Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

13 January 2016

Assistant Secretary
Infrastructure Security and Resilience Branch
Department of Communications and the Arts

Assistant Secretary
Communications Security Branch
Attorney-General's Branch

Re: ACCESS TO RETAINED DATA IN CIVIL PROCEEDINGS

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached. The APF welcomes the invitation to make a submission on the prohibition on the disclosure of telecommunications data for the purpose of civil proceedings in s 280(1B) and ss 281(2) and (3) of the *Telecommunications Act 1997* (Cth) (the TA).

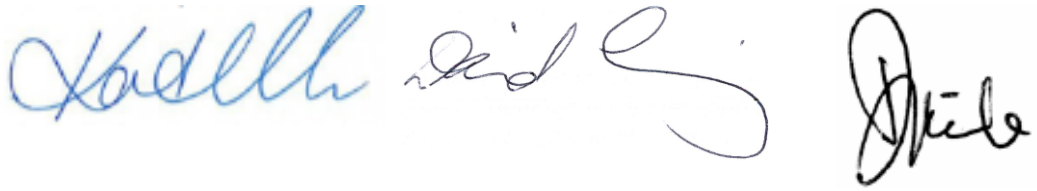
Please find attached the APF's submission to the inquiry into access to data retained under the data retention regime for the purpose of civil proceedings.

In summary, the APF submits that:

1. The prohibitions on the use or disclosure of telecommunications data for the purpose of civil proceedings in s 280(1B) and ss 281(2) and (3) of the TA should be retained.
2. There is no case for the relaxation of the prohibitions by means of regulations made pursuant to s 280(1B)(v) and s 281(2)(v).
3. There is a case for reviewing Part 13 of the TA to ensure it is fit for purpose in the context of the mass collection of revelatory telecommunications metadata.
4. There is a case for tightening the prohibitions on the disclosure of telecommunications data for the purpose of civil proceedings beyond the terms of s 280(1B) and ss 281(2) and (3) of the TA so that access is permitted to only a subset of the data set specified in s 187AA of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act).

Thank you for your consideration.

Yours sincerely



Kat Lane, Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

(Dr) David Lindsay, Vice-Chair
(03) 9905 5547
David.Lindsay@privacy.org.au

David Vaile, Vice-Chair
0414 731 249
David.Vaile@privacy.org.au

AUSTRALIAN PRIVACY FOUNDATION: SUBMISSION TO REVIEW OF ACCESS TO RETAINED DATA IN CIVIL PROCEEDINGS

1. Background: The Data Retention Regime

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) amended the TIA Act to introduce a regime that requires telecommunications service providers to retain a set of telecommunications data (commonly referred to as 'metadata' in this submission) for a minimum period of two years. In previous submissions, the APF has consistently maintained that the data retention regime is a disproportionate interference with the privacy of Australians.[1] The APF submits that broad-based mandatory data retention is inimical to the right to privacy and that the legitimate objectives of law enforcement and national security could be better served by more targeted measures. Accordingly, the APF supports proposals for an expedited review of the data retention regime.

The data retention regime was introduced with the sole objective of ensuring that certain telecommunications data is available for the purposes of law enforcement and national security. As the Revised Explanatory Memorandum to the Data Retention Bill put it:

> The data retention measures contained in the Bill ensure the retention of the basic telecommunications data that is essential to support Australian law enforcement and security agencies in the performance of their functions.[2]

The telecommunications data required to be retained under the regime is specified in set out in s 187AA of the TIA and is defined by reference to six kinds of information: the identity of the subscriber to a communications service; the source of the communication; the destination of the communication; the date, time and duration of the communication; the type of the communication; and the location of the equipment used in the communication.

The potential for the data retained under the regime to be used for purposes other than law enforcement and national security as considered by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its report on the Data Retention Bill of February 2015.[3] In relation to the use of retained data for the purposes of civil proceedings, the PJCIS stated that it:

---

[1] See Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Submission 75,* February 2015.

[2] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Revised Explanatory Memorandum, [25].

[3] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,* February 2015.

> … considers 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 the regime to be drawn upon as a new source of evidence in civil disputes.[4]

Accordingly, the PJCIS recommended that the Bill:

> … be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime.[5]

As noted in the Revised Explanatory Memorandum to the Bill:

> The Committee received evidence of concerns about a possible increase in the frequency and volume of telecommunications data accessed by civil litigants as a result of the implementation of the data retention scheme and the public interest in confining disclosure of and access to, telecommunications data, to protect the broader privacy interests of the community.[6]

The limited purpose of the data retention regime was emphasised by Attorney-General Brandis prior to passage of the legislation. In comments made on the *Q&A program* on 3 November 2014, the Attorney-General stated that:

> 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.

The Attorney-General then specifically added that:

> Breach of copyright is a civil wrong. Civil wrongs have got nothing to do with this scheme.[7]

In the APF submission to the PJCIS inquiry into the Data Retention Bill, we warned of the potential dangers of 'scope creep' in the following terms:

> Given the volume of data that will be retained by carriers and ISPs, there will be considerable pressure for such data to be accessed and used for purposes other than law enforcement and national security. In particular, there will be immense pressure for the data to be accessed and used in both civil and criminal legal proceedings by parties who are not authorised to access the data under the TIA Act. In terms of criminal law proceedings, prosecutors will have clear incentives to seek to access data on the basis of speculation alone; while defence lawyers will have incentives to request access to potentially exculpate

---

[4] *Ibid.* [6.115].
[5] *Ibid.* Recommendation 23, p. xx.
[6] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Revised Explanatory Memorandum, [167].
[7] Rohan Pearce, 'Data retention laws 'can't be and they won't be' used against pirates: Brandis', *Computerworld,* 4 November 2014, http://www.computerworld.com.au/article/558785/data-retention-laws-can-t-they-won-t-used-against-piracy-brandis/.

> their clients. And further, Courts may clearly order the disclosure of records wherever relevant across a broad range of cases. In terms of civil litigation, the data exists as a 'honey-pot' for a broad range of actors. Parties to disputes in family law, and in all manner of commercial disputes (involving, for example, trade secrets, intellectual property, and defamation) will likely seek disclosure of retained metadata.[8]

The prohibitions in s 280(1B) and ss 281(2) and (3) were introduced to the TA to give effect to the PJCIS recommendation to prohibit access to retained data for the purpose of civil proceedings. In its report, however, the PJCIS also recommended the introduction of a regulation making power to provide for exclusions on the prohibitions 'such as family law proceedings relating to violence or international child abduction cases'.[9] Powers to make regulations to exclude the prohibitions were introduced as s 280(1B)(v) and s 281(2)(v) of the TA. The PJCIS also recommended that 'the Minister for Communications and the Attorney-General review this measure and report to the Parliament on the findings of that review by the end of the implementation phase of the Bill'.[10] The current inquiry arises from this recommendation. Nevertheless, the issues raised in the inquiry give rise to precisely the same concerns as those identified by the APF in our submission to the PJCIS inquiry.

2. Context for the Review: Ubiquitous Metadata

In undertaking this review, it is essential to take into account the significant legal and policy challenges arising from the relatively recent massive increase in the generation and use of telecommunications metadata. This section of the submission reviews the privacy implications of this development.

This review occurs in the context of the increased generation, use, matching and value of telecommunications metadata, and especially data generated from ubiquitous mobile devices. Importantly, such data is potentially extremely revelatory. As District Judge Leon pointed out in *Klayman v Obama:*

> Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life.[11]

---

[8] Australian Privacy Foundation, Submission to Parliamentary Joint Committee on Intelligence and Security Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Submission 75,* February 2015, pp. 15-16.
[9] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,* February 2015, [6.117], Recommendation 23, p. 224.
[10] *Ibid.* Recommendation 23, p. 224.
[11] *Klayman v Obama,* 957 F. Supp. 2d 1 (D.D.C. 2013).

Similarly, In *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources,*[12] the Court of Justice of the European Union (CJEU) stated, in relation to the retention of telecommunications metadata, that:

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the social relationships of those persons and the social environments frequented by them.[13]

The highly revelatory nature of telecommunications metadata was aptly summarised by computer scientist, Edward Felten, in evidence to a 2013 U.S. Senate Committee hearing:

> Metadata can now yield startling insights about individuals and groups, particularly when collected in large quantities across the population. It is no longer safe to assume that this "summary" or "non-content" information is less revealing or less sensitive than the content it describes. Just by using new technologies such as smart phones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many details of our lives can be gleaned by examining those trails. Taken together, a group's metadata can reveal intricacies of social, political, and religious associations. Metadata is naturally organized in a way that lends itself to analysis, and a growing set of computing tools can turn these trails into penetrating insights. Given limited analytical resources, analyzing metadata is often a far more powerful analytical strategy than investigating content: It can yield far more insight with the same amount of effort.[14]

The ever-increasing quantity of metatada creates significant challenges for the protection of privacy; and the law has been slow in adapting to these challenges. In particular, the ubiquity and value of telecommunications metadata creates the temptation for such data to be used for a wide variety of purposes beyond that for which the data were collected, with attendant risks to privacy.

Recommendation:

In the context of ubiquitous metadata, to ensure that privacy is properly protected it is absolutely essential that appropriate limits be imposed on the collection, use and disclosure of telecommunications metadata.

---

[12] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Maine and Natural Resources* [2013] ECR I-847.

[13] [2013] ECR I-847, para [27].

[14] Edward W Felten, Written Testimony to United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, 2 October 2013, http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf.

3. Context for the Review: Metadata as 'Personal Information'

The status of certain telecommunications metadata as 'personal information' for the purpose of the *Privacy Act 1988* (Cth) (the 'PA') is currently before the Full Federal Court, on appeal from *Telstra Corporation Limited v Privacy Commissioner.*[15] There is a very strong case for some metadata, such as Internet Protocol (IP) addresses, to be regarded as 'personal information' for the purpose of information privacy laws. This is even more so given the evolution of data matching techniques and re-identification by, for example, data linking.[16]

This conclusion is reinforced by s 187LA of the TIA Act, which provides that information or documents kept under the data retention regime are 'personal information' for the purpose of the PA. Section 187LA emphasises the importance of safeguards for the protection of telecommunications metadata, including limits on the use and disclosure of such data.

Recommendation:
The highly revelatory nature of telecommunications metadata, especially when it is matched with other data, creates a strong case for it to be treated as 'personal information' for the purpose of information privacy laws. This indicates that strict and proportionate limits should be imposed on the collection, use and disclosure of telecommunications metadata, on a par with the regulation of other forms of 'personal information'.

4. The Statutory Provisions

This section of the submission outlines the relevant statutory provisions in the TA and identifies issues in the interpretation and application of the provisions. The relevant provisions are s 280(1B), and ss 281(2) and (3), of the TA.

4.1 Section 280(1B)

Part 13 of the TA regulates the use and disclosure of any information or document obtained by an eligible person, such as a carrier or carriage service provider (CSP), during the supply of telecommunications services. In particular, the TA prohibits the use or disclosure of information relating to the:

- contents of a communication carried, or being carried, by a carrier or CSP;
- carriage services supplied or intended to be supplied by a carrier or CSP; or

[15] [2015] AATA 991 (18 December 2015).
[16] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review* 1701.

- affairs or personal particulars (including any unlisted telephone number or any address) of another person.[17]

The TA specifies a number of exceptions to the prohibition on the use or disclosure of information or documents. Section 280(1) provides that the prohibition does not apply to: a disclosure or use by an enforcement agency that is required or authorised under a warrant; or if the disclosure or use is required or authorised by or under law. Use or disclosure of information or documents is authorised by law if provided by witnesses summoned to give evidence or produce documents.

Section 280(1B) was introduced by the Data Retention Bill to give effect to the PJCIS recommendation to prohibit the use of telecommunications data in civil proceedings. It provides that the exception which permits the use or disclosure of information authorised by law does not apply to the disclosure of information or a document where:

- the disclosure is required or authorised because of a subpoena, or notice of disclosure, or court order, in connection with a civil proceeding;
- the information or document is kept solely for the purpose of complying with the data retention regime;
- the information or document is not used or disclosed otherwise than for specified limited purposes, including a purpose prescribed by regulations.[18]

The following issues arise in relation to the interpretation and application of s 280(1B):

- Given that Part 13 of the TA was drafted before the relatively recent massive increase in the generation and use of telecommunications metadata, there are questions as to whether or not it is fit for purpose in protecting privacy in relation to data held by carriers and CSPs. For example, there may be questions as to the extent to which the statutory confidentiality obligations imposed on carriers and CSPs, which apply to information relating to the 'affairs and personal particulars' of a person, apply to all categories of telecommunications metadata. Moreover, the exception allowing disclosure or use of information 'required or authorised by or under law' is so broad as to potentially undermine the regime.
- The limitation of the s 280(1B) prohibition to information or documents 'kept solely for the purpose' of complying with the data retention regime raises practical issues of implementation: it may be difficult to determine, in any given case, whether or not data has been kept *solely* for the purpose of the data retention regime.

4.2 Sections 281(2) and (3)

Section 281(1) of the TA provides that the prohibition on the use or disclosure of information or documents by a carrier or CSP does not apply to prevent disclosures by a witness summoned to

[17] *Telecommunications Act 1997* (Cth) ss 276-8.
[18] *Telecommunications Act 1997* (Cth) s 280(1B)(c)(v).

give evidence or produce documents. Section 281(2), which was introduced to give effect to the PJCIS recommendation, effectively prohibits the disclosure by a witness in civil proceedings of information or documents that are kept by a carrier or CSP solely for the purpose of complying with the data retention regime. Section 281(3), on the other hand, permits disclosure by a witness for the specified limited purposes identified in s 280(1B), including for a purpose specified by regulations. Sections 281(2) and (3) were therefore introduced to support the prohibition on the use of telecommunications metadata in s 280(1B), and shares the same problems of interpretation and application.

Recommendations

- In the context of mass retention and use of telecommunications metadata, there is a strong case for a comprehensive review of Part 13 of the TA to ensure that it remains fit for purpose.
- The limitation of the prohibition on the use of telecommunications data in civil proceedings to information or documents kept 'solely for the purpose' of the data retention regime may be difficult to implement. There may be a case for introducing a simpler legislative distinction between metadata which is prohibited from being used in civil proceedings and data which may be used. This is explained further subsequently in this submission. Nevertheless, as further explained, even though there is a case for a simpler legislative distinction, where it is established that telecommunications data has been retained solely due to the data retention regime, the prohibition on the use of data in civil proceedings should remain.

5. The 'Purpose Limitation Principle': Application to Metadata

As explained above, there is a good case for treating certain telecommunications metadata as 'personal information' for the purpose of information privacy laws. The most relevant information privacy principle for the purpose of this inquiry is the 'purpose limitation principle'. This section of the submission explains the application of the purpose limitation principle to the question of whether or not to relax the prohibition on the use of retained data in civil proceedings.

The purpose limitation (or 'purpose specification') principle is a fundamental principle of information privacy law. The principle provides that personal information 'should be collected for specified, legitimate purposes and not used in ways that are incompatible with those purposes'.[19] The purpose limitation principle is incorporated in the Australian Privacy Principles (APPs) with, for example, APP 6.1 providing that personal information that was collected for a particular purpose must not generally be used or disclosed for another purpose.

[19] Lee Andrew Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 153.

The data retention regime is premised on the assumption that it was necessary to ensure that law enforcement and security agencies have access to data that would otherwise not be retained. The Revised Explanatory Memorandum to the Data Retention Bill made this abundantly clear:

> The purpose of the Bill is 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.[20]

Given that the data would not otherwise be retained, and in some cases not collected, it is contrary to the purpose limitation principle for the data to be used or disclosed for a purpose other than law enforcement or national security purposes.

Recommendation:

The highly revelatory nature of telecommunications metadata means that such data should be subject to essentially the same regulations and limitations as apply to 'personal information' under information privacy laws. The application of the purpose limitation principle to retained metadata leads to the conclusion that the use and disclosure of such data should be restricted strictly to the purpose for which the data was collected and retained, namely for the purposes of law enforcement and national security.

6. Applications for Telecommunications Metadata in Civil Proceedings

Given the ubiquity and highly revelatory nature of data held by telecommunications carriers and ISPs, it is unsurprising that it may be potentially useful in civil proceedings. This section of the submission reviews relevant case law in the EU, UK and Australia relating to applications for such data in civil proceedings.

In *Promusicae,*[21] the Court of Justice of the European Union (CJEU), was required to consider an application by an organisation representing copyright owners for an order requiring an Internet Service Provider (ISP) to disclose of the identities of subscribers involved with copyright infringements by means of a peer-to-peer (P2P) system. The case concerned a provision of a Spanish law applying to the use of telecommunications data required to be retained by telecommunications service providers which, in the relevant Article, provided that:

> The operators of electronic communications networks and services and the service providers to which this article refers may not use the data retained for purposes other than

[20] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Revised Explanatory Memorandum, [22].
[21] Case C-275/06 *Productores de Música de Espańa (Promusicae) v Telefónica de Espańa SAU* [2008] ECR I-271.

> those indicated in the paragraph below or other purposes permitted by the Law and must adopt appropriate security measures to avoid the loss or alteration of the data and unauthorised access to the data.
>
> The data shall be retained for use in the context of a criminal investigation or to safeguard public security and national defence, and shall be made available to the courts or the public prosecutor at their request.[22]

The CJEU ruled that there was nothing in EU law that required Member States to lay down an obligation to communicate personal data in the context of civil proceedings. Moreover, the Court held that in transposing EU directives into national laws, Member States must rely on an interpretation that is proportionate in that it strikes a 'fair balance' between the fundamental rights safeguarded by the EU Charter of Fundamental Rights,[23] especially the right to intellectual property protected by Article 17 and the right to data privacy protected by Article 8.

In *Golden Eye v Telefonika,*[24] licence holders of copyright works sought a *Norwich Pharmacal*[25] order against ISPs for disclosure of details of subscribers who had allegedly infringed copyright by means of P2P file-sharing. Applying *Promusicae,* Arnold J held that the order had to be proportionate in that it struck a fair balance between the rights of copyright owners and the rights of users to protection of personal data. In relation to the subscribers, Arnold J observed that:

> The grant of the order sought will invade their privacy and impinge upon their data protection rights. Furthermore, it will expose them to receiving letters of claim and may expose them to proceedings for infringement in circumstances where they may not be guilty of infringement, where the subject matter of the claim may cause them embarrassment, where a proper defence to the claim would require specialised legal advice that they may not be able to afford and where they may not consider it cost-effective for them to defend the claim even if they are innocent.[26]

While not rejecting the order, Arnold J applied the proportionality principle to carefully scrutinise the terms of the order, especially given the potential for applicants to engage in speculative invoicing.

In *Dallas Buyers Club v iiNet,*[27] Perram J considered an application for preliminary discovery against ISPs to identify subscribers associated with IP addresses allegedly involved with copyright infringements by means of a P2P system. In the course of granting the application, subject to

[22] Law 34/2002 on information society services and electronic commerce of 11 July 2002, Article 12(2), (3).
[23] Charter of Fundamental Rights of the European Union, 2010 O.J. C364.
[24] *Golden Eye (International) Limited v Telefónica UK Limited* [2012] EWHC 723 (Ch).
[25] *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133.
[26] [2012] EWHC 723 (Ch), [119].
[27] *Dallas Buyers Club LLC v iiNet Limited* [2015] FCA 317.

conditions, Perram J referred to the protection of privacy under Part 13 of the TA and under the PA, concluding that:

> Together, these provisions demonstrate that the privacy of account holders of ISPs is regarded by the Parliament as having significant value.[28]

Acknowledging that the grant of the order involved a clash between the rights of the copyright owners and the privacy rights of subscribers, Perram J imposed strict conditions on the use of information obtained pursuant to the order. Subsequently, Perram J dismissed an application to lift a stay on the order for preliminary discovery primarily due to concerns about claims for disproportionate damages made by the copyright owners.[29]

These cases illustrate the following points:

1. The courts in Australia and elsewhere have consistently acknowledged the importance of the privacy rights of users in applications for information from intermediaries such as ISPs to disclose the personal information of subscribers. In order to protect the privacy of users, such applications must be carefully scrutinised.
2. The courts in Australia and elsewhere have consistently expressed concerns that the jurisdiction to grant orders against telecommunications carriers and ISPs to disclose information may be abused, especially by practices such as 'speculative invoicing'.
3. If the protection of privacy is important in applications for disclosure of information about subscribers held by carriers and ISPs for their own business purposes, it is even more important in relation to data that a carrier or ISP might not otherwise retain, or even collect, apart from the obligations imposed by the data retention regime.

Recommendations

The following conclusions and recommendations follow from the above review of relevant case law:

1. Applications for orders, such as orders for preliminary discovery, have been restricted to a very limited class of information held by carriers or ISPs, especially information that identifies subscribers associated with IP addresses. This strongly suggests that there is no case for allowing access to all categories of data identified in s 187AA of the TIA Act.
2. Consideration should therefore be given to the possibility of simplifying the distinction between telecommunications metadata which can be accessed for use in civil proceedings and data which cannot be accessed by restricting applications for access to specific kinds of data, such as data identifying a subscriber. For the most part, this would be telecommunications data that would be held by a carrier or CSP for its own business

[28] [2015] FCA 317, [85].
[29] *Dallas Buyers Club LLC v iiNet Limited (No 5)* [2015] FCA 1437.

purposes, and not retained solely due to the obligations imposed under the data retention regime.

3. In the event that some data sought in applications for preliminary discovery would not have been retained except for the data retention regime, the prohibition should remain as, apart from the data retention regime, this data would not otherwise have been available. The continuation of the prohibition would therefore not impose undue hardship on applicants in civil proceedings, and strike a balance between the protection of privacy of subscribers and the rights of potential litigants in civil suits.
4. Given the importance of privacy considerations in applications for preliminary discovery for information or documents held by carriers or CSPs, consideration should be given to introducing reforms to laws relating to preliminary discovery, such as rule 7.22 of the *Federal Court Rules 2011* (Cth), which expressly require considerations relating to privacy to be taken into account in the exercise of the Court's discretion to grant preliminary discovery.

7. Answers to Questions and Conclusions

This section of the submission provides answers to the specific questions raised by the review; and summarises the conclusions of the submission.

7.1 Questions Raised by the Review

The Consultation Paper for the review asks three specific questions which are addressed in this section of the submission.

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?

To the APF's knowledge, access to the data set is primarily sought in relation to a relatively small subset of the data defined in s 187AA of the TIA Act, mostly data about the identity of a subscriber and their association with an IP address. For the most part, this is likely to be data that will already be held by a carrier or CSP for their business purposes.

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?

Strictly speaking, the review raises the question of whether or not parties to civil proceedings should be able to access the subset of telecommunications data, as defined in s 187AA of the TIA Act, which are kept solely for the purpose of the data retention regime; access to other data is

not subject to the prohibition. As the vast majority, or almost all, applications for access to data are likely to be made in relation to data held by carriers or CSPs for their own purposes, continuing the prohibition on the use or disclosure of such data in civil proceedings would have negligible impact on the parties. Moreover, as suggested in this submission, there is a case for limiting access to telecommunications data for the purpose of civil proceedings to a defined subset of the data set out in s 187AA. This would have the following advantages. First, it would benefit all parties, including carriers and CSPs, by simplifying the process for deciding whether or not the prohibition applies to particular data. Secondly, it would strike a better balance between the rights of potential parties to civil litigation and the privacy rights of subscribers, especially given the context of the mass collection of telecommunications metadata. Thirdly, it would prevent the possibility, raised by potential open slather access to telecommunications metadata, on resources being wasted on 'fishing expeditions' by potential parties to civil litigation, including the use of scarce court resources in dealing with such applications.

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?

The PJCIS report on the Data Retention Bill, which recommended a review of the prohibition on the use of telecommunications data, suggested that the regulation-making power might be used to allow applications in relation 'family law proceedings relating to violence or international child abduction cases'.[30] This implies that the power to relax the prohibition on the use or disclosure of telecommunications data was intended to be used, if at all, only in the most serious cases. The APF does not consider that the case has made that, in relation to the limited subset of telecommunications data that is retained solely for the purpose of the data retention regime, there is a benefit in making the data accessible to potential litigants. Moreover, the APF submits that before a decision is made to exercise the regulation-making power, there needs to be much more information about the kind of data which is subject to the prohibition: what data are being retained by carriers and CSPs solely due to the data retention regime? Without such information, there is simply no basis for a reasoned decision to be made on the relaxation of the prohibition, even for use in the most serious civil proceedings.

7.2 Conclusions and Recommendations

This section summarises the conclusions and recommendations made in this submission. The submission draws the following conclusions. In doing so, the APF acknowledges that some of the conclusions extend beyond the scope of the current review, but we consider that this is essential to ensure that the context involving the mass collection and storage of telecommunications metadata is fully taken into account.

1. The data retention regime is a disproportionate interference with the privacy of Australians. While s 187N of the TIA Act requires that the PJCIS conduct a review of the regime within three years of the implementation phase for the regime, the APF submits that this review should be brought forward, especially in order to properly address the significant privacy implications of a mandatory mass data retention scheme.

2. In the context of ubiquitous metadata, to ensure that privacy is properly protected it is absolutely essential that appropriate limits be imposed on the collection, use and disclosure of telecommunications metadata.

3. The highly revelatory nature of telecommunications metadata, especially when it is matched with other data, creates a strong case for it to be treated as 'personal information' for the purpose of information privacy laws. This indicates that strict and proportionate limits should be imposed on the collection, use and disclosure of telecommunications metadata, on a par with the regulation of other forms of 'personal information'.

4. In the context of mass retention and use of telecommunications metadata, there is a strong case for a comprehensive review of Part 13 of the TA to ensure that it remains fit for purpose.

5. The limitation of the prohibition on the use of telecommunications data in civil proceedings to information or documents kept 'solely for the purpose' of the data retention regime may be difficult to implement. There is a case for introducing a simpler legislative distinction between metadata which is prohibited from being used in civil proceedings and data which may be used. Nevertheless, even though there is a case for a simpler legislative distinction, where it is established that telecommunications data has been retained solely due to the data retention regime, the prohibition on the use of data in civil proceedings should remain.

6. The highly revelatory nature of telecommunications metadata means that such data should be subject to essentially the same regulations and limitations as apply to 'personal

[30] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,* February 2015, [6.117].

information' under information privacy laws. The application of the purpose limitation principle to retained metadata leads to the conclusion that the use and disclosure of such data should be restricted strictly to the purpose for which the data was collected and retained, namely for the purposes of law enforcement and national security.

7. Applications for orders, such as orders for preliminary discovery, have been restricted to a very limited class of information held by carriers or ISPs, especially information that identifies subscribers associated with IP addresses. This strongly suggests that there is no case for allowing access to all categories of data identified in s 187AA of the TIA Act.

8. Consideration should therefore be given to the possibility of simplifying the distinction between telecommunications metadata which can be accessed for use in civil proceedings and data which cannot be accessed by restricting applications for access to specific kinds of data, such as data identifying a subscriber and linking the subscriber to an IP address. For the most part, this would be telecommunications data that would be held by a carrier or CSP for its own business purposes, and not retained solely due to the obligations imposed under the data retention regime.

9. In the event that some data sought in applications for preliminary discovery would not have been retained except for the data retention regime, the prohibition should remain as, apart from the data retention regime, this data would not otherwise have been available. The continuation of the prohibition would therefore not impose undue hardship on applicants in civil proceedings, and strike a balance between the protection of privacy of subscribers and the rights of potential litigants in civil suits.

10. Given the importance of privacy considerations in applications for preliminary discovery for information or documents held by carriers or CSPs, consideration should be given to introducing reforms to laws relating to preliminary discovery, such as rule 7.22 of the *Federal Court Rules 2011* (Cth), which expressly require considerations relating to privacy to be taken into account in the exercise of the Court's discretion to grant preliminary discovery.

In summary, the main recommendations made by this submission are:

1. The PJCIS review of the data retention regime, mandated by s 185N of the TIA, should be brought forward so as to properly address the significant privacy implications of the scheme, and assess these in the context of information arising from the implementation of the regime.

2. The prohibitions on the use or disclosure of telecommunications data for the purpose of civil proceedings in s 280(1B) and ss 281(2) and (3) of the TA should be retained unchanged.

3. There is no case for the relaxation of the prohibitions by means of regulations made pursuant to s 280(1B)(v) and s 281(2)(v). In the absence of compelling information relating to the data that may be retained by carriers and CSPs solely for the purpose of the data retention regime, and the need for access to such data by potential litigants, there is simply no case for relaxing the statutory prohibitions even in the most serious civil cases. Retaining the prohibitions in the current form will ensure that unnecessary costs are not imposed on carriers and CSPs; spare the scarce resources of courts that may otherwise be squandered on 'fishing expeditions' by vexatious litigants; and constrain questionable practices such as 'speculative invoicing'.

4. There is a case for further restricting access to the data set specified in s 187AA so that use and disclosure is confined to data that are relevant to applications for preliminary discovery in civil proceedings. This would have a number of advantages. It would simplify the process of determining whether or not the prohibition applies to particular data. It would also ensure that a better balance is struck between the privacy rights of telecommunications users and the rights of potential litigants.

5. There is a case for reviewing Part 13 of the TA to ensure it is fit for purpose in the context of the mass collection of revelatory telecommunications metadata. The telecommunications-specific privacy regime has not been reviewed since the 2008 ALRC report, *For Your Information.* Since then, there have been very significant changes in the collection and use of telecommunications metadata, posing considerable challenges for the protection of privacy, but without proper attention to law reforms to better protect privacy. In short, the changes in practices in this area are so significant that proper consideration of the issues raised by this review is best undertaken in the context of a fundamental review of the regulatory regimes that apply to telecommunications data.

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/