Access to Retained Data in Civil Proceedings

Submission to the Attorney-General's Department and the Department of Communications and the Arts

27 January 2017

Communications Security Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Contact: Emily Ryan
President, NSW Young Lawyers

Richard Prangell
Chair, NSW Young Lawyers Communications, Entertainment and Technology Law Committee

Contributors: Irene Halforty, Steven Mulhall, Ruthushan Muttusamy, Ravi Nayyar, Quyen Nguyen, Jacqueline Serkowski, Shariqa Shaheed, James Wood and Karen Zhong

NSW Young Lawyers
Communications, Entertainment and Technology Law Committee
170 Phillip Street
Sydney NSW 2000
ylgeneral@lawsociety.com.au
www.younglawyers.com.au
NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 16 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Communications, Entertainment and Technology Law Committee (Committee) of NSW Young Lawyers aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice); intellectual property; advertising and consumer protection; confidential information and privacy; entertainment; and the media. As innovation inevitably challenges custom, the Committee promotes forward thinking, particularly about the shape of the law and the legal profession as a whole.
Summary

Legislative Background
1. The metadata retention regime was introduced by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (*2015 Amendment*) to counter threats to national security and serious crime.

2. Metadata is any data that describes and gives information about a communication. Collected metadata is highly descriptive of the behaviours of individuals.

Standard of Proof
3. Civil proceedings require a substantially lower standard of proof than is required in criminal proceedings. The proliferation of metadata in this context may lead to a miscarriage of justice.

Question 1
4. There are no reliable records or reported instances of civil litigants requesting access to metadata under the metadata retention regime.

5. The Committee expresses concern that while there exist a number of cogent matters that the Minister must consider when declaring a government authority an ‘enforcement agency’ under the existing regime, the Minister’s statutory discretion to make exceptions for civil litigants is largely unfettered.

Question 2
6. Civil proceedings cannot be adversely impacted by a prohibition from accessing metadata which has not previously existed.

7. Public support for the 2015 Amendment was afforded on the basis that retained metadata would be used for the purpose of serious criminal investigations, and not for civil matters.

8. The Committee has concerns with respect to the privacy of individuals, and other unintended consequences, arising out of the proliferation of metadata in civil proceedings.

9. Expense in collecting and storing metadata will substantially increase should that data become the subject of subpoenas or other court orders in civil proceedings.

Question 3
10. Due to the limited consultation period for these issues, the Committee cannot provide a comprehensive analysis of classes of matters in which the use of retained data would be appropriate.

11. An exception to the prohibition against access to metadata in civil proceedings should not be made for the purposes of enforcing copyright infringement, on the grounds that the retained data may establish a target for “fishing expeditions” by rights holders.

Conclusion
12. The Committee is of the view that it is inappropriate for retained metadata to be accessed and used in civil proceedings.
Introduction

1. The Committee welcomes the opportunity to provide the Attorney-General’s Department and the Department of Communications and the Arts (collectively the Departments) with its views in relation to the use of retained data in civil proceedings, and more particularly the Departments’ review of the prohibition and regulation-making power under the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act).

2. Due to the limited consultation period, the Committee has not been able to undertake a comprehensive review of the prohibition and regulation-making powers under the TIA Act. Consequently, this submission does not intend to present a comprehensive review of the issues and concerns raised by the Departments’ questions in the Consultation Paper, but provides an outline of key issues that the Committee submits require further consideration and consultation. Given the potential impact of expanding access to the retained data for use in civil proceedings, the Committee is of the view that the Departments would benefit from extended consultation with key stakeholders and experts on the issues raised.

3. For a number of reasons, the Committee is of the view that there should be a strong presumption against expanding access to the retained data under the TIA Act in civil proceedings. These include the overriding purpose of the legislation; the disproportionate impact on the privacy of individuals; the significant transparency issues present in the current legislative framework and the potential for unintended consequences.

4. The Committee is also of the view that extensive data collection and retention for law enforcement purposes does not necessarily equate to pervasive surveillance and monitoring of individuals.

Overview of the Telecommunications (Interception and Access) Act 1979 (Cth)

Legislative History

5. The law of telecommunications interception was developed to protect the expectations of confidentiality between individuals’ communications and provided a reasonable expectation that communications would not be monitored and reported to others without consent. Judicial oversight provided an important and necessary checkpoint to balance the expectations of confidentiality with public interest.

6. Contextual information regarding communications (or rather, information about communications) was historically considered ‘less sensitive’ and consequently the procedures that permitted lawful access to this information were less demanding compared to the warrants regime for interception of
communication content. However, rapid advancement in communication technologies has changed the way in which we communicate to such an extent that the information about communications assembles a rich picture of each person’s solitary and social life.\(^2\) As noted by Peter Leonard:

> What people do, where they do it and who they do it with, has become more easy to ‘read’ through observing electronic data that surrounds them than by physical surveillance. […] It should therefore not be surprising that what an individual does, where that individual did it and who with, is often much more valuable to intelligence and law enforcement agencies than what that individual said.\(^3\)

7. In 2012, with the aim to modernise telecommunications law, the Government introduced an amendment to the TIA Act. Given a ‘domestic preservation notice\(^4\)’ or ‘foreign preservation notice\(^5\)’ issued by specified classes of agencies, ‘certain stored communications\(^6\)’ contained on ‘equipment operated by or in possession of an Australian carrier or carriage service provider\(^7\)’ had to be preserved.

8. In 2015, the Government established a data retention regime by enacting the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (the 2015 Amendment). This legislation represents the “most far-reaching data collection and retention requirements among advanced industrialised democracies imposed upon telecommunications service providers.”\(^8\) It is unique in mandating blanket collection and retention of data of specified categories, not tailored to specific requests,\(^9\) and in breaking from previous laws giving service providers discretion to collect and retain data.\(^10\)

9. Importantly, the 2015 Amendment provides a clear limitation as to who can access the retained data and for what purposes. Firstly, only ‘criminal law enforcement agencies’ as defined by s 110A – not ‘enforcement agencies’ as defined by s 176A – of the TIA Act may access and require preservation of

---


3 Ibid 10-11.

4 Leonard, above n 2, 46.

5 Ibid 47.

6 Ibid.

7 Ibid 43.

8 Leonard, above n 2, 43.

9 Ibid 46.

10 Ibid.
stored communications as defined by s 5 of the TIA Act. This careful limiting of the number of agencies is justified by the "intrusive nature of warrants that authorise access to stored communications."  

10. Secondly, the definition of 'enforcement agency' in the TIA Act was amended, replacing s 5 of the TIA Act. It now includes criminal law enforcement agencies, and 'any authority or body' that has been declared an enforcement agency by the Commonwealth Attorney-General under s 176A(3) of the TIA Act. The new definition is in contrast with the prior open-ended laws enabling agencies 'with functions concerning the enforcement of laws administering a pecuniary penalty or protection of the public revenue' to authorise the 'disclosure of telecommunications and seek stored communication warrants'. Notably, the 2015 Amendment did not increase the access of agencies to the retained data.

Legislative Context

11. The Committee is of the view that any proposed amendments to the TIA Act that seek to extend access to the retained data must not be made without thorough consultation given the context in which, and the surrounding debates with which, the TIA Act and the 2015 Amendment were introduced and passed.

12. A central aspect to the debate surrounding the enactment of the TIA Act and the 2015 Amendment was the need to balance the privacy of individuals with law enforcement and national security needs. The 2015 Amendment is viewed as being the third tranche of national security reforms introduced in 2014, in response to the perceived threat of home-grown terrorism and the security risks posed by terrorists returning to Australia. The need for the

---


15 Ibid.


Government to carefully balance its data retention needs with individual privacy remained a major public concern. It was in this context that the 2015 Amendment restricted access to the retained data to criminal law enforcement agencies and provided for the retention of only the data "necessary for the investigation of serious criminal offences and national security threats."\(^\text{19}\)

13. The Committee recognises the complexity of the “privacy versus security” debate in covering “an expanding variety of public agenda issues.”\(^\text{20}\) These include “counter terrorism, use of telecommunications data, aerial drones, biometrics, the e-health system, downloadable apps, and credit regulation.”\(^\text{21}\)

14. Proponents of data retention emphasise the goals of the regime as ensuring national security and assisting with the enforcement against serious criminal activity,\(^\text{22}\) and assert that retained data is vital for “virtually every counter-terrorism, organised crime, counter-espionage and cyber-security investigation, as well as almost every serious criminal investigation.”\(^\text{23}\)

15. However, the Committee is not aware of any statistical evidence in an Australian context that supports the view that the data retained pursuant to the 2015 Amendment serves a critical role in successful criminal investigations.\(^\text{24}\) There is evidence that Australia’s pre-2015 data retention arrangements were adequate from a law enforcement perspective.\(^\text{25}\) The Committee notes that Germany’s experience is illustrative as following the introduction of its metadata retention regime there was an increase of only 0.006% in criminal convictions. Considering the lack of statistical evidence to support the necessity of wide scale collection of metadata in securing convictions for serious criminal offences, the Committee is concerned that the data retention regime ‘cement[s] a place for a mass surveillance regime’,\(^\text{26}\) that ignores the ‘necessity or proportionality to the investigation and resolution to serious criminal activity’.\(^\text{27}\)

\(^{19}\) Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 12.


\(^{21}\) Ibid.

\(^{22}\) Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 5.

\(^{23}\) Ibid.


\(^{25}\) Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 29 January 2015, 31 (Peter Leonard’).


\(^{27}\) Ibid.
16. The lack of necessity and proportionality, when balanced against the expectation of individuals of privacy, is a concern amongst most liberal democracies who have implemented data retention regimes similar to Australia’s. A recent decision by the Court of Justice of the European Union ruled that the general and indiscriminate retention of data is contrary to the European Union’s laws, because it disproportionately interfered with fundamental rights and that “only the objective of fighting serious crime is capable of justifying such interference.”\(^{28}\)

17. The Committee believes that individual privacy is an essential ingredient “of one’s humanity, of one’s human dignity [and] autonomy.”\(^{29}\) The data retained pursuant to the 2015 Amendment can be particularly revealing\(^{30}\) of individuals’ solitary and social life.\(^{31}\) The inferences about a person that are capable of being drawn from the metadata are so significant that security services regard such information as more valuable than the content of communications:

> The real story of our lives is now not in what we say, but what we do, as potentially disclosed through analysis of information about electronic communications.\(^{32}\)

### Legislative Purpose

18. The Committee accepts that the data retention regime introduced by the 2015 Amendment was aimed at bolstering the capabilities of law enforcement and intelligence communities to counter threats to national security and serious crime,\(^{33}\) including new threats of internet facilitated terrorism, human trafficking and child exploitation.\(^{34}\) The 2015 Amendment was designed and implemented with the aim to provide law enforcement agencies with the tools to counter the erosion of its enforcement activities as the result of the emergence of communication technologies that enabled serious criminals and terrorists to evade detection.\(^{35}\) This is supported by the fact that the duration period for the data retention “is based (in part) on the advice of our law enforcement and security agencies.”\(^{36}\)

---


\(^{29}\) Michael Fraser, ‘A Right to Privacy? Comments as Part of a Discussion on Data Collection / Surveillance’ [2016] (83) *AIAL FORUM* 83, 83.

\(^{30}\) Williams and Hardy, above n 18, 70.

\(^{31}\) Leonard, above n 3, 10-11.

\(^{32}\) Leonard, above n 2, 47.

\(^{33}\) Commonwealth, Parliamentary Debates, House of Representatives, 30 October 2014, 12560 (Malcolm Turnbull).

\(^{34}\) Leonard, above n 3, 3.

\(^{35}\) PJCIS Advisory Report, above n 13, 69.

\(^{36}\) Commonwealth, Parliamentary Debates, House of Representatives, 30 October 2014,
19. Furthermore, the language of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (PJCIS Advisory Report)*, as well as the submissions of Government agencies, indicate the primacy, in terms of policy reasoning, of the utility of retained data for achieving national security goals.

20. The Committee reiterates the comments of the PJCIS that it is inappropriate for retained data to be accessed and used in civil proceedings. The proposed amendment to s 280(1B) of the TIA Act not only detracts from the law enforcement and national security purposes of the TIA Act and the 2015 Amendment, but provides for an entirely new purpose altogether. In the words of Senator Nick Xenophon:

> This is not so much a case of mission creep as a new mission altogether and many would see these metadata laws as being a Trojan horse for incursions that were never contemplated when this legislation was debated two years ago.

21. The Committee submits that extending access to the retained data under the TIA Act to civil proceedings would be poor policy given the problems already surrounding the data retention regime, including the legislation’s existing internal inconsistencies and lack of clarity.

22. The Committee also submits that the wide scale collection of metadata for use in civil proceedings would be “an unjustified infringement on human rights.” Unlike with matters pertaining to national security and the enforcement of serious crimes, it would be extremely difficult to justify the wide scale collection of metadata for use in civil proceedings. This conclusion is inescapable because the wide scale collection of metadata for use in civil proceedings is entirely disproportionate to the purpose of collection, and ignores the need to delicately balance public interest with the privacy of individuals.

23. It is unclear how the Government intends to balance the privacy of individuals with the private interests of parties to civil proceedings. The Committee questions whether this balancing exercise can be undertaken with respect to extending access to the retained data under the TIA Act for use in civil

---

37 PJCIS Advisory Report, above n 13, 223.

38 Ibid.


41 This is a view shared by the Victorian Commissioner for Privacy and Data Protection. See: PJCIS Advisory Report, above n 13, 50.
proceedings as there is no purported ‘public benefit or interest’ which the proposed amendment seeks to protect. The interests of parties in civil proceedings are by their nature, private, and not public.

24. In this regard, the Committee notes the Australian Privacy Commissioner’s warning that blanket data retention risks the misuse of the collected data, ‘such as through inappropriate access or the risk of identity theft and fraud’. The Committee is of the view that these flaws in the regime must be rectified before there is any consideration of extending access to the retained data for use in civil proceedings.

What is ‘metadata’?

1. Broadly, metadata can be defined as a set of data that describes and gives information about other data. However, this is too inaccurate to describe what metadata is for the purposes of the proposed changes to the metadata retention legislation.

2. The kinds of data that service providers in Australia are currently required to keep can be found in s 187AA of the TIA Act. The Committee is of the view that missing from the list found in s 187AA of the TIA Act is the actual content of the communication. For the purposes of metadata retention legislation, metadata is all the data needed to identify who a person communicates with, how long they communicate for, what they look at online and where they are, every single time they use an electronic device with either a data or cellular connection.

Standard of Proof

1. It is worth noting the distinction between the standard of proof in civil matters and the standard of proof in criminal matters. The weight that metadata is given will be a matter for the Court in each circumstance. However, the Committee notes that the data is limited to the nature of evidence it provides. For example, metadata could establish that a particular device made a communication at a particular time. However, the metadata cannot itself prove the identity of the person using the device at the time the metadata was created. While an obvious assumption may be that the owner of the device had use of it, this will not always be the case

2. For this reason, the Committee submits that in the absence of corroborative evidence, metadata on its own is unlikely to be sufficient to prove the existence of a fact on the balance of probabilities.

3. In the absence of other evidence, the evidence provided by metadata is unlikely to meet the high standard of proof required in criminal proceedings, being “beyond reasonable doubt”.

---

42 Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 29 January 2015, 46 (Timothy Pilgrim).

43 https://www.merriam-webster.com/dictionary/metadata
The Australian Privacy Principles and the TIA Act

1. The Australian Privacy Principles (the Privacy Principles), contained in Schedule 1 of the Privacy Act 1988 (Cth) (Privacy Act), provide guidelines on how most Australian government agencies and private organisations with an annual turnover exceeding $3 million must use and manage personal information. The Privacy Principles place obligations on Government to consider the open and transparent management of personal information, for individuals to have a choice of transacting anonymously or using a pseudonym where practical, and the giving of a notice of collection for personal information.

2. The Committee is of the view that strict adherence to the Privacy Principles is essential as they serve as one of the only protections of the privacy of individuals. The Committee notes that Australia is still one of the only advanced countries in the world without a tort for the serious invasion of privacy, and the Australian Law Reform Commission has consistently recommended the introduction of a general right to privacy. \(^{44} \,^{45}\)

3. The Australian Privacy Principle3 (APP3) from the Privacy Act states:

   the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity’s functions or activities.

4. By definition, the data required to be retained under the metadata retention scheme is "personal information"\(^{46}\) and should be treated in accordance with APP3. However, there are broad exemptions from the application of APP3, including where agencies are required by law or for law enforcement purposes to collect the personal information.

5. Whereas the broad exemption from the application of APP3 can generally be accepted on the basis of public interest, the Committee questions whether the exemption is appropriate for the retention of metadata for use in civil proceedings.

Question 1

In what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act?

1. To the Committee’s knowledge, there are no reliable records or reported instances of civil litigants requesting access to the data set outlined in s 187AA of the TIA Act. The Committee has therefore considered whether


\(^{46}\) Telecommunications (Interception and Access) Act 1979 (Cth), s 187LA.
there are circumstances within the current framework in which civil litigants could request this data.

**Rationale for limiting access for civil litigants**

2. The purpose of the restriction was to limit the use of retained data to criminal proceedings for the following reasons:

   Subsections 280(1B) and 281(2) and (3) [of the Telecommunications Act 1997 (Cth)] strictly limit the circumstances in which a service provider may disclose data that has been retained for the purpose of Part 5-1A in relation to or as part of civil litigation. This measure engages the right to a fair hearing, specifically the principle of equality of arms because it has the potential to affect procedural fairness in terms of the general conduct of the proceedings and the nature and quantum of evidence capable of being adduced by the parties and available for the court's deliberative processes.  

3. Notwithstanding this, there are circumstances in which the data could be accessed by civil litigants despite the recommendation of the PJCIS to narrow the restriction. A regulation-making power was included in the TIA Act ‘to enable [a] provision for appropriate exclusions such as family law proceedings relating to violence or international child abduction cases’.  

4. The basis for this exemption was to ensure that the legitimate rights and interests of civil litigants were not adversely affected in such circumstances where the law would “constitute an additional ex ante barrier to mounting or defending a claim”. The Attorney-General’s Department also observed that it may assist other circumstances like ‘civil child protection investigations, apprehended violence orders and actions involving incidents of stalking and harassment, which often involve the use of a carriage service’.  

5. While there are some cogent reasons that the data should be accessible to civil litigants, it is the view of the Committee that these perceived benefits are outweighed by the associated risks.

**The current framework for access**

6. The kinds of telecommunications data listed in s 187AA of the TIA Act that service providers must keep or cause to be kept, largely relate to data pertaining to an individual subscriber’s identity as gleaned from their IP address.

7. Under the TIA Act, it is an offence for service providers to disclose this data other than to authorised officers of an ‘enforcement agency’.  

---

47 Ibid [166].
48 PJCIS Advisory Report, above n 13, 223 [6.117].
49 Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, [168].
50 PJCIS Advisory Report, above n 1 3, 222 [6.111].
51 Telecommunications (Interception and Access) Act 1979 (Cth) s 177.
‘enforcement agency’ is either:

(a) a criminal law-enforcement agency (which includes a closed list of organisations: the Australian Federal Police, a Police Force of a State, the Australian Commission for Law Enforcement Integrity, the Immigration and Border Protection Department (for certain functions), the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission (‘ACCC’), the Crime Commission, the Independent Commission Against Corruption, the Police Integrity Commission, the IBAC, the Crime and Corruption Commission, the Corruption and Crime Commission, the Independent Commissioner Against Corruption); or

(b) an authority or body which has been declared by the Minister to be included within this definition.

8. The Committee notes that the prohibition contained in s 280 of the Telecommunications Act 1997 (Cth) (Telecommunications Act) for the use of data retained pursuant to the TIA Act in civil proceedings only applies to data retained solely for the purpose of complying with the TIA Act. Consequently, where service providers retain metadata as business records in addition to compliance with the TIA Act, the metadata may be accessible for use in civil proceedings through the process of discovery.

9. The Committee notes the following issues that could arise from the ability of the Minister to declare an authority or body as being an enforcement agency.

The Minister’s declaration-making power

10. There are certain factors that the Minister must take into account when declaring whether a body or authority is an ‘enforcement agency’. Some factors include whether the body or authority is seeking to enforce criminal law, a pecuniary penalty or protect public revenue, the degree of compliance with the Privacy Principles, or whether making a declaration is within in the public interest.

11. However, the Minister’s statutory discretion is largely unfettered. It is therefore conceivable that agencies such as local councils and the Australian Taxation Office could be granted access to the data, despite their purposes being at odds with the legislative purpose of ensuring national security. In addition, there is a risk that authorities declared as enforcement agencies are shielded from parliamentary scrutiny.

12. The Committee notes that prior to the enactment of the 2015 Amendment, 293,501 requests were made by law enforcement agencies other than the

---

52 Telecommunications (Interception and Access) Act 1979 (Cth), s 110.
53 Telecommunications (Interception and Access) Act 1979 (Cth), s 176A.
54 Telecommunications (Interception and Access) Act 1979 (Cth), s 177.
55 Telecommunications (Interception and Access) Act 1979 (Cth), s 176A(3B).
56 Telecommunications (Interception and Access) Act 1979 (Cth), s 176A(4)(c).
57 Telecommunications (Interception and Access) Act 1979 (Cth), s 176A(4)(c).
Australian Security Intelligence Organisation (ASIO) in 2011 - 2012 for telecommunications data “without a warrant or any judicial oversight.” The Committee also notes that a partially redacted response to a Freedom of Information Request in January 2016 revealed that at least 61 authorities had applied to be declared law enforcement agencies to obtain this data.

13. At the time of writing this submission, the Committee is not aware of any Ministerial declarations being made. The Committee considers this is problematic as parties who are permitted access to this data are not listed in the primary statute but are 'buried' in a legislative instrument. In addition, for the reasons below, the Committee is unable to ascertain the precise number of non-criminal enforcement agencies that have been granted access to this data.

Lack of transparency

14. The Committee is of the view that there is limited oversight as to how metadata is accessed and used by entities characterised as law enforcement agencies. The Committee notes the attempts by other government departments to access the data retained pursuant to the TIA Act by requesting law enforcement agencies to obtain the metadata. As such, the metadata could be used by any enforcement agency that successfully requests the information from criminal law enforcement agencies.

15. The extent to which enforcement agencies would be able to use the data retained under the TIA Act in civil proceedings cannot be accurately measured.

16. Although the Commonwealth Ombudsman is tasked with conducting internal audits of certain agencies acquiring this data, this auditing process would only apply to some enforcement agencies.

17. The Committee submits that there are still significant transparency issues present in the current legislative framework and recommend that these issues be resolved.

Question 2

What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?


61 Ibid.
Impact on Civil Proceedings

1. The Committee notes that s 280(1B) of the Telecommunications Act has the effect of prohibiting the disclosure in civil proceedings of data, which is kept by service providers solely for the purpose of complying with Part 5-1A of the TIA Act (as amended by the 2015 Amendment) (i.e. the mandatory data retention regime). Importantly, it does not prohibit the disclosure of data retained by service providers for business purposes (e.g. billing or load management).

2. Data retained by service providers for business purposes has previously been available to civil litigants pursuant to court processes. Paragraphs 401 to 403 of the Explanatory Memorandum to the 2015 Amendment make it clear that such access continues in spite of s 280(1B). Conversely, material that is held by service providers solely for the purpose of the metadata retention regime has never been available in civil proceedings, because it has, by definition, not previously been retained.

3. The Committee submits that civil proceedings cannot be adversely impacted by litigants being prohibited from accessing evidence which has not previously existed. This consultation is concerned, in reality, with an expansion of the scope of evidentiary material available to civil litigants, rather than the imposition of some novel restriction.

4. The Committee is therefore of the view that there should be a strong presumption against expanding access to mandatorily retained metadata in any civil proceedings.

Grounds for Introduction

5. The 2015 Amendment was introduced for the purposes of assisting law enforcement. Public statements by the Attorney-General and the Commissioner for the Australian Federal Police made this clear:

   "The mandatory metadata retention regime applies only to the most serious crime — to terrorism, to international and transnational organised crime, to paedophilia, where the use of metadata has been particularly useful as an investigative tool … Civil wrongs have got nothing to do with this scheme."

And:

   "I want to be very clear on this. The Government's introducing this to address vital needs of national security and law enforcement, not copyright. Copyright is essentially a civil matter. This is about criminal matters. So we will be using it for criminal matters. The Telecommunications Intercept Act makes it very clear that we can only do this to enforce criminal laws. Copyright breaches are civil wrongs and that's not what we're interested in."

6. As such, it is apparent that legislative justification for the 2015 Amendment

---


was on the basis that retained metadata would be used for the purpose of serious criminal investigations, and not to support civil proceedings.

7. The Committee is concerned over the implication to be derived from the recent removal of the FAQ section dealing with the use of metadata for copyright enforcement from the Attorney-General’s Department website:

Source: Electronic Frontiers Australia

Nature of Data Retained

8. Secondly, the data retained under the scheme is of a personal nature, potentially revealing who a person has contacted and when, the person’s location and movements over time, and the person’s activities on the internet.

9. While a number of amendments were made before the passage of the 2015 Amendment with a view to protecting the privacy of individuals, the acceptability of a breach of privacy depends in part on to whom the information is disclosed and for what purpose. For this reason, a breach of privacy may be acceptable in the context of a serious criminal investigation undertaken by an approved government entity, and less so in civil proceedings where any person may be a litigant, and therefore the recipient, of the information.

Expense of Collection

10. Thirdly, service providers have incurred and continue to incur expense in collecting and storing data in compliance with the TIA Act. Should that same data become the subject of subpoenas or other court orders in civil proceedings, the burden on service providers would be further increased.

Question 3

Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the Telecommunications Act 1997 should not

---

apply?

1. The Committee recognises that exceptions to the prohibition in s 280(1B) of the Telecommunications Act are possible, and given the potentially valuable insights gained from data collected solely for complying with the data retention regime of the TIA Act Pt 5-1A\(^{65}\) (retained data) it could thus be useful in a variety of civil proceedings.

2. Nonetheless, the Committee strongly recommends for the maintenance of the prohibition, given that:

   - granting exemptions would be contrary to the ostensible objectives of the data retention regime; and
   - the potential for unintended consequences in expanding access to the retained data for use in civil proceedings.

**Exemptions Contrary to Objectives of the Data Retention Regime**

3. In 2014, when the data retention Bill was introduced, the collected data was retained solely for 'law enforcement and national security purposes'.\(^{66}\) In the Revised Explanatory Memorandum the purpose of the Bill was:

   to require service providers to retain a strictly defined subset of telecommunications data produced in the course of providing telecommunications services. This ensures the availability of a specified range of basic telecommunications data for law enforcement and national security purposes.\(^{67}\)

4. This very specific purpose of the data retention regime is echoed by the words of the PJCIS who considered 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. The Committee considers that the Bill should be amended to include a prohibition on civil litigant access to telecommunications data retained for the purpose of complying with the mandatory data retention regime.\(^{68}\)

5. The Telecommunications Act was amended to effect the recommendations of the PJCIS that access to telecommunications data for the use of civil proceedings be prohibited.\(^{69}\) The PJCIS, however, considered the potential for certain civil proceedings where the collected data could be used, would take the form of an exemption to the prohibition under s 280(1B) of the Telecommunications Act. The PJCIS recommended that consideration be

---

\(^{65}\) *Telecommunications (Interception and Access) Act* 1979 (Cth).

\(^{66}\) PJCIS Advisory Report, above n 13, 223.

\(^{67}\) Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*, 22.

\(^{68}\) PJCIS Advisory Report, above n 13, 223.

\(^{69}\) Revised Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*, 22.
given to amendments for a regulation-making power to this effect.

6. The Committee submits that, given the law enforcement and national security objectives of the data retention regime, it is not appropriate to extend access to the retained data for use in civil proceedings.

**PJCIS Examples of Potential Classes that Could be Excluded and Unintended Consequences**

7. The Committee notes that a regulation-making power is included in the TIA Act to enable provision for appropriate exclusions to the prohibition of the use of retained data in civil proceedings. In recommending the inclusion of the regulation-making power in the TIA Act, the PJCIS gave the examples of family law proceedings involving violence or international child abduction cases as potential classes of matters that could be excluded from the scope of the prohibition.  

8. The Committee is concerned by the possible range of unintended consequences in expanding access to retained data for use in civil proceedings. In the PJCIS example of family law proceedings involving violence as a potential class of family law proceedings that could be exempt from the prohibition, the Committee is of the view that access to metadata in these circumstances is inappropriate and may result in intimidation and further violence. Fiona McLeod SC, President of the Law Council of Australia, illustrates the unintended consequences that could flow from allowing parties to family law proceedings to access the retained data:

> You might have a case [...] where there has been allegation of violence alleged in a family breakdown. If a party to the proceedings can access the metadata, using that metadata, they can build a picture to track someone’s movement. So the perpetrator of violence could, in theory, track the movements of the victim.

> They could know who, or which phone numbers they were contacting, they could know where they were moving, what time they were leaving for work, what time they were leaving the house, so that people on the house or the contents of the house were vulnerable.

> They could know what time they were home and not using their devices, so in other words, what time they were home and sleeping and therefore very vulnerable.  

9. The PJCIS also provided cases of international child abduction as an example of potential classes that could be excluded from the prohibition. Cases of international (and local) child abduction are criminal matters that arguably fall within the scope of ‘serious criminal offences’. As such, the Committee is of the view that expanding the scope of access to retained data for use in civil proceedings will provide no utility to matters involving international (or local) child abduction as these cases do not suffer from a

---

70 PJCIS Advisory Report, above n 13, 223 [6.117].

71 Fiona McLeod SC, Concerns metadata could be used in civil cases, including divorce, 7:30 ABC (6 January 2017), <http://www.abc.net.au/news/2017-01-05/concerns-metadata-could-be-used-in-civil-cases/8164602>. 
prohibition on the use of the retained data during proceedings.

10. Due to the limited consultation period for these issues, the Committee cannot provide a comprehensive analysis of cases or classes of matters in which the use of retained data would be appropriate. Furthermore, the Committee cannot in the limited consultation period undertake a thorough consideration of the potential unintended consequences that could flow from allowing access to retained data during civil proceedings. The Committee is of the view that the Departments would benefit from an extended and comprehensive review into the potential unintended consequences.

11. The Committee submits that there should be a strong presumption against expanding access to the retained data under the TIA Act in civil proceedings.

12. However, the Committee is of the view that if any exceptions to the prohibition are required to be made that they should be made on a case-by-case basis by the Courts. The judiciary is best equipped to balance the competing interests of the parties, privacy and the administration of the civil justice system, in determining when an exception to the prohibition is appropriate.

Copyright Litigation

13. The Committee is of the view that copyright enforcement is an appropriate kind of civil proceedings where the prohibition in s 280(1B) of the Telecommunications Act should continue to apply.

14. Use of the retained data has significant value to rights holders in the enforcement of alleged online copyright infringement.  

15. Notwithstanding this potential benefit, the Committee submits that the case against the granting of such an exemption is stronger.

16. The Committee, like the PJCIS, views the use of the retained data in civil litigation as “inappropriate” as it risks the retained data becoming a “honey-pot” or establishing a clear target for a “fishing expedition” by rights holders at the expense of individual privacy. Rights holders may use the regime to “self-police their intellectual property.”

17. The Committee is particularly concerned with the potential situations where innocent people are threatened with legal action as a result of copyright infringement committed by a third party, arising out of shared or overlapping metadata identifiers.

18. Furthermore, use of the retained data in copyright litigation as evidence could

---

73 Ibid.
be problematic, given that it ignores the sizable number of Australians using privacy enhancing technologies such as “TOR” and virtual private network clients. This is exacerbated by “readily available and freely given” instruction in these technologies and detracts from the utility of an exemption from the s 280(1B) prohibition for copyright proceedings.

19. It is the Committee’s view, that more investigation would be required to analyse the merits and flaws of such an exemption, especially considering the potential floodgates of copyright litigation that would be opened as a result of such an exemption.

Concluding Comments

20. NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions please contact the undersigned at your convenience.

Contact:

Emily Ryan
President
NSW Young Lawyers
Email: president@younglawyers.com.au

Alternate Contact:

Richard Prangell
Chair
Communications, Entertainment and Technology Law Committee
Email: cet.chair@younglawyers.com.au

76 Leonard, above n 2, 43.