Law Council
OF AUSTRALIA

Review of the mandatory data retention regime

Parliamentary Joint Committee on Intelligence and Security

18 July 2019

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 2019 Executive as at 28 June 2019 are:

- Mr Arthur Moses SC, President
- Ms Pauline Wright, Treasurer
- Mr Tass Liveris, Executive Member
- Dr Jacoba Brasch QC, Executive Member
- Mr Ross Drinnan, Executive Member

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

Acknowledgement

The Law Council acknowledges the assistance of its National Criminal Law Committee, the Law Society of South Australia, the Law Society of New South Wales in the preparation of this submission, as well as the Business Law Section's Privacy Law Committee.

Executive Summary

1. The Law Council of Australia (**Law Council**) welcomes the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) in relation to its review of the mandatory data retention regime contained in Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**).

2. The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (**Data Retention Act**) introduced amendments to the TIA Act to establish a mandatory national data retention regime which commenced on 13 October 2015. The Law Council notes that this statutory review is mandated by section 187N of the TIA Act.

3. The Law Council acknowledges that the purpose of the regime is to pursue the legitimate objective of investigating and combatting serious crime including terrorism related offending.[1] However, the Law Council considers that 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 unnecessary intrusion of their privacy by the State. It is important that the regime provides safeguards against the wilful, systematic degradation of human rights in the digital era such as the fundamental human right to privacy.

4. The Law Council previously provided a submission to the Committee in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (**Data Retention Bill**) when it was first introduced to Parliament.[2] In that submission, the Law Council opposed the introduction of the mandatory data retention scheme as proposed by the Data Retention Bill.

5. The Law Council continues to have concerns in relation to the data retention regime, including in relation to:

   - the reasonableness, necessity and proportionality of blanket mandatory telecommunications data retention in respect of all citizens, residents and visitors;
   - the security of the retained telecommunications data,
   - issues of client legal privilege; and
   - the adequacy of oversight mechanisms to safeguard privacy including the need for pre-access oversight of authorisations to access data.

6. In this submission the Law Council will comment on these issues, as well as the following:

   - the appropriateness of the data set, retention periods and access arrangements;
   - the continued effectiveness of the scheme, taking into account changes in the use of technology since the legislation came into effect; and
   - developments in international jurisdictions since the introduction of the scheme.

[1] The Law Council notes that the judgement of the Court of Justice of the European Union in *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: at [42]-[51]. This was subsequently affirmed in the decision of *Tele2 Sverige AB v Post-och Telestyrelsen and SSHD v Tom Watson and Others* (C-203/15) (C-698/15) [2016] CJEU 22.

[2] Law Council of Australia, Submission No 126 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (20 January 2015).

7. In order to improve the scheme, the Law Council makes the following recommendations:

- The TIA Act should clearly define the terms 'contents' and 'substance' of a communication as referred to in paragraph 187A(4)(a).
- The data retention period should be reduced to no longer than the minimal period required by law enforcement and security agencies.
- Agencies which can access stored communications and telecommunications data should be exhaustively listed in the primary legislation.
- Access to existing telecommunications data should be limited to agencies required to investigate serious indictable offences, specific threats to national security or to assist in the location of missing persons as defined in the legislation.
- There is a need for greater clarity as to when retained data will be considered 'personal information' under section 187LA of the TIA Act.
- Law enforcement bodies should be required to notify the Commonwealth Ombudsman as soon as practicable following a decision not to notify an affected individual of a serious data breach under section 26WN of the *Privacy Act 1988* (Cth) (**Privacy Act**). This information should be reported annually by the Commonwealth Ombudsman.
- Access to retained telecommunications data should be authorised by a warrant issued by an independent court or 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.
- 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.
- Section 180H of the TIA Act should be amended to include a paragraph so that a journalist information warrant is required for the authorisation of access to the telecommunications data of any person that may reasonably be believed as being used to identify a journalist's source.
- Government agencies that have access to telecommunications data should develop minimum standards for the security of telecommunications data and put them forward for consideration and approval of the Committee.
- Entities subject to telecommunications data retention requirements under the TIA Act should be required to demonstrate to the Australian Communications and Media Authority (**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.

Proportionality: the data set, retention periods and access

Background

8. The *International Covenant on Civil and Political Rights*[3] (**ICCPR**) provides for the protection for individuals from arbitrary or unlawful interference with their privacy, family home or correspondence.[4] Any assessment of the legitimacy of the mandatory data retention regime in relation to recognised international human rights, such as the right to privacy, must analyse whether the laws are reasonably necessary and proportionate to achieving a legitimate purpose. The Law Council acknowledges the aim of the data retention regime is legitimate, however, the Law Council maintains concerns that the laws as they are currently framed are not the least restrictive means of achieving the aim of investigating and preventing serious criminal activity.

9. The Law Council acknowledges the evidence from various law enforcement agencies that was put to the Committee when it previously considered the Data Retention Bill, in particular the observations that the ability of agencies to access telecommunications data was in long-term decline. The Committee concluded that this decline was having an adverse impact on the capacity of law enforcement agencies to detect, investigate and prevent serious criminal activity, including threats to national security, public safety and in the sexual exploitation of children.[5] On this basis, the Committee found that the mandatory data retention regime was in fact necessary. It considered that a case had been made that warranted legislative intervention to preserve the availability of telecommunications data for law enforcement purposes which was considered to be in the public interest.

10. However, as observed by the Committee in its 2015 report on the Data Retention Bill, 'the adequacy of safeguards around access to telecommunications data are relevant to the proportionality of the proposed data retention regime'.[6] An issue for the Law Council is the adequacy of those safeguards put in place to ensure the scheme is proportionate to its legitimate purpose, so as to address privacy and civil liberties concerns, particularly given the scheme applies indiscriminately to all people.

11. The Parliamentary Joint Committee on Human Rights (**PJCHR**) also examined the Data Retention Bill, and in its report on the compatibility of the Data Retention Bill with international human rights obligations stated:

> *A requirement to collect and retain data on every customer just in case that data is needed for law enforcement purposes is very intrusive of privacy, and raises an issue of proportionality…The committee therefore considers that the scheme must be sufficiently circumscribed to ensure that the limitations of the right to privacy are proportionate*…[7]

[3] *International Covenant on Civil and Political Rights*, opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
[4] Ibid art 17.
[5] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 70.
[6] Ibid 23.
[7] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Telecommunications (Interception and Access) Bill 2014* (Fifteenth Report of the 44th Parliament, November 2014) 1-31.

The data set

12. The mandatory retention of data scheme was established in 2015. The Data Retention Act mandated the collection and retention of certain categories of telecommunications data by:

    - services set out in subsection 187A(3) of the TIA Act, being a service for carrying communications, or that enable communications to be carried, by guided or unguided electromagnetic energy or both;
    - services as operated by a carrier or internet service provider;
    - a service, if the person operating the service owns or operates 'infrastructure' in Australia that is used in the provision of prescribed carriage service providers, including internet services providers; and
    - any other service provider that is declared by the Minister to be subject to the scheme as permitted by subsection 187A(3C) of the TIA Act.

13. These services are required to collect and retain certain types of data as defined in the schedule attached to section 187AA of the TIA Act for a period of two years.[8]

14. Section 187AA of the TIA Act sets out the kinds of information that a service provider must keep, or cause to be kept under subsection 187A(1) of the TIA Act. This includes information pertaining to the following:

    - the subscriber of, and accounts, services, telecommunications devices, and other relevant services;
    - the source and destination of a communication;
    - the date, time and duration of a communication, or of its connection to a relevant service;
    - the type of communication or of a relevant service used in connection with a communication, such as SMS, email, chat, forum or social media, ADSL, wi-fi, call waiting, data volume usage; and
    - the location of the equipment, or a line, used in connection with a communication.

15. While subsection 187A(4) of the TIA Act states that a service provider is not required to keep information that 'is the contents or substance of a communication' or about a subscriber's web browsing history, this does not mean that this information will not be retained by the service provider, especially if it is more cost effective to do so when complying with the scheme. As a consequence, enforcement agencies can potentially have access to a wide range of what could reasonably be considered as personal information.[9]

16. The method for separating or filtering the contents or substance from the non-content of communications by service providers in the course of meeting their data retention obligations remains unclear. As the individual is not aware when their data is being accessed, it is unlikely that a person will enquire as to whether the content of the data is also available to be accessed by the enforcement agencies.

[8] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187C.
[9] Consideration of whether some forms of telecommunications data can be properly classified as 'personal information' has been a subject of judicial interpretation. See, eg, the discussion of *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4 in paragraph 42 of this submission.

17. Further, there is no definition of what is 'contents' of a communication for the purpose of this legislation. For example, it is not clear whether meta-tags would be captured.

18. The Law Council considers that to address the issue of proportionality, it would be useful to provide a definition in the legislation of what constitutes the 'contents or substance of a communication'. This recommendation would also address one of the recommendations made by the PJCHR that 'the bill be amended to include an exclusive definition of 'content' for the purposes of the scheme'[10] to assist in the retention of telecommunications data that does not include aspects of content.

Recommendation:

- **The TIA Act should clearly define the terms 'contents' and 'substance' of a communication as referred to in paragraph 187A(4)(a).**

The retention period

19. Limitations on law enforcement and national security agencies' powers are necessary to ensure the data retention scheme is proportionate. A scheme which applies to all Australians, involving the retention of a large amount of personal data, as well as imposing high-cost obligations and the imposition of civil penalties on service providers, dictates a requirement for defined, appropriate limits.

20. The Law Council considers that the two-year retention period required under the scheme is 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'.[11] The Explanatory Memorandum for the Data Retention Bill noted 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'.[12] However, law enforcement and security agencies were unable to approximate 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.[13]

21. In the submission provided by the Australian Federal Police (**AFP**) to the current review, it records the duration or age of the data covered since the introduction of the scheme in 2015. Across all the years where information is recorded, it consistently shows that the vast majority of authorisations relate to data that is 12 months old or less. For example, in the period 2017-2018, 13,086 authorisations related to data that was three months old or less, compared to 161 authorisations that were between 21 and 24 months old.[14]

---

[10] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Telecommunications (Interception and Access) Bill 2014* (Fifteenth Report of the 44th Parliament, November 2014) 1-39.
[11] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 19.
[12] Ibid.
[13] 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) <https://www.theguardian.com/world/2014/dec/29/metadata-most-australian-police-forces-cant-say-how-many-times-it-has-been-used-to-prevent>.
[14] Australian Federal Police, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (2019).

22. In its previous consideration of the data retention measures contained in the Data Retention Bill, the Committee considered the two year retention period to be necessary and proportionate as older data was required for the investigation of criminal offences which were of greater objective criminality, complexity, and sophistication that could often relate to issues of national security or child sexual exploitation.[15] However, the Law Council notes there is no evidence in material provided by the AFP in the current review which provides a correlation between the age of the data and the nature of the offence which it was being used to investigate.

23. The Commonwealth Government has also produced two annual reports outlining the extent to, and the circumstances in which, government agencies have used the access powers available under the TIA Act since commencement of the scheme (for the reporting years 2015-2016 and 2016-2017).[16] The most recent report provides a breakdown of the age of data accessed under the scheme over the 2016-2017 reporting year. The Law Council notes that approximately 94 per cent of access to retained data was to data less than 12 months old, less than 5 per cent was for data between 12 months and two years old, and 1.5 per cent was for data more than two years old, while 79 per cent of data access was for data less than three months old.[17]

24. Noting the vast majority of data access requests are made within the first 12 months of storage (based on statistics presently available), the Law Council considers it questionable whether retention for a two-year period is necessary or whether a reduced mandatory retention period may be more appropriate.

25. 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.

Recommendation:

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

Accessibility of data

26. The TIA Act states that an 'enforcement agency' for the purposes of the data retention scheme includes 'criminal law-enforcement agencies' as listed in section 110A, or an authority or body for which a declaration is in force.[18] In relation to the latter, the legislation permits the Minister to declare the authority or body to be an 'enforcement agency' by way of legislative instrument.

---

[15] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 146.
[16] Attorney-General's Department, Commonwealth, (Cth), *Telecommunications (Interception and Access) Act 1979 – Annual Report 2015-2016* (Report, 2016) <www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-15-16.pdf>; Department of Home Affairs, Commonwealth, *Telecommunications (Interception and Access) Act 1979 – Annual Report 2016-2017* (Report, 2017) <www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-16-17.pdf>.
[17] Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 (Cth) – Annual Report 2016-2017* (Report, 2017) Table 38.
[18] *Telecommunications (Interception and Access) Act 1979* (Cth) s 176A. See also *Telecommunications (Interception and Access) Act 1979* (Cth) s 110A which provides the definition of 'criminal law enforcement agency'.

27. 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 telecommunications data retention regime.

28. The vesting of such a power in the Minister, notwithstanding disallowance procedures available to Parliament, provides a potentially broad scope in which the legislation operates. 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 telecommunications data. 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.

29. As was noted by the PJCHR when considering the Data Retention Bill:

> *Because of the significant developments in technology since the TIA was passed, the types of data that can now be accessed without a warrant is considerably broader than was the case when the access provisions under the TIA Act were enacted.*[19]

30. In this context, the PJCHR considered that 'confining the number of agencies that may access retained metadata is relevant to ensuring the proportionality of the scheme's limitation on the right to privacy'.[20]

31. A great deal of information can be gleaned about an individual through telecommunications data and the application of data analytics, which takes advantage of real advances in artificial intelligence (**AI**). Despite assurances that the scheme provides sufficient protections to the privacy of a communication by not permitting access to the content of communications,[21] there is significant research that has established that a certain amount of telecommunications data about an individual may provide sufficient information to construct a complete profile of that individual, particularly if it is matched with publicly available records.[22]

32. As was stated by the Court of Justice of the European Union (**CJEU**) in December 2016 in *Tele2 Sverige AB v Post-Och Telestyrelsen and Secretary of State for the Home Department v Watson*[23] (**Tele2 decision**), access to traffic and location data can 'allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained'.[24] The CJEU found that telecommunications data may provide a means 'of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications'.[25]

33. The Law Council considers that the categories of telecommunications data which are retained are so broadly defined as to provide information about crucial matters such as

---

[19] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Telecommunications (Interception and Access) Bill 2014* (Fifteenth Report of the 44th Parliament, November 2014) 1-41.
[20] Ibid 1-46.
[21] Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* (Cth).
[22] See, eg, L Hardesty, 'Privacy Challenges, Analysis: Its Surprisingly Easy to Identify Individuals from Credit-card Metadata', *MIT News Office* (online, 29 January 2015) <http://news.mit.edu/2015/identify-from-credit-card-metadata-0129>.
[23] (C-203/15) (C-698/15) [2016] CJEU 22.
[24] Ibid [99].
[25] Ibid.

an individual's associations and their whereabouts. For example, the following information could be revealed about a person from the subset of telecommunications data allowed 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.

34. There is an increasing number of devices connected to the Internet and by next year it is estimated that there will be in excess of 50 billion.[26] Such has been the increasing range of uses of communications through smart phones, social media, apps and into the future, other personal devices such as eHealth devices (enabling close monitoring as to an individual's physical activity), that the plethora of digital information that is available from these trails of communication is an increasingly valuable source of information. However, it has been noted that 'the increasing diversity of data collection points received scant attention in the Parliamentary debates about mandatory communications data retention'.[27]

35. In these circumstances, the Law Council considers that there needs to be greater precision in the legislation as to who is permitted to access the data and in what circumstances, particularly as the scheme operates in such a way that person is not informed when their telecommunications data is being accessed. Consequently, the Law Council considers that those agencies which can access data should be listed in the primary legislation.

36. The Law Council maintains the view that access to telecommunications data should be restricted to agencies investigating a serious indictable offence, a specific threat to national security or where it may genuinely assist in locating a missing person. This was a point commented on by the PJCHR who stated that the 'lack of a threshold, relating to the nature and seriousness of the offence, for access to retained data appears to be a disproportionate limitation on the right to privacy'.[28] The PJCHR therefore recommended that the Data Retention Bill be amended to limit 'disclosure authorisation for existing data to where it is 'necessary' for the investigation of specified serious crimes, or categories of serious crimes'.[29]

37. The internal access approval requires accessing existing or historical telecommunications data to be 'reasonably necessary'[30] for the enforcement of the 'criminal law'. While 'reasonably necessary' is not a low threshold, the regime prescribes no limitation on the types of investigation for which telecommunications data may be used, by reference to either the nature or seriousness of a considered offence. This is in contrast to section 180 of the TIA which relates to access to prospective information or documents. In this section, the authorised officer may only authorise access to prospective information that comes into existence during the period covered

[26] Dave Evans 'The Internet of Things – How the Next Evolution of the Internet is Changing Everything' (White Paper, CISCO, April 2011) 3 <www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. See also Liam Tung 'IoT Devices Will Outnumber the World's Population This Year for the First Time' *ZD Net* (Web Page, 7 February 2017) <www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/>.
[27] Peter Leonard, *Mandatory Internet Data Retention In Australia – Looking The Horse In The Moth After It Has Bolted* (Gilbert and Tobin Lawyers, May 2015) 13.
[28] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Telecommunications (Interception and Access) Bill 2014* (Fifteenth Report of the 44th Parliament, November 2014) 1-48.
[29] Ibid 1-49.
[30] *Telecommunications (Interception and Access) Act 1979* (Cth) s 178(3).

by the authority, where the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of a 'serious offence' or an offence punishable by at least three years' imprisonment.[31]

38. The Committee previously acknowledged the issue of the threshold before law enforcement agencies should be permitted to access telecommunications data retained under the regime and made certain recommendations in relation to section 180F of the TIA Act and the requirement for the Authorised officer to consider the criteria now listed in that section.[32] While regard must be had to the 'seriousness of any offence', this is very general and there should be more specific requirements listed in the legislation which defines the 'seriousness' of the offence by reference to the applicable maximum penalty.

39. The Law Council considers that for the regime to be proportionate with its aim of assisting in the protection of national security, public safety and addressing crime, access to existing 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) (**ASIO Act**)). A serious indictable offence could be defined in similar terms to section 15GE of the *Crimes Act 1914* (Cth) (**Crimes Act**) 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.

Recommendations:

- **Agencies which can access stored communications and telecommunications data should be exhaustively listed in the primary legislation;**
- **Access to existing telecommunications data should be limited to agencies required to investigate serious indictable offences, specific threats to national security or to assist in the location of missing persons as defined in the legislation.**

International perspectives on proportionality

40. To assist the Committee, the Law Council draws attention to international developments since the introduction of the mandatory data scheme in Australia which relate to issues of proportionality. The Data Retention Directive (**DRD**) of the European Union (**EU**) was designed to assist member states in the investigation and prevention of serious crime and terror related offending. The DRD required telecommunication service providers in member states to retain telecommunications data for between six months and two

[31] Note that s 180(4) of the *Telecommunications (Interception and Access) Act 1979* (Cth) also places a time limit on the available period to access prospective data to being within 45 days of the date of authorisation. See also s 180B of the *Telecommunications (Interception and Access) Act 1979* (Cth) in relation to limits of access to prospective information in relation to investigation of foreign criminal laws.
[32] *Telecommunications (Interception and Access) Act 1979* (Cth) s 180F provides the Authorised officer must be satisfied on reasonable grounds that the authorisation is a necessary interference with the privacy of the person having regard to the gravity of the conduct in which the authorisation is sought including, inter alia, 'the seriousness of any offence in relation to which the authorisation is sought'.

years.[33] The Committee has previously noted that the Data Retention Bill was based on the DRD.[34]

41. The DRD has been subject to challenge in the CJEU.[35] The CJEU accepted that the objective of the DRD, namely to ensure public safety by assisting with the investigation of terrorism and other offending, was legitimate. However, this legitimate need had to be balanced with the requirement for the protection of the fundamental right to privacy. The court held the directive to be invalid on the basis that the directive did not meet the principle of proportionality and should have provided greater safeguards to protect the right to privacy and protection of personal telecommunications data.[36]

42. In the EU, the CJEU can rule on whether the laws enacted in relation to establishing a data retention scheme are consistent with the *Charter of Fundamental Rights of the European Union* (**CFR**).[37] Article 7 of the CFR states that '[e]veryone has the right to the protection of personal data concerning him or her'. Article 8 states that '[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[38]

43. The scheme in Australia 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 DRD of 2006 which the CJEU found invalid, partly on the basis of its indiscriminate application. 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.

44. The Committee has also previously acknowledged that the outcomes of the decisions relating to the DRD indicate that:

> *… the assessment of proportionality of a mandatory data retention scheme must take into account the existence of safeguards to protect against unlawful or improper access to or use of retained information*.[39]

45. In the EU, following the decision of the CJEU ruling the DRD of 2006 as invalid there has been a range of approaches taken to implementing a data retention scheme, which have again been found to be invalid as they are infringing Articles 7 and 8 of the CFR. In Britain the *Data Retention and Investigative Powers Act 2014* (UK) (**DRIPA**) was ruled invalid by the United Kingdom High Court of Justice as it was deemed to be inconsistent with EU law as it was not sufficiently restricted and that the process lacked a requirement for independent prior approval.[40]

---

[33] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54.
[34] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 61 [2.181].
[35] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) *and Kärntner Landesregierung* (C 594/12*)* [2014] ECR.
[36] Ibid [54]-[55].
[37] *Charter of Fundamental Human Rights of the European Union* [2000] OJ L 364/1.
[38] Ibid.
[39] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 63.
[40] *R (David Davis MP, Tom Watson MP, Peter Brice, Geoffrey Lewis) v The Secretary of State for the Home Department* [2015] EWHC 2092.

46. There have subsequently been a number of court challenges to a number of pieces of legislation that have sought to introduce a telecommunications data retention scheme which have been ruled to be invalid due to their inconsistency with Articles 7 and 8 of the CFR. In the United Kingdom, the Government, having had the DRIPA ruled invalid, enacted the *Investigatory Powers Act 2016* (UK) (**IPA**). However, once again the High Court in the United Kingdom ruled the data retention provisions of the IPA to be invalid because the minister could issue data collection orders without independent judicial review or authorisation and for reasons that were not relevant to the investigation of serious crime.[41]

47. In 2016 a new directive was issued by the Parliament of the European Union which sought to reinforce the importance of the protection of personal privacy, particularly in the area of encouraging organisations to have a higher level of privacy protection in the area of criminal investigations so that any exchange of personal data 'should be facilitated while ensuring a high level of protection of personal data'.[42]

48. In 2016 the *General Data Protection Regulation* (**GDPR**) was enacted which came into effect on 25 May 2018.[43] The GDPR is a regulation in EU law on data protection and privacy for all individual citizens in the EU and the European Economic Area (**EEA**). It aims to give control to individuals over their personal data, including some forms of metadata, and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation requires controllers of personal data to put in place appropriate technical and organisational measures to implement the data protection principles. This includes the requirement of a processor of personal telecommunications data to clearly disclose any data collection and declare the lawful basis and purpose for data processing (for example if for law enforcement purposes, the clear basis for this purpose), and state how long the data is being retained.

Privacy considerations

49. Section 187LA of the TIA Act extends the meaning of 'personal information' to cover information kept under Part 5-1A of the TIA Act. Specifically, this section states that information that is retained as part of the data retention scheme is taken, for the purposes of the Privacy Act, to be personal information about an individual if the information relates to:

    - the individual; or
    - a communication to which the individual is a party.

50. However, despite section 187LA of the TIA Act stating that retained data is 'personal information' for the purposes of the Privacy Act, which would have the effect of engaging the protections of the Australian Privacy Principles, this is not a settled point of law as illustrated by the decision in *Privacy Commissioner v Telstra Corporation Ltd.*[44] In this decision, it was held that telecommunications data, specifically relating to the operation of mobile telephone services, is not regarded as 'personal information'

[41] *R (National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department, Secretary of State for Foreign and Commonwealth Affairs* [2018] EWHC 975.
[42] *Directive (EU) 2016/680 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such data, and Repealing Council Framework Decision 2008/977/JHA* [2016] OJ L 119/89.
[43] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('***GDPR***').
[44] [2017] FCAFC 4.

for the purpose of section 6 of the Privacy Act as it not information 'about an individual' for the purpose of that section. The Law Council suggests that clarification in this area is needed.

51. Since 22 February 2018, a national mandatory data breach notification scheme has operated under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), creating notification obligations for agencies and organisations with existing obligations under the Privacy Act in the event of a data breach, which includes most Australian Government law enforcement agencies.[45] This scheme creates an obligation to notify individuals whose personal information has been subject to an 'eligible data breach'.[46] An eligible data breach occurs where:

    - there is unauthorised access or disclosure of personal information held by an entity;
    - that is likely to result in serious harm to the individual; and
    - the entity has been unable to prevent the likely risk of harm with remedial action.

52. The notifiable data breach scheme applies to entities with existing personal information security obligations under the Privacy Act, including telecommunications operators and government agencies. There is, however, an exception[47] from the notifiable data breach scheme for 'enforcement related activities' where an entity is an enforcement body[48] conducting a range of surveillance, information gathering or monitoring activities. The decision as to whether this exception applies is delegated to the chief executive officer of the relevant enforcement body.

53. The Law Council is concerned that while certain instances of unauthorised access to retained telecommunications data may captured by the notifiable data breach scheme, the exception for enforcement related activities has the potential to remove the obligation to notify an individual where their personal data obtained under the data retention framework has been accessed without authority.

54. The Law Council submits that greater transparency and accountability is needed in relation to a decision by a law enforcement body to rely on the notification exception for enforcement related activities. In the Law Council's 2016 submission to the exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill (Cth) it was suggested that the Commonwealth Ombudsman, who has oversight of the data retention regime for law enforcement bodies, is well-placed to have independent oversight of the exercise of law enforcement agencies' exercise of powers relating to this exception. The Law Council again makes this recommendation to the Committee.

Recommendations:

- **There is a need for greater clarity as to when retained data will be considered 'personal information' under section 187LA of the TIA Act.**
- **Law enforcement bodies should be required to notify the Commonwealth Ombudsman as soon as practicable following a decision not to notify an affected individual of a serious data breach under section 26WN of the Privacy Act. This information should be reported annually by the Commonwealth Ombudsman.**

[45] The Privacy Act does not cover some Australian Government agencies involved in law enforcement, intelligence gathering and national security such as The Office of National Assessments and The Australian Security Intelligence Organisation.
[46] *Privacy Act 1988* (Cth) s 26WE.
[47] Ibid, 2 26WN.
[48] Ibid, s 6(1).

The continued effectiveness of the scheme

Effectiveness of data disclosures

55. When the Data Retention Bill was first introduced to the Parliament it was argued the purpose of the regime was to provide for:

> *… [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*.[49]

56. In the annual report of the Department of Home Affairs for 2016-2017, it is stated that over 2016-2017 'enforcement agencies' made 300,224 authorisations for the disclosure of historical telecommunications data. The report says that of these authorisations, 293,069 were made to enforce a criminal law,[50] and were made by the twenty 'criminal law enforcement agencies'. The report states that the majority of offences for which historical data was requested were illicit drug offences, being 71,684 requests, 33,358 requests were made for homicide and related offences and 18,856 requests were made for fraud. However, it is unclear what the remaining 176,326 requests were used for. The report states in 2016-2017 that:

> *law enforcement agencies made 394 arrests, conducted 1064 proceedings and obtained 442 convictions based on evidence obtained under stored communications warrants.*[51]

57. There is no reference to exactly how useful the telecommunications data was in the enforcement of the law. It is also unclear whether a 'proceeding' relates to a criminal prosecution. The annual report of the Department of Home Affairs states only that:

> *Data is often the first source of lead information for further investigations, helping to eliminate potential suspects and to support applications for privacy intrusive investigative tools including search warrants and interception warrants.*[52]

58. The annual report from the Department of Home Affairs lists the total number of authorisations made for enforcement of a law imposing a penalty or protecting public revenue by a criminal law enforcement agency as 2,607 in 2016-2017. It does not state the number that resulted in any enforcement action being initiated as a result of accessing the data.[53]

59. The figures reveal that internally authorised access to data is widespread and common, however it is difficult to assess the extent it is proving to be effective, or indeed truly necessary as an investigative tool, especially in the area of the 'protection of national security'. The available evidence show that the proportion of convictions in 2016-2017, being 442 as compared to the number of times data was accessed, for criminal law enforcement alone, being 293,069, serves to illustrate that the scheme as it presently operates is not necessarily being used to obtain specific evidence that can result in a criminal conviction. However, the Law Council concedes that there can be numerous

[49] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 10.
[50] Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 (Cth) – Annual Report 2016-2017* (Report, 2017) vi.
[51] Ibid.
[52] Ibid 35.
[53] Ibid 38.

authorisations to access data which can relate to one individual and it is difficult to discern the extent to which the authorisations correlate with the specific convictions.

60. The AFP submission to the current review indicates that there were 19,636 instances where there was access to historical telecommunications data in the period from 2017-2018.[54] Of those, 19,432 were made under section 178 of the TIA Act, namely that is was considered reasonably necessary for the enforcement of the criminal law. Of those, 8,200 were for illicit drug offences, 1,672 for terrorism offences and 425 for sexual assault and related offences.[55] It is unclear whether that category includes child sexual exploitation offences.

61. It is clear that the majority of offences for which the data is being obtained are drug related offences, rather than offences relating to national security or child exploitation, and it is difficult to assess whether the offences investigated would be considered as serious crime without further information.

Availability of retained data for unintended purposes

62. The Law Council previously raised concerns about the availability of retained telecommunications data for civil and non-law enforcement purposes.[56] While some of these concerns have been addressed in the legislation, including that data is precluded from being used by civil litigants,[57] there is still the potential for 'function creep' under the regime due to the lack of prescription as to what purpose telecommunications data retained under the regime may be used for, potentially allowing for information collected for one reason to be later used for other purposes.

63. The Committee, when considering the Data Retention Bill, noted that:

> *the proposed data retention regime is being established specifically for law enforcement and national security purposes and that as a general principle it would be inappropriate for the data retained under that regime to be drawn upon as a new source of evidence in civil disputes*.[58]

64. The Committee recommended the Data Retention Bill be amended to include a prohibition on civil litigant access to data retained for the purpose of complying with the mandatory data retention regime. However, the resulting amendment to sections 280 and 281 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) may still have some limitations in their scope.

65. For example, there remains the potential for telecommunications data retained under the scheme to be used in matters of online piracy as telecommunications data may provide an irrefutable download history. Former Attorney-General Brandis and the former AFP Commissioner have stated that the regime will not be used to tackle digital piracy, but should digital piracy offences of individual consumers become criminalised in the future (currently piracy is only a criminal offence when at a commercial scale) it is possible that this position would be reassessed by the Government of the day.

---

[54] Australian Federal Police, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (2019) Table 1.
[55] Ibid Table 4.
[56] Law Council of Australia, Submission No 126 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (20 January 2015) 21.
[57] *Telecommunications Act 1997* (Cth) s 280B.
[58] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 223.

66. The Law Council notes that there is already Australian precedent for the release of customer account information in relation to civil copyright proceedings. In 2015, the Federal Court ordered that the applicant in *Dallas Buyers Club LCC v iiNet Ltd* [59] was permitted to request that iiNet provide the names and contact details of 4,726 customers whose IP addresses improperly shared a digital film file. The court ordered that, what could be considered to be a category of telecommunications data being subscriber information, be disclosed to the applicant to assist in the claim for breach of copyright. This is despite the protection afforded to data retained under the regime to not being used in civil proceedings contained in subsection 280(1B) of the Telecommunications Act.

Potential improvements to oversight

Use of warrants to access to telecommunications data

67. The Law Council considers that access to the telecommunications data by a particular agency should only be accessible by warrant unless the access is strictly necessary due to an emergency situation.

68. In maintaining this position, the Law Council acknowledges that the Committee considered this issue in some detail as noted in its advisory report on the Data Retention Bill. While it is true that the existing powers to access telecommunications data were set out in the TIA Act, including that access could be granted by 'Authorised officers' of enforcement agencies[60] prior to the introduction of the mandatory data retention scheme, the Committee acknowledged that 'in some circumstances access to telecommunications data can represent a significant privacy intrusion'.[61] However, the Committee concluded that the requirement for a warrant process 'would significantly impede the operational effectiveness of agencies and that this would be to the detriment of the protection of the Australian community'.[62]

69. The Law Council understands this is a serious matter to consider, however, maintains that, as there is requirement for a warrant to be issued before access can be permitted to the telecommunications data of a journalist, the same requirement for a warrant should apply in relation to accessing the metadata of all members of the Australian community. The concerns identified by the PJCHR about the chilling effect of access to telecommunications data by government agencies in freedom of expression[63] have equal application to both journalists as well as other members of the community who may provide the information to a journalist or engage in other acts of disclosure considered to be in the public interest.

70. The requirement for approval for access to be granted prior to seeing the data is to ensure there is protective mechanisms so that:

- access to telecommunications data is only permitted when the public interest outweighs the individual's right to privacy;
- is limited to those particular agencies who can establish a legitimate need for access; and

[59] *Dallas Buyers Club LLC v iiNet Ltd* [2015] FCA 317.
[60] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5, 5AB.
[61] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 245.
[62] Ibid.
[63] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Telecommunications (Interception and Access) Bill 2014* (Fifteenth Report of the 44th Parliament, November 2014) 1-70.

- there is not an unjustified intrusion to individual rights, including privacy, and the unauthorised use or disclosure of such information.

71. The Law Council considers that given the extent of information that can be discerned from access to telecommunications data, it is more analogous to 'stored communication' and the requirements to access that information and telecommunications data should be aligned accordingly. In this regard, the Law Council further 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.[64] These existing processes could be extended and applied to access retained telecommunications data for investigation of threats to national security or serious criminal activity.

72. At present, apart from the journalist information warrant provisions, all of the current oversight mechanisms in the TIA Act are directed at reviewing telecommunications data access powers *after* they have been exercised. The Law Council considers that while these are necessary oversight mechanisms, 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.

73. The CJEU found that the EU DRD of 2006 was invalid, partly on the basis that it lacked any requirement of prior review by a court or independent administrative body.[65] In the Tele2 decision, the CJEU reaffirmed the requirement for a mechanism for independent review of the decision to authorise access to telecommunications data prior to the access being granted, in order for a data retention regime to be considered consistent with the *European Charter of Fundamental Rights of the European Union*.[66]

74. The issue of delay previously identified by the Committee can be allayed by requiring a prompt-approval process as is currently the case for emergency warrants issued under the TIA Act.[67] 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 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.

75. 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'[68] as it would not prohibit an agency utilising and pursuing other methods of investigation. 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.[69] The Law Council does not agree that the method of access to retained communications should be the paramount

[64] *Telecommunications (Interception and Access) Act 1979 (Cth)* ss 110, 116.
[65] *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].
[66] *Charter of Fundamental Human Rights of the European Union* [2000] OJ L 364/1.
[67] See, eg, *Telecommunications (Interception and Access) Act 1979 (Cth)* s 10.
[68] Attorney-General's Department, Submission No 26 to the Senate Legal and Constitutional Affairs References Committee, *Inquiry into a Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015) 22.
[69] Ibid.

consideration. Rather, protection and oversight of rights of privacy should be paramount.

Recommendations:

- **Access to retained telecommunications data should be authorised by a warrant issued by an independent court or 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.**

Client legal privilege and confidentiality

76. Client legal privilege is a right for a client of a lawyer to not 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.

77. The Law Council has previously raised concerns with the fact that while 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; and
    - the number of communications and type of communications between a lawyer and a client, witnesses and the duration of these communications.

78. The Law Council acknowledges the previous findings of the Committee that noted evidence from the Attorney-General's Department, that privilege attaches to the content of the communications, and that access to telecommunications data under the regime will not include any such content.[70] However, the Law Council maintains its concerns that a significant amount of information can be inferred from accessing telecommunications data, and that given the particular importance of this information, it warrants additional legislative protection than what is currently provided.

79. The Law Council further notes that while the Committee did not consider that there is a need 'for additional legislative protection in respect of accessing telecommunications data that may relate to a lawyer', [71] in the United Kingdom the Intelligence and Security Committee of Parliament did conclude that the communications of lawyers did justify heightened protection.[72]

80. The concern raised by the Law Council also attaches to the potential situation where the contents of communications, while not required to be retained, may still be retained

[70] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014* (February 2015) 257.
[71] Ibid 257.
[72] Intelligence and Security Committee of Parliament, Parliament of the United Kingdom, *Privacy and Security: A Modern and Transparent Legal Framework* (12 March 2015) 99.

(and disclosed) with other telecommunication data that is mandated to be retained under the scheme, and there is no means by which to identify and prevent this from occurring until after the disclosure is made. The Law Council also notes that the TIA Act does not expressly or impliedly abrogate the right to claim client legal privilege and it is important there be some capacity for this right to be argued and, where necessary, protected.

81. In *Baker v Campbell*,[73] Murphy J emphasised the importance of protecting a client's privacy from the intrusion of the state, noting:

> *the client's legal privilege is essential for the orderly and dignified conduct of individual affairs in a social atmosphere which is being poisoned by official and unofficial eavesdropping and other invasions of privacy.*[74]

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

83. 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 which have been protected to some degree with the introduction of the journalist warrant information provisions.

84. The Law Council wrote to the former Attorney-General, the Hon George Brandis QC when the Bill was under consideration by the Parliament requesting that protecting the confidentiality of the client/lawyer relationship and related communications should, as a minimum, have the same level of protection as journalist's sources. In the correspondence of the Law Council it was argued that adequate safeguards are particularly important, for example, where:

- client legal privilege attaches to a client's identity or contact details which may be revealed by telecommunications data;
- a prosecuting agency can access information revealing how an individual seeks to defend her/himself; or
- whistle blowers seek legal advice prior to, or during, communicating with a journalist.

85. In that correspondence it was noted that in the United Kingdom, it has in fact been held that, in certain circumstances, the telephone number and email address of the relevant client were protected from disclosure by legal professional privilege.[75]

86. The Law Council maintains that it is important 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 where inadvertently, that breaches confidentiality or privilege.

[73] (1983) 153 CLR 52.
[74] *Baker v Campbell* (1983) 153 CLR 52, [116]-[117] (Murphy J).
[75] *JSC BTA Bank v Ablyazoz* [2012] EWHC 1252 (Comm).

Recommendations:

- **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.**

Journalist information warrants

87. When the data retention scheme was introduced in October 2015, a higher threshold was required for access to telecommunications data where the metadata was being sought in relation to a journalist for the purpose of identifying that journalist's source. Division 4C of Chapter 4.1 of the TIA Act sets out the requirements and procedure for a law enforcement agency to apply for a journalist information warrant to be issued. The applications for this type of warrant are also subject to the scrutiny of the Public Interest Advocate.

88. According to the Annual Report of the Department of Home Affairs during the reporting period of 2016-2017, there were no authorisations made for the issue of a journalist information warrant.[76] This is not to say that access was not obtained by a law enforcement agency to metadata pertaining to a journalist. In the 2019 submission of the AFP to the Committee for the current review, it reveals that 58 authorisations were made in the year 2017-2018, yet only 2 journalist information warrants were issued in the same period.[77]

89. On 28 April 2017, the AFP Commissioner, Andrew Colvin APM OAM, held a press conference to disclose that a breach of the TIA Act had occurred within the AFP. The breach occurred within the Professional Standards Unit (**PRS**) and involved access by officers from the AFP to the telecommunications data of a journalist used to identify the journalist's source without a warrant. This breach of the TIA Act was subsequently investigated by the Ombudsman who found there were four discreet authorisations associated with this breach.[78]

90. The report of the Ombudsman stated there were four main reasons for the breach of the TIA Act by the AFP in failing to apply for a journalist information warrant:

    - there was insufficient awareness surrounding the journalist information warrant requirements within the PRS;
    - within the PRS, a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers;

[76] Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 (Cth) – Annual Report 2016-2017* (Report, 2017) 51.
[77] Australian Federal Police, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (2019) Table 7.
[78] Michael Manthorpe PSM, Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979* (October 2017) 3.

- the AFP relied heavily on manual checks and corporate knowledge as it did not have in place strong system controls for preventing applications that did not meet relevant thresholds; and
- the guidance documents were not effective as a control to prevent this breach.[79]

91. The Ombudsman subsequently recommended that the AFP immediately review its approach to metadata awareness raising and training to ensure that all staff involved in exercising metadata powers have a thorough understanding of their responsibilities and obligations under Chapter 4 of the TIA Act.[80]

92. The Ombudsman also observed that 'there is ambiguity surrounding the circumstances of when a journalist information warrant is required' in that if an authorisation was issued for the purpose of identifying a journalist's source, but not made directly in relation to the journalist or their employer, a warrant is not required, even though the information may still reveal the source of the journalist to the AFP.[81]

93. This may serve to highlight a practical difficulty in that without first accessing and examining the telecommunications data, it may not be possible to identify if the data is that of the journalist, their employer or is capable of being used to identify a journalist's source. As with the data retention scheme generally, it is not possible for the journalist, or anybody else, to discover that their data is being accessed unlawfully.

94. The Law Council agrees with the observation made by the Ombudsman that the definition of a 'particular person' for the purpose of subsection 180H(1) of the TIA Act to be either a 'person working in a professional capacity as a journalist' or 'an employer of such a person' is too narrow. Rather the section should focus on the intention of identifying a journalist's source and should include a paragraph that captures 'or any other person whose telecommunications data may reasonably be believed to be used to identify any journalist's source'.

95. The Law Council also considers that the recent use of the new powers conferred by the *Telecommunications (Assistance and Access) Act 2018* (Cth) (**Assistance and Access Act**) by the AFP to execute search warrants on the office of the Australian Broadcasting Corporation and the residence of a News Corporation journalist illustrates that the protection afforded by the journalist information warrant scheme can be easily bypassed. The utility of the provisions in the TIA Act devised to protect freedom of speech and protect journalistic sources has effectively been rendered ineffectual with reforms introduced by the Assistance and Access Act. A search warrant that is executed on a journalist now enables the police, pursuant to the amended section 3F of the Crimes Act to access computers and information that under the Data Retention Act which would require the issuance of a journalist information warrant.[82]

96. In these circumstances, the Law Council considers that the legal protection afforded to journalists and freedom of expression should be strengthened generally and the data retention regime is one area that could benefit from reform, especially given the implications of the Assistance and Access Act.

---

[79] Ibid 2.
[80] Ibid.
[81] Ibid 3.
[82] Josh Taylor, 'Australia's Anti-Encryption Laws Being Used to Bypass Journalist Protections, Expert Says', *The Guardian* (online, 8 July 2019) <www.theguardian.com/australia-news/2019/jul/08/australias-anti-encryption-laws-being-used-to-bypass-journalist-protections-expert-says>.

Recommendation:

- **Section 180H of the TIA Act should be amended to include a paragraph so that a journalist information warrant is required for the authorisation of access to the telecommunications data of any person that may reasonably be believed as being used to identify a journalist's source.**

97. In the 2017 report by the Ombudsman, it was stated that during the inspection 'we identified the role that an external agency played in identifying this breach at the AFP' and 'it was due to a prompt by that external agency that the relevant officer in the AFP reviewed the relevant investigation'.[83]

98. While the external agency was not identified, it raises a question as to how effective the oversight mechanisms for the journalist information warrant scheme are in practice for all the other law enforcement agencies operating under the scheme. It is likely that the issues identified by the Ombudsman in relation to the AFP could have equal application to other law enforcement agencies, particularly as to inadequate training in relation to the obligations imposed on the law enforcement by the journalist information warrant provisions. As stated in the Ombudsman's report:

> *In any large, decentralised agency, there will inevitably be a risk that awareness raising does not reach every officer who is required to be in-the-know. In recognising this risk, all law enforcement agencies that can access metadata have implemented complementary measures to mitigate legislative non-compliance. Unfortunately, the complementary measures adopted by the AFP were not strong enough to prevent this breach from occurring.*[84]

99. In the report of the Ombudsman released in January 2019, it was noted that the while the AFP 'has made progress', the previous recommendation of the Ombudsman from the October 2017 report in relation to PRS staff undergoing additional training in relation to the journalist information warrant provisions was yet to be implemented.[85]

100. The Inspector-General of Intelligence and Security (**IGIS**) also reported that IGIS staff identified a small number of instances in which staff from ASIO retained either telecommunications data or telecommunications interception data that was not relevant to security.[86]

101. There is a range of experience, capabilities and resources of law enforcement agencies authorised to access data under the scheme, and in their capacity to comply with their requirements under the TIA Act. Indeed, the Ombudsman identified various discrepancies between the processes and systems that each agency has in place and their overall compliance with the scheme. In its report on the monitoring of agency access to stored communications and telecommunications data for the period 2015-2016, the Ombudsman found that while agencies at that time were generally attempting to become compliant with the scheme, the (then) Department of Immigration and Border Protection (**DIBP**) was non-compliant and did not have sufficient processes in

[83] Ibid.
[84] Ibid 18.
[85] Michael Manthorpe PSM, Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979* (October 2017) 1.
[86] Inspector-General of Intelligence and Security, *Annual Report 2017-18* (24 September 2018) 23.

place for the Ombudsman to determine whether the DIBP was lawfully dealing with stored data.[87]

102. In its report on the monitoring of agency access to stored communications and telecommunications data for the period 2016-2017, the Ombudsman noted that DIBP had not implemented the Ombudsman's previous recommendation for a centralised record keeping system and advised that the risks previously identified in relation to DIBP's record keeping practices had not been addressed.[88] In that report, the Ombudsman made two formal recommendations to the Department of Home Affairs (which replaced DIBP), for improved storage practices and processes, and for accurate accounting of authorisations made.

103. While the Law Council notes the Ombudsman provides a level of oversight over law enforcement agencies' use of the scheme, its approach is retrospective – it assesses compliance once agencies have used their relevant access powers. The Ombudsman has recognised that a 'person who has been subject to the powers will not be aware of the fact, and therefore, will not be in a position to make a complaint'.[89] The covert nature of agencies' access powers tends to corrode a person's right to obtain a remedy, noting they are almost always unaware any intrusion has occurred.

104. In the recent case of *Big Brother Watch v The United Kingdom*,[90] the European Court of Human Rights (**ECHR**) considered whether certain aspects of a mass surveillance regime being applied in the United Kingdom were unlawful due to their inconsistency with the right to privacy and the right to freedom of expression under the *European Convention on Human Rights* (**the Convention**).[91] One of the issues addressed was the lawfulness of obtaining communications data from communications service providers. The court held that the scheme in this regard was incompatible with the Convention because it's use was not limited to combatting 'serious crime' and its use was not subject to prior review by a national authority. The court held that:

> *since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her own rights.*[92]

105. In these circumstances, the court held the scheme violated the Convention due to the 'absence of robust independent oversight'.[93]

---

[87] Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2015 to 30 June 2016* (Report, March 2017) 30 <www.ombudsman.gov.au/__data/assets/pdf_file/0018/45423/TIA-Act-Annual-Report-2015-16.pdf>.
[88] Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2016 to 30 June 2017* (Report, November 2018) 33 <www.ombudsman.gov.au/__data/assets/pdf_file/0033/96747/201617-Chapter-4A-Annual-Report.pdf>.
[89] Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979: For the Period 1 July 2015 to 30 June 2016* (Report, March 2017) 1.
[90] *Case of Big Brother Watch and Others v The United Kingdom* (European Court of Human Rights, Chamber, Application Nos 58170/13, 6322/14 and 24960/15, 13 September 2018).
[91] *Convention for the Protection of Human Rights and Fundamental Freedoms,* opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953). Article 8 provides for the right to respect for private life and art 10 the right to freedom of expression.
[92] *Case of Big Brother Watch and Others v The United Kingdom* (European Court of Human Rights, Chamber, Application Nos 58170/13, 6322/14 and 24960/15, 13 September 2018) [309].
[93] Ibid [347].

106. The Law Council considers that in the Australian context, the existence of instances of non-compliance discussed above serve to justify the reasoning applied by the ECHR in *Big Brother Watch*. The fact there have been instances of non-compliance with the requirements of the existing legislation illustrate the need for tightening of the legislation to ensure that the fundamental human right to privacy is afforded greater protection by the provision of more effective procedural safeguards.

Security of retained data

107. The legislation does not require service providers to retain the telecommunications data within Australia and there is little by way of regulatory obligations as to the security of the data. It is foreseeable that service providers will want to find the cheapest data retention solutions as service providers are a business designed to maximise profit, especially where the service providers already have to pay costs associated with compliance with the legislation. As was stated in the Explanatory Memorandum to the Data Retention Bill, the implementation plan process was partly intended to 'allow service providers to develop and implement more cost-effective solutions to their data retention obligations'.[94] As there is no requirement to retain the stored data within Australia, it may increase the risk that data could be stolen or hacked as there is no capacity for effective oversight by the Australian media authorities such as the ACMA.

108. The Law Council notes the Telecommunications Sector Security Reforms (**TSSR**) which commenced on 18 September 2018, and the intention of the amendments to the Telecommunications Act 1997 to create a regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities and impose a requirement that carriers and carriage service providers 'must do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access'.[95] Subsection 313(1A) of the Telecommunications Act now imposes a statutory obligation on a carrier or provider of carriage services to 'protect telecommunications networks and facilities' so as to ensure the confidentiality of communication and information contained on those networks and facilities. However, the phrase 'do the carrier's best' lacks precision or definition as to what the minimum objective standards are to be considered acceptable to achieve the aims of the TSSR.

109. Given the lack of prescribed objective standards, the Law Council remains concerned that offshore storage is still permitted under the mandatory data retention regime. Where data is stored overseas it is essentially governed by the host country's legislative system. Foreign laws apply and can have extra-territorial application to the telecommunication service provider itself, potentially enabling foreign governments to legally access the telecommunications data. Secondly, offshore storage necessarily involves contracting with external foreign parties, which further heightens the risk of a data breach.

110. The Law Council notes that the CJEU held the EU DRD of 2006 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.[96]

---

[94] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 35.
[95] *Telecommunications Act 1997*(Cth) s 5.
[96] *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].

111. While the legislation requires the service provider to protect the confidentiality of information that is retained by encrypting the information and protecting the information from unauthorised interference or access,[97] there is no specific detail as to the minimum standards by which these aims are to be achieved or the type of encryption that is to be utilised.

112. The utility of encryption as a means of protecting privacy has also been undermined by the amendments to the Telecommunications Act introduced by the Assistance and Access Act which enables Australian law enforcement agencies to access the content of end-to-end encrypted information. There may also the ability for this to occur in foreign countries that have enacted similar legislation. For example, India recently passed amendments to enable law enforcement to compel the decryption of data by internet service providers and there are in excess of twenty countries throughout the world that have enacted similar legislation to enable law enforcement agencies to access encrypted data.[98]

113. The Law Council considers that minimum standards for the security of retained data should be developed. Entities subject to mandatory telecommunications data retention requirements under the TIA Act should be required to demonstrate to the ACMA that they have met minimum standards for ensuring the security of retained telecommunications data, including a minimum national standard of encryption to be applied by industry. In this regard, the Law Council notes that the Commonwealth Scientific and Industrial Research Organisation is currently developing a set of minimum standards in relation to the use of AI, taking into account the ethical implications of the increasing use of AI in industry.[99]

114. Security of data is of concern, particularly as hacking capabilities have become increasingly sophisticated and governments and large corporations have been unable to protect themselves against sophisticated attacks on their stored information. These attacks may be mounted by state actors or sophisticated criminal groups.[100] In these circumstances, the dangers of maintaining such large telecommunications data sets, even in encrypted format, are significant, and pose an attractive target to would-be attackers.

115. The Law Council considers there should be a legislative requirement for law enforcement and security agencies to de-identify telecommunications data containing personal information, which is irrelevant or no longer required by the agency, within a prescribed time limit.

116. The Law Council considers that information in relation to how telecommunications data is stored, encrypted and disposed of should be made available to the public so that there is greater transparency in these key requirements of the scheme.

Recommendations:

- **Government agencies that have access to telecommunications data should develop minimum standards for the security of**

[97] *Telecommunication (Interception and Access) Act 1979* (Cth) s 187BA.
[98] Global Partners Digital Limited, *World Map of Encryption Laws and Policies* (Web Page) <www.gp-digital.org/world-map-of-encryption/>.
[99] See CSIRO, *Artificial Intelligence: Australia's Ethics Framework* (Discussion Paper, 2019) h <https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf>.
[100] See eg, N Mckenzie and A Grigg, 'Australia's Defence Department was Badly Exposed to China's Hackers', *Sydney Morning Herald* (online, 29 November 2018) <www.smh.com.au/politics/federal/australia-s-defence-department-was-badly-exposed-to-china-s-hackers-20181129-p50j48.html>.

telecommunications data and put them forward for consideration and approval of the Committee.

- **Entities subject to telecommunications data retention requirements under the TIA Act 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.**

International developments since the introduction of the data retention scheme

117. Due to developments in technology that enable the cost-effective storage and processing of large data sets, the broad, state-based surveillance of members of a population has increased globally. The trend towards mass, indiscriminate surveillance has, however, been met with increasing opposition.

118. In particular, the Law Council notes the abovementioned Tele2 decision, where the CJEU found that, to be consistent with privacy rights, any law concerning metadata retention must limit the categories of data to be retained, the means of communication affected, the persons concerned, and retention period adopted. Following this decision, the Irish Government commissioned the former Chief Justice of Ireland, John Murray, to review its current telecommunications data retention legislation. That report was released on 4 October 2017, finding that the Irish data retention regime breached European law and amounted to mass surveillance of the entire population of the Irish State.[101] The scheme in Ireland, much like in Australia, enabled police and other state authorities to access telecommunications data with a disclosure request and without judicial oversight. The report stated the statutory framework was indiscriminate in application and scope and was being implemented without the consent of those affected.[102]

119. In the 2016 decision in *Big Brother Watch v The United Kingdom*,[103] the ECHR considered a challenge to three different systems of mass surveillance adopted by the United Kingdom's intelligence services. Relevantly, the ECHR found the regime for obtaining communications data from communications service providers was not limited to combatting 'serious crime', was not subject to prior review by a national authority and did not sufficiently protect journalists' confidential communications. The Court held the regime was therefore in breach of the *European Convention on Human Rights*.

120. Finally, in the United States, the National Security Agency (**NSA**) to have extensive powers to collect telephone records and telecommunications data.[104] While the *Privacy Act 1974* (US) (**US Privacy Act**) imposes certain standards on federal agencies when

[101] Sarah Bardon, 'Irish Data Law Amounts to Mass Surveillance, Says Ex-Chief Justice', *Irish Times* (online, 3 October 2017) <www.irishtimes.com/news/politics/irish-data-law-amounts-to-mass-surveillance-says-ex-chief-justice-1.3243354>.
[102] Justice John Murray, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) <www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf>.
[103] *Case of Big Brother Watch and Others v The United Kingdom* (European Court of Human Rights, Chamber, Application Nos 58170/13, 6322/14 and 24960/15, 13 September 2018).
[104] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub L No 107-56, 2001, 115 Stat 272.

collecting, maintaining and using personal information, it does not apply to records created or held by intelligence agencies, meaning a number of sources of information do not fall within the ambit of the US Privacy Act

121. However, the United States Congress has since enacted legislation to try and restore some protection to the right to privacy afforded to American citizens by the US Privacy Act via the *Freedom Act 2015* (US) (**Freedom Act**).[105] While the Freedom Act imposed some new limits on the bulk collection of telecommunications data on US citizens by American intelligence agencies, it has been argued that the Freedom Act does not go far enough in curtailing the existing surveillance programs.[106]

122. The Freedom Act does prevent the mandatory retention and collection of telecommunications data by telecommunications carriers for the use of US government agencies. However, government agencies can access the voluntary retention of telecommunications data by commercial telecommunications companies is by seeking access through the *Electronic Communications Privacy Act* 1986 (US) (**ECPA**) which enables law enforcement to obtain information on telephone calling patterns without a warrant to investigate particular offences prescribed in the ECPA.

[105] *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015,* Pub L No 114-23, 129 Stat 268.
[106] See 'Surveillance Reform Bill Returns with Concessions to NSA On Data Collection', *The Guardian* (online, 24 April 2015) <www.theguardian.com/world/2015/apr/23/usa-freedom-act-revised-senate-bill-nsa>.