Access to telecommunications data in civil proceedings

Response to Consultation Paper circulated by the Attorney-General’s Department and the Department of Communication and the Arts

27 January 2017
Contents

Who we are ........................................................................................................................................... 3
Introduction ............................................................................................................................................. 4
What is metadata? .................................................................................................................................. 4
Use of metadata in civil litigation ........................................................................................................ 4
   Concerns regarding expanded access ............................................................................................... 6
Terms of reference .................................................................................................................................. 8
   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? .... 8
   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? 9
   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? ......................................................................................................................... 10
Data retention and human rights ......................................................................................................... 11
   The European Directive ....................................................................................................................... 13
Recommendations ................................................................................................................................... 15
Who we are

The Australian Lawyers Alliance (ALA) is a national association of lawyers, academics and other professionals dedicated to protecting and promoting justice, freedom and the rights of the individual.

We estimate that our 1,500 members represent up to 200,000 people each year in Australia. We promote access to justice and equality before the law for all individuals regardless of their wealth, position, gender, age, race or religious belief.

The ALA started in 1994 as the Australian Plaintiff Lawyers Association, when a small group of personal injury lawyers decided to pool their knowledge and resources to secure better outcomes for their clients – victims of negligence. While maintaining our plaintiff common law focus, our advocacy has since expanded to criminal and administrative law, in line with our dedication to justice, freedom and rights.

The ALA is represented in every state and territory in Australia. More information about us is available on our website.¹

Introduction

1. The Australian Lawyers Alliance (ALA) welcomes the opportunity to have input into the issues raised by the terms of reference of the Consultation Paper on Access to telecommunications data in civil proceedings circulated by the Attorney-General’s Department and the Department of Communications and the Arts.

2. This submission includes some general comments about the availability of telecommunications data (referred to in this submission as metadata, or simply data) in civil proceedings and the ALA’s concerns, before directly addressing all of the Terms of Reference. We then explore human rights issues in greater detail. Our focus is on civil litigation around personal injury. Any reforms would of course have wider ramifications, including in family and intellectual property law.

What is metadata?

3. Metadata is the data that is created around a communication, as opposed to its content. It can reveal substantial personal details, including who the subject is in contact with, how often they are in contact, the length of the contact and, with mobile devices, the location of the individual. It holds the possibility of identifying an individual’s movements on a particular date, and could demonstrate a pattern of movement or communications throughout the day, week or year.

4. The absence of data can also be telling. When a device is idle for a period of time, the absence of data might indicate that the individual is sleeping or otherwise engaged, possibly revealing when the individual is vulnerable.

5. Significant private details can be revealed by metadata. It can also be misleading: the data relates to the use of the device, rather than the activities of the individual owner of the device.

Use of metadata in civil litigation

6. Metadata is currently used widely in civil litigation. Telecommunications service providers will be required to be compliant with the reforms in the Telecommunications (Interception and Access) Amendment (Data Retention) Act
2015 (which amends the *Telecommunications (Interception and Access) Act 1979* (TIA Act) by inserting Part 5-1A) in April 2017. That Act will require telecommunications service providers to retain metadata for two years, so it can be made available to specified law enforcement agencies for national security and law enforcement purposes.

7. The *Telecommunications Act 1997* (Cth) prohibits the disclosure of metadata kept solely by the service provider to comply with requirements of Part 5-1A of the TIA Act in civil litigation: s280(1B). This restriction will come into force at the same time as the Part 5-1A data retention requirements, in April this year.

8. However, service providers retain metadata for numerous purposes in relation to running their businesses, such as billing. The restriction would not prevent disclosure of this data retained for other purposes. There is a lack of clarity as to the exact data to which the restrictions in s280(1B) apply.

9. It is the ALA’s understanding that the decision as to which data are retained for operational reasons is made by the service provider in question and will depend on how that service provider chooses to manage its data. According to the Department of Communications and the Arts, “Submissions to the Parliamentary Joint Committee on Intelligence and Security and discussions with providers have indicated that providers were already retaining much of the data they are required to retain under the data retention scheme, particularly subscriber information.”

While the Australian Privacy Principles (APPs) will have a role in determining the nature and use of the data, as well as how it is stored, these Principles do not provide sufficient clarity to determine whether a specific piece of metadata would have been retained in the absence of Part 5-1A.

10. It does not appear that the subject of the data will have any meaningful access to recourse if they disagree with the service provider’s decision whether or not the s280(1B) restriction applies to the data in question. If a service provider fails to comply with a subpoena to present documents, they may be held in contempt of court. If they breach the restriction, they could be subject to regulatory compliance

---

2 Email received by Anna Talbot, Legal and Policy Adviser, Australian Lawyers Alliance, from Damian Mahoney, Assistant Director, Communications Law Enforcement, Infrastructure Security and Resilience Branch, Department of Communications and the Arts, 25 January 2017.
measures.\(^3\) The subject of the data does not appear to have any meaningful avenue to influence how the data about them can be used in civil litigation, or indeed means of assessing whether the service provider has complied with the obligations in s280(1B).

11. It is accordingly difficult to see how s280(1B) will work in practice. There is a need for greater clarity regarding which data are affected by the restriction and which will continue to be available. Without this clarity, a comprehensive assessment of how the s280(1B) restriction will impact on civil litigation is impossible.

12. Clarity on what is proposed would also be useful. Without it, responding to Terms of Reference 2 and particularly 3 is difficult, as it is unclear what data are being referred to. This lack of clarity also gives rise to concerns regarding privacy: if it is not possible to know what will be protected by s280(1B), the law may be arbitrarily applied.

13. Below we explore some of the current uses of metadata, as well as outlining concerns regarding expanding access to metadata beyond current uses.

**Concerns regarding expanded access**

14. As far as the ALA is aware, there is no proposal that data would be available in civil litigation other than by way of a court order. If availability beyond that was proposed, we would strongly oppose it. Expansion of this nature would have a significant impact on the cost and time involved in civil litigation and the possibly restrict accessibility of this form of dispute resolution for many people. It would also constitute an invasion of people’s rights to privacy and freedom of expression, as acknowledged by the Joint Committee on Intelligence and Security (the Joint Committee), explored in more detail below.\(^4\)

---

\(^3\) Email received by Anna Talbot, Legal and Policy Adviser, Australian Lawyers Alliance, from Damian Mahoney, Assistant Director, Communications Law Enforcement, Infrastructure Security and Resilience Branch, Department of Communications and the Arts, 23 January 2017.

15. Any reform of the law to expand access to metadata would require that the case be made, and then for the case to be balanced against the rights that such reform might compromise, such as the right to privacy and freedom of expression. The ALA does not believe there is a need for expanded access, and indeed any expanded access could pose a danger to proceedings, litigants, and human rights more broadly.

16. There is a risk that increased availability of metadata could allow aggressive litigants to waste court time and resources in reviewing large volumes of data in the hope of finding useful evidence. This tactic could be used in bad faith, to try to pressure less well-resourced litigants to concede.

17. If this data were to be made available, routine review of it may become required to present the best case for one’s client, much as medical records are often routinely reviewed. This could add significant time to the preparation of cases, as the data available would be voluminous and interpreting it would require additional details including which phone number, locations or other details would be relevant in the search for evidence. Costs could escalate dramatically.

18. Psychiatric injury claims could be particularly affected. If a plaintiff in proceedings were claiming that they were too depressed to leave the house, for example, it may be attractive to the defendant to review the plaintiff’s metadata to see if their mobile phone did in fact leave the house. There could be a perfectly innocent explanation for any data that indicated that the mobile had regularly left the house, such as it was being borrowed by a family member, or the plaintiff was attending medical appointments. This additional evidence would require extra time on the part of both parties, however, inevitably increasing costs and potentially wasting the time of the court as the evidence was presented and rebutted.

19. Greater access to metadata could also give rise to risks of violence towards people, or their property, involved in civil litigation. In family law matters, for example, the location details provided in metadata could give rise to a risk of violence between parties, even in cases where there was no history or indication that this risk might arise. Both civil litigation and relationship breakdown are times of extreme stress. Metadata might reveal regular contact between a party to the proceedings and a new partner (or someone who the other party might suspect is a new partner), placing that person at risk also.
20. It is not just in family disputes that metadata might give rise to a risk of violence or threats. Neighbourhood disputes or proceedings involving whistleblowers could involve increased intimidation, threats or violence if metadata were to reveal locations or other details. It would be important for courts to consider these risks in considering whether to grant court orders.

21. Further, there is no clarity provided as to whose metadata can be revealed in civil litigation. The privacy of those not involved in the litigation, whose details may be revealed in metadata, must also be considered. If someone has been in regular contact with a party whose metadata might be considered relevant even if they are not a party to the dispute, there is a real risk that their right to privacy could be infringed unfairly, if the court considers the details relevant and probative.

Terms of reference

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?

22. Data outlined in s187AA is currently available to parties to civil proceedings pursuant to a subpoena or court order in any number of circumstances. Our members (the majority of whom are personal injury lawyers) currently access metadata routinely in civil proceedings as needed, depending on the facts in issue in the case.

23. Parties to proceedings relating to motor vehicle accidents might have cause to access metadata. If there is a dispute as to whether a driver was operating their mobile phone at the time that the accident took place, for example, metadata can be useful to demonstrate whether the phone was in operation and was in the same location as the accident at the time.

24. Similarly, metadata can be useful in refuting claims that mobile phone use was responsible for an accident. Where a mobile phone might be found in the vicinity of a workplace accident, for example, metadata can clarify whether or not the phone was in use, clarifying questions of contributory negligence.
25. Metadata must be carefully interpreted. During a recent Joint Parliamentary Committee on Security and Intelligence, barrister Dr David Neal SC revealed that location data, which is often what metadata is used to reveal, had resulted in a control order being imposed on his client based on faulty interpretation of this data. Police had alleged that the client had been in a particular location, due to the data from a tracking device. However, when the data coming from the device was examined by defence counsel, it emerged that it had in fact been attached to the police car, not the client’s. As with any evidence, there are dangers in placing too much faith in metadata. Expanding access to it could increase this risk and costs associated with refuting it.

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?

26. The current legislation does not prevent parties to civil proceedings accessing all data referred to in s187AA, as mentioned above. It is only data retained under that section that would not otherwise be retained that parties to civil litigation are prevented from accessing, according to s280(1B)(b) of the Telecommunications Act 1997. There is a need for greater clarity on what specific data is restricted from use in civil litigation, and how that data can be identified. Individual subjects of the data should have access to information on how the service provider assesses whether s280(1B) applies to the data and be able to dispute the decision if they disagree with it.

27. Despite the lack of clarity, there is a very good reason for this restriction to remain in place. Assessments of the data retention regime found that infringements on rights that the regime would introduce were justifiable, due to the fact that the data collected under it would be made available only for national security and law enforcement purposes. To make data originally collected for these reasons available for other purposes would render those assessments obsolete.

28. The analysis would have to be re-done. ALA believes that the infringements on privacy are likely to be found to be too great if the data retained solely to meet

---

5 Parliamentary Joint Committee on Intelligence and Security, Hansard, 14 October 2016, pp8-9.
obligations under the TIA Act were to become available in civil proceedings. Assisting parties to civil litigation to resolve their disputes would be unlikely to meet the threshold of being necessary and proportionate to the legitimate aim of protecting national security and law enforcement. These issues are discussed in greater detail below.

29. It is unclear whether there would be much, if any, impact on civil proceedings if the limitation in s280(1B) were retained, due to the uncertainty as to the specific data the limitation relates to. It is possible that parties may be unable to access relevant evidence if they are unable to access telecommunications data that is retained solely to meet TIA Amendment Act obligations.

30. An equally important consideration, however, is what the impact might be if parties to civil proceedings were able to access the data as set out in s187AA. The ALA has a number of concerns in this regard, as outlined above under the heading ‘Concerns regarding expanded access’.

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?

31. No. The ALA believes that the system currently in place is sufficient to balance the rights of parties to civil proceedings and the public’s rights to privacy and freedom of expression.

32. It may be possible that, when the restriction comes into force, unforeseen impacts point to the need to review the use of the data that will become unavailable. If that is the case, it will be important to conduct a comprehensive review of the impact of using this data on the right to privacy, the right to freedom of expression and other human rights that Australia has agreed to be bound by. It would also be prudent to consider the risk that the use of the data might continue to be expanded, and how such an ongoing expansion might be guarded against.
Data retention and human rights

33. Forcing telecommunications companies to retain specified metadata, and granting access to this data to selected agencies without a warrant or court approval, effectively authorises mass surveillance in Australia. Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) grants the right to be free from arbitrary or unlawful interference with privacy. Article 19 of that Covenant grants the right to freedom of expression. Australia has agreed to be bound by this Covenant and is obliged to respect, protect and promote the rights contained therein.

34. Restrictions on these rights must be clear and precise, and limited to those strictly necessary to achieve a legitimate aim (such as protecting national security).6

35. As acknowledged in both the report of the Parliamentary Joint Committee and the Statement of Compatibility with Human Rights on the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015 (TIA Amendment Act), infringements on the rights to privacy and freedom of expression are only justifiable in certain circumstances.7 National security and law enforcement concerns are valid reasons to limit these rights, but those limits must be necessary and proportionate, according to Australia’s human rights obligations.

36. The report and the Statement acknowledged that these rights were impacted by these reforms.8 Ultimately, the Revised Explanatory Memorandum argued that

---


infringements on the right to privacy and freedom of expression were justified in this context due to the security arguments that had been made.9

37. Prior to its introduction, the Attorney-General, George Brandis SC, gave the assurance that the metadata retained under the new scheme would be used only in relation to the most serious crimes:

‘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, only to as a tool [sic], only to crime and only to the highest levels of crime... Civil wrongs have nothing to do with this scheme.’10

38. There are disputes about the effectiveness of the reforms as a national security measure (which will determine whether the regime complies with international human rights obligations). It is clear, however, that the reforms were passed for reasons of national security and law enforcement and thus seek to conform with these human rights obligations.

39. The Statement of Compatibility with Human Rights makes all of its assessments regarding compatibility with human rights on the basis that the data will be made available for these permissible reasons. There is no reference to the use of the data for civil litigation, and indeed, the Statement suggests that the right to privacy would not be met if the data were used in this way.11

40. By expanding the use of this data beyond what is strictly necessary for national security and law enforcement and making it available in civil litigation, the government is likely to be overstepping permissible limitations.

---

9 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Revised Explanatory Memorandum, [15].


11 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Revised Explanatory Memorandum, [96], [128].
The European Directive

41. In Europe, a data retention regime similar to that which is currently in place in Australia was struck down as unjustly interfering with the rights to privacy and protection of personal data, in the 2014 case of Digital Rights Ireland. This case provides some guidance as to how mass surveillance impacts on human rights, and how using data collected for national security and law enforcement for civil litigation might be viewed.

42. The European Court of Justice considered that the regime was designed to protect national security and assist in law enforcement, which constituted permissible reasons to impact on these rights. Ultimately, however, it was felt that the regime was not proportionate in balancing rights against these interests. Specifically, the Court noted that ‘the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that interference is actually limited to what is strictly necessary’.\(^{12}\) The Court’s concerns included the length of time the data was to be retained (up to 24 months), access to the data without a court order, and the indiscriminate nature of the data retention, without any basis of suspicion that the interference with the right was strictly necessary to achieve the stated aims.

43. In determining how access to the data would be regulated, the Directive that was struck down required member states to:

‘adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the [European Convention for the Protection of Human Rights and

44. While these requirements do not explicitly prohibit the use of data for the purposes of civil litigation, the fact that it might only be provided to competent national authorities in accordance with necessity and proportionality requirements appears to obviate this possibility. Civil proceedings are unlikely to reach that bar.

45. Australia’s data retention laws are based on this Directive, despite the fact that it was invalidated prior to the passage of the TIA Amendment Act. Australia does not enjoy the human rights protections that exist in Europe, and Australian courts have consistently ruled that legislation which conflicts with international human rights obligations is nevertheless valid and will be enforced, so long as it is clear.

46. In this context, the suggestion that restrictions on the use of data being retained under Part 5-1A of the TIA Act might be relaxed gives rise to significant concerns. There is every possibility given that the European Directive was ruled to infringe on fundamental rights, despite its strict national security and law enforcement purpose, that the TIA regime does too. Expanding the use of this data beyond permissible purposes would be highly likely to infringe human rights, as the data would be being used for purposes that do not comply with the requirements of necessity and proportionality.

47. Australia would benefit from an enforceable federal Human Rights Act, to ensure that the rights of people in Australia enjoy a similar level of protection to those in Europe.

---


Recommendations

The ALA makes the following recommendations:

- The Attorney-General and the Minister for Communications and the Arts must urgently clarify what data the restrictions on the use of data under s280(1B) of the Telecommunications Act 1997 relate to.
- The Attorney-General and the Minister for Communications and the Arts must clarify how subject of the data can assess whether it can be validly released under the s280(1B), and that avenues are made available to seek review of a decision to release or restrict access to the data;
- Courts should be aware of the risks inherent in releasing metadata and conduct risk assessments before granting orders that the data be made available;
- The restriction on the use of data collected under Part 5-1A of the TIA Act should be maintained in its current form;
- Any proposal to expand the use of metadata should include consideration of how this would impact on the human rights obligations that Australia has agreed to be bound by under international law; and
- An enforceable Human Rights Act should be introduced to ensure that rights to privacy, freedom of expression and all other human rights are adequately balanced in all law reform, especially that related to national security and law enforcement.