings (e.g. concerning an injury sustained);
- Copyright infringement proceedings;
- Bankruptcy or other financial proceedings;
- Proceedings in the Family Court of Australia, including in relation to divorce proceedings, or in property proceedings when ownership of property or assets might be disputed or issues about whether a de facto relationship existed, when it started, and when it ended;
- Proceedings in various courts under the *Family Law Act 1975* (Cth) (**the Family Law Act**), for parenting arrangements;
- State and Territory Domestic and Family Violence/apprehended violence orders/personal protection hearings and breach hearings; and
- State and Territory child protection proceedings;
- Guardianship and Administration matters;
- Royal Commission proceedings or other Commissions of Inquiry;
- Unfair dismissal/employment proceedings;

[36] Peter Leonard, 'Fishing By Subpoena in the Rising Ocean of Communications 'Metadata': A Debate Yet to Start', *Gilbert + Tobin* (2015) 2.

- Worker's Compensation proceedings; and
- Transport accident proceedings.

45. In addition, telecommunications data may be sought in the context of a preliminary discovery application. For example, in matter of *Dallas Buyers Club LLC v iiNet Limited (No 4*) [2015] FCA 838 the applicant sought from iiNet Limited, a service provider under the TIA Act*,* information that a service provider must keep, or cause to be kept, under subsection 187A(1) of the TIA Act.

46. The Law Council recommends that the Attorney-General's Department release a further Consultation Paper which clearly outlines and explains the circumstances where parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act.

47. In its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, the PJCIS recognised that additional privacy safeguards were needed in light of the possible increase in the frequency and volume of telecommunications data accessed by civil litigants as a result of the implementation of the scheme and the public interest in confining disclosure of and access to, telecommunications data, to protect the broader privacy interests of the community.[37]

48. Section 280 of the Telecommunications Act was subsequently amended by the Data Retention Act such that data retained *solely* for the purposes of the mandatory data retention scheme cannot be used for civil proceedings. That prohibition commences on 13 April 2017. The provision includes a regulation making power to enable appropriate exceptions to be made.

49. Subsection 280(1B) of the Telecommunications Act currently prohibits who may access telecommunications data in section 187AA of the TIA Act where:

    - The disclosure is required or authorised because of a subpoena, a notice of disclosure, or an order of a court in connection with a civil proceeding;
    - The information or document is kept by a service provider 'solely for the purpose of complying' with the mandatory statutory data retention obligation;[38] and
    - The disclosure sought is not for the purpose of:
        - complying with a written authorisation under the TIA Act;
        - complying with other warrants or authorisations under the TIA Act;
        - certain public interest disclosures provided for in the Telecommunications Act (e.g. an emergency warning , a call to an emergency services number, a threat to life situation, or preservation of human life at sea);

[37] Peter Leonard, 'Mandatory Internet Data Retention in Australia – Looking the horse in the mouth after it has bolted', *Gilbert + Tobin* (May 2015), 28.
[38] *Telecommunications Act 1997* (Cth) s 280(IB)(b).

- providing persons with access to their personal information in accordance with the Privacy Act;
- a purpose prescribed by the regulations; or
- a purpose incidental to any of these purposes.

50. A purpose is yet to be prescribed by the regulations and is a subject at issue in the current inquiry. This power is only subject to the normal disallowance procedures prescribed by the *Legislative Instruments Act* 2003 (Cth).

51. The Law Council notes that a practical difficulty that might arise is whether access to telecommunications data in a civil proceeding is permitted because the service provider is holding the data for purposes other than complying with their mandatory data retention obligations, for example, business purposes, other regulatory purposes, billing verification, data analytics or service quality monitoring/assurance. The Revised Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (**Data Retention Bill**) states:

> *This provision thereby ensures that telecommunications data that is collected, retained or used for a service providers ordinary business purposes or other purposes unrelated to the data retention obligation, continues to be available for such [legal] proceedings.*[39]

52. The Chair of the Law Council's Business Law Section's Media and Communications Law Committee, Mr Peter Leonard, has previously noted that 'in practice this often will not be an easy determination'.[40] Mr Leonard has also noted that:

> *… it is unfortunate that the issue is left for uncertainty and possible disputation, particularly given the potential jeopardy facing the carrier in determining whether to release and potentially be exposed to criminal sanctions in Part 13 of the Telecommunications Act 1997 and breach of the Privacy Act, or not to release and then possibly be in contempt of court.*[41]

53. The Law Council agrees with this assessment.

54. The Law Council also notes that, while parties may be able to subpoena documents containing this data, mandating its retention and use for these non-criminal purposes is a further incursion into people's privacy. If a party to proceedings can demonstrate a legitimate forensic purpose, they may possibly get access to a very limited subset of data – a much different mechanism than this which requires the retention and storage of everybody's data.

[39] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Supplementary Explanatory Memorandum, 33.
[40] Peter Leonard, 'Fishing By Subpoena in the Rising Ocean of Communications 'Metadata': A Debate Yet to Start', *Gilbert + Tobin* (2015) 3.
[41] Peter Leonard, 'Mandatory Internet Data Retention in Australia – Looking the horse in the mouth after it has bolted', *Gilbert + Tobin* (May 2015), 29.

Recommendation

- **A further Consultation Paper should be released by the Attorney-General's Department which clearly outlines and explains the circumstances where parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act.**

Impact on civil proceedings

55. This part of the Law Council's submission addresses the second question raised in the Consultation Paper, namely: what, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?

56. The information outlined in section 187AA is collected and retained for law enforcement and intelligence purposes. Since the mandatory data retention scheme was not designed for civil litigation, the consequences of allowing civil litigants to access this data are unclear.

57. Telecommunications data is currently often the subject of subpoenas but not the metadata in the form required to be retained under the TIA Act. The Law Council considers that the impact on litigation time, expense and efficiency is unknown but a serious consideration that should be the subject of assessment in a regulation impact statement or an independent cost benefit analysis. Possible impacts on access to justice should be considered in any such assessment.

Recommendations

- **A further Consultation Paper should be released by the Attorney-General's Department which clearly discusses the basis of the Consultation Paper's second question and discusses the possible impact on civil proceedings.**

- **Any expansion of the mandatory data retention regime to civil proceedings should be the subject of assessment in a regulation impact statement or an independent cost benefit analysis.**

Civil proceedings or circumstances where the mandatory data retention prohibition should not apply

58. The third Consultation Paper question asks whether there are particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the Telecommunications Act should not apply. The Consultation Paper is silent as to whether there are particular kinds of civil proceedings in which it is contemplated an exception to the prohibition should be made. This makes it very difficult for non-

government organisations to usefully comment in light of the vast array of possible civil proceedings.

59. In the absence of specific proposals demonstrating a need for an exception, the Law Council, LIV and LSSA's preliminary position is that civil litigants should continue to be prohibited from accessing telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime. This is because any exemption may be (depending on its purpose) contrary to the intention of the mandatory data retention regime. The Law Council and LIV are concerned regarding potential 'scope creep' given the intention of the mandatory data retention regime and how it has been designed to operate.

60. The LSSA has submitted that allowing some access to compulsorily retained telecommunication data by reference to arbitrary categories of civil litigation is inappropriate in that:

    - It is inconsistent with the underlying policy and reason the TIA Act was introduced;
    - There will be an increase in the cost and time of all civil litigation;
    - Any categories would be arbitrary; and
    - The infringement of privacy, in the circumstances, is not justified.

61. The LSSA also noted the difficulty in determining whether an action is within an exemption category (noted above).

62. On this basis, the LSSA is of the view that the regulations should not allow any exemption for use of such data in any civil proceedings.

63. In the alternative, if there is to be any exception to prohibition of use of data compulsorily retained by reason of TIA Act, the LSSA recommends that the regulations should not attempt to categorise types of civil litigation but should include a provision '*unless there are exceptional circumstances, and the data is directly relevant, and there is a Court order permitting access*'. However, for the reasons noted, the far preferable approach in the LSSA's view is that there should be no exceptions.

64. Previously, the Attorney-General's Department's supplementary submission to the PJCIS's Data Retention Bill Inquiry,[42]has noted that the following kinds of civil proceedings or circumstances may potentially warrant an exception in the 280(1B) Telecommunications Act regulation making power:

    - Proceeds of crime actions;
    - Civil child protection investigations;

[42] Attorney General's Department, *Limiting the availability of telecommunications data to criminal proceedings*, Supplementary Submission to the Parliamentary Joint Committee on Intelligence and Security's inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (2015).

- Apprehended violence orders;[43]
- Actions involving incidents of stalking and harassment, which often involve the use of a carriage service; and
- Laws that impose a pecuniary penalty or which protect the public revenue.

65. However, the necessity of these exceptions and how they would operate has not been clearly articulated.

66. Each of these matters is briefly discussed below. However, the Law Council recommends that the Attorney-General's Department release a further Consultation Paper which outlines specific proposals where it considers that there might be a need to create particular civil proceedings exceptions. This would allow organisations to better determine the necessity and proportionality of such proposals.

67. The Law Council would welcome the opportunity to provide its views on the additional matters via further submissions to the Department.

Recommendations

- **A further Consultation Paper should be released by the Attorney-General's Department which outlines specific proposals where it considers that there might be a need to create particular civil proceedings exceptions to section 280 of the Telecommunications Act..**
- **Any exceptions must be considered in light of Australia's international human rights obligations, including the right to privacy.**

Proceeds of crime actions

68. Law enforcement can already access telecommunications data to pursue proceeds of crime civil proceedings by way of a court order. Proceeds of crime civil forfeiture matters allow the confiscation of assets without the need for a criminal conviction.[44] The court is required to determine whether it is more probable than not that a person committed a serious offence and that property has been derived from that conduct[45]. A serious offence is defined to cover a broad range of offences as prescribed by regulation.[46] The person about whom it is said it is more probable than not that they have committed a serious offence must prove to the court that his or her assets were

[43] While the Attorney-General's Department's supplementary submission used the phase 'apprehended violence orders', the Law Council notes that this term is not used in all jurisdictions. For example, in Queensland, the term 'domestic and family violence orders' is used. The Law Council would prefer the use of the more neutral term 'personal protection orders' in this context.
[44] See, e.g. *Proceeds of Crime Act 2002* (Cth) ss 17, 18 and 51.
[45] See e.g. *Criminal Proceeds Confiscation Act* 2002 (Qld) s 58(1).
[46] See, e.g. *Proceeds of Crime Act 2002* (Cth) Dictionary.

lawfully derived, reversing the onus of proof.[47] The Family Law Act also provides for proceeds of crime claims.[48]

69. The Law Council acknowledges the value of telecommunications data to proceeds of crime investigations. This value may rise as criminals increasingly rely on communications technology.

70. Mandatory data retention legislation requiring data retention for two years was justified to support critical investigative capabilities in fighting serious crime and terrorism. As proceeds of crime proceedings are increasingly being used by law enforcement in the fight against serious crime, there may be a higher requirement for data up to two years old for serious offences as prescribed under proceeds of crime legislation.

71. However, evidence is required to demonstrate this proposition and whether mandatory data retention is a necessary and proportionate measure for proceeds of crime purposes. This is particularly important in light of the telecommunications data that may already be accessed in proceeds of crime matters.

Civil child protection investigations

72. Child abuse and neglect are often closely linked to family violence.[49] Civil law measures of child protection and family violence are akin to criminal law measures insofar as both have the common and principal objective of protecting and securing the future welfare of those who are at risk of harm caused by family violence.[50] The complex interrelationship between criminal and care and protection issues has previously been noted by the Australian Law Reform Commission as requiring the 'strongest approach to decisions about how to deal with offences against children' involving 'co-operative relationships between key agencies that bring different interests, skills and responsibilities to the process'.[51]

73. The Law Council acknowledges that an exception relating to civil child protection investigations would be in pursuit of the pressing issue of safety for children as a legitimate objective. Similarly, location orders under section 67J of the Family Law Act may assist a court when it needs to find a child. Nonetheless, evidence is required to demonstrate the kinds of circumstances where mandatory data retention is a necessary and proportionate measure for civil child protection investigations and location orders.

[47] Ibid ss 29, 73.
[48] See, e.g. *Family Law Act 1975* (Cth) s 90VD.
[49] Australian Law Reform Commission, *Family Violence – A National Legal Response Report 114* (11 November 2010), [20.8].
[50] Ibid [20.27].
[51] Ibid [20.28].

Apprehended violence orders[52]

74. The Family Law Act subsection 4(1) defines 'family violence orders' as an order (including an interim order) made under a prescribed law of a State or Territory to protect a person from family violence. Section 4AB of the Family Law Act defines family violence to mean 'violent, threatening or other behaviour by a person that coerces or controls a member of the person's family, or causes the family member to be fearful'.[53] Family violence orders are given various names under State and Territory Acts; personal protection orders, restraining orders or apprehended violence orders.

75. In addition, to State based personal protection orders domestic violence may be alleged in family law proceedings. Section 68B of the Family Law Act provides for personal protection injunctions, but is rarely used due to the availability of State based orders.

76. Difficulties in permitting access to telecommunications data retained *solely* for the purpose of the mandatory data retention scheme in circumstances of personal protection orders include:

    - Determining the seriousness of the behaviour to justify access. Subpoenas are issued over the counter by administrative staff in court registries without judicial consideration of their merits,[54] though a party may be able to object to the inspection of material produced under a subpoena.[55]

    - Whether such data will be made available to both parties. While allowing data to be available to both parties might be consistent with the equality of arms principle, there are clear dangers in allowing alleged perpetrators to have access to telecommunications data of victims (as discussed above). In family law litigation, for example, procedural fairness means the parties/their lawyers are able to have access to what is produced in answer to a subpoena. Under the Rules applicable to family law proceedings there is also an obligation for full and frank disclosure on litigants. There are also obligations on practitioners in some instances, to disclose all relevant material to the other parties in the litigation.[56] Often there are concurrent proceedings in federal, state or territory courts. The former may relate to family law matters and the later may relate to

[52] While the Attorney-General's Department's supplementary submission used the phase 'apprehended violence orders', the Law Council notes that this term is not used in all jurisdictions. For example, in Queensland, the term 'domestic and family violence orders' is used. The Law Council would prefer the use of the more neutral term 'personal protection orders' in this context.
[53] Examples of behaviour that may constitute family violence include (but not limited to): an assault; a sexual assault or other sexually abusive behaviour; stalking; repeated derogatory taunts; intentionally damaging or destroying property; intentionally causing death or injury to an animal; unreasonably denying the family member the financial autonomy that he or she would have otherwise have had; unreasonably withholding financial support needed to meet the reasonable living expenses of the family member, or his or her child, at a time when the family member is entirely or predominantly dependent on the person for financial support; preventing the family member from making or keeping connections with his or her family, friends or culture; or unlawfully depriving the family member, or any member of the family member's family, of his or her liberty – *Family Law Act 1975* (Cth) s 4AB(2).
[54] Peter Leonard Fishing By Subpoena in the Rising Ocean of Communications 'Metadata': A Debate Yet to Start', *Gilbert + Tobin* (2015) 5.
[55] See, e.g. *Federal Court Rules 2011* r 24.20(6).
[56] Ibid r 13.01.

personal protection orders. It may be problematic as to how information can be 'siloed' between the two proceedings.

77. A party to a family law or civil domestic violence matter may wish to obtain data on their former partner or spouse for nefarious gain or to perpetuate the intimidation and harassment aspects of domestic violence through use of the court system. This should not be permitted.

78. The Law Council's preliminary view in the absence of a detailed proposal is that if access to telecommunications mandatorily retained data for apprehended violence orders is to be justified, there must be the ability for the court to assess the merits of granting a court order taking into account the potential danger to the victim in granting access, the privacy of the parties and the seriousness of the alleged behaviour.

Actions involving incidents of stalking and/or harassment, which often involve the use of a carriage service

79. The Law Council notes that stalking and harassment involving the use of a carriage service but also other various forms of family violence may also amount to a serious invasion of privacy. Not only is stalking a criminal offence, both stalking and harassment are forms of domestic and family violence of themselves, and can cause anxiety, distress or other harm and may restrict the ability of an individual to live freely. This is particularly so where conduct is repeated, unwanted and intended to distress and demean an individual. Stalking and harassment can also be part of a broader history of domestic violence and abuse.

80. State and Territory jurisdictions have a range of stalking and harassment criminal offences.[57] Section 474.17 of the *Criminal Code Act 1995* (Cth) also provides for a criminal offence punishable by a maximum of three years' imprisonment for using a carriage service to menace, harass or cause offense. A person commits an offence if (a) the person uses a carriage service; and (b) the person does so in a way (whether by use or the content of the communication or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing, or offensive. This can apply to menacing, harassing or causing offence to: an employee of an NRS provider; or an emergency call person; or an employee of an emergency service organisation or an APS employee in the Attorney-General's Department acting as a National Security Hotline call taker.

81. In addition to criminal offences for stalking and harassment, civil remedies in the form of protection or intervention orders designed to prevent stalking behaviour may be available.[58]

---

[57] *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13; *Crimes Act 1958* (Vic) Section 21A; *Crimes Act 1900* (ACT) 35; *Criminal Code 1899* (Qld) s 359E; *Criminal Code Act* (NT) s 189; *Criminal Code (WA)* s 338E*; Criminal Code 1924* (Tas) s 192; *Criminal Law Consolidation Act 1935* (SA) s 19AA.

[58] There are a range of Commonwealth, state and territory criminal offences for conduct that may amount to harassment. See, e.g. *Crimes Act 1958* (Vic) s 21A; *Crimes Act 1900* (NSW) s 60E; *Criminal Code Act 1995* (Cth) ss 474.15 and 474.17. In the domestic and family violence area criminal offences include: *Domestic and Personal Violence Act 2007* (NSW) s 16; *Family Violence Protection Act 2008* (Vic) ss 53, 74; *Domestic Violence and Protection Orders Act 2008* (ACT) s 46; *Domestic and Family Violence Protection Act 2012* (Qld) s 37 *Domestic and Family Violence Act* (NT) s 18; *Restraining Orders Act 1997* (WA) s 11A; *Family Violence Act 2004* (Tas) s 16; *Intervention Orders (Prevention of Abuse) Act 2009* (SA) s 6.

82. The Law Council understands that the use of criminal sanctions for stalking and harassing behaviour may occur less frequently than personal protection intervention orders. An intervention order can still be obtained, notwithstanding the absence of any criminal conviction against an alleged stalker, provided the relevant statutory criteria for the making of the intervention order have been satisfied.

83. Difficulties in permitting access to telecommunications data retained *solely* for the purpose of the mandatory data retention scheme in stalking and harassment cases include:

    - Determining the seriousness of the stalking or harassing behaviour to justify access. Subpoenas are issued over the counter by administrative staff in court registries without judicial consideration of their merits,[59] though a party may be able to object to the inspection of material produced under a subpoena.[60]

    - Whether such data will be made available to both parties. While allowing data to be available to both parties might be consistent with the equality of arms principle, there are clear dangers in allowing alleged perpetrators to have access to telecommunications data of victims.

84. The Law Council's preliminary view in the absence of a detailed proposal is that if access to telecommunications mandatorily retained data for actions involving incidents of stalking and harassment is to be justified, there must be the ability for the court to assess the merits of granting a court order taking into account the potential danger to the victim in granting access, the privacy of the parties and the seriousness of the alleged behaviour.

Laws that impose a pecuniary penalty or which protect the public revenue

85. There are many laws that impose a pecuniary penalty or which protect the public revenue ranging in seriousness. Mandatory data retention was enacted to assist in preventing and prosecuting serious crime and terrorism. Less serious laws imposing penalties for licence breaches and overdue taxes would appear to constitute an unjustifiable expansion of the mandatory data retention regime. More detail is required as to whether there are particular laws where there is an identified operational need for access to telecommunications data pursuant to the mandatory data retention scheme.

Oversight arrangements

86. The Law Council notes it is of critical importance that any proposed exceptions for civil proceedings include appropriate safeguards to ensure transparency, accountability and protection for the privacy of individuals.

87. Absent from the Consultation Paper is an examination of specific options for safeguards, scrutiny and oversight mechanisms that might apply to access to telecommunications data retained solely for the purpose of the mandatory data

[59] Peter Leonard 'Fishing By Subpoena in the Rising Ocean of Communications 'Metadata': A Debate Yet to Start', *Gilbert + Tobin* (2015) 5.
[60] See, e.g. *Federal Court Rules 2011* r 24.20(6).

retention regime in civil proceedings. Categories of possible oversight arrangements could include for example:

- Requirements for ex ante (before access) independent review and certification that the access requirements have been met.[61] The Law Council notes that its submission dated 20 January 2015 in respect of the Data Retention Bill, the Law Council called for the introduction of a warrant process to ensure that the data was being appropriately and justly accessed.[62] In respect of any possible expansion of accessing data for use in civil proceedings, the Law Council and QLS would like to see a similar level of judicial oversight applied;

- Legislation clearly stipulating the criteria a judge must assess when making a decision to allow the release of telecommunications data. For example, such criteria could be similar to the criteria which enable parties to access documents under notices of non party disclosure and subpoenas. The criteria could also be based on where the data exists and can have significant benefit to parties to a proceeding, where a judge decides on a case by case basis that it is in the interests of justice and balancing privacy considerations to do so. The QLS would welcome such an approach. It might also be worth exploring, as the LSSA has noted (subsequent to preferring an approach that there should be no exceptions), whether the criteria should include a provision to the effect that 'unless there are exceptional circumstances, and the data is directly relevant, and there is a court order permitting access';

- Retrospective oversight and review, for example, by randomised check audit or other review process;[63]

- The use of public interest monitors during proceedings; and

- Public reporting obligations.

88. The Law Council is of the view that access to telecommunications data under mandatory data legislation should ordinarily require an independent tribunal warrant, 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. However, this was not accepted by the PJCIS or the Australian Parliament when the Data Retention Act was enacted.

89. Current oversight arrangements are directed at reviewing telecommunications data access powers *after* they have been exercised. This change heightens the risk of an encroachment on rights of privacy without testing the proportionality of the action.

90. The role of the Commonwealth Ombudsman might be expected to expand significantly with any broadening of the mandatory data retention regime to civil proceedings. Impact on security and privacy oversight mechanisms should also be

[61] Peter Leonard, 'Mandatory Internet Data Retention in Australia– Looking the horse in the mouth after it has bolted', *Gilbert + Tobin* (May 2015), 4.
[62] Law Council of Australia, *Submission on the Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, (January 2015), 4.
[63] Peter Leonard, 'Mandatory Internet Data Retention in Australia– Looking the horse in the mouth after it has bolted', *Gilbert + Tobin* (May 2015), 4.

considered. Accordingly, the Commonwealth Ombudsman, Privacy Commissioner and Inspector General of Intelligence and Security Commonwealth Ombudsman should be consulted on any proposals. They should also be adequately resourced to perform their important oversight functions under the mandatory data retention legislation. Effective oversight depends on adequate resourcing.

Recommendations

- **A further Consultation Paper should be released by the Attorney-General's Department which examines options for oversight mechanisms and public reporting obligations for any expansion of the mandatory data retention regime.**
- **The Commonwealth Ombudsman, Privacy Commissioner and Inspector-General of Intelligence and Security Commonwealth Ombudsman should be consulted on any proposals. They should also be adequately resourced to perform their important oversight functions under the mandatory data retention legislation.**