

NOTICE OF FILING

This document was lodged electronically in the FEDERAL COURT OF AUSTRALIA (FCA) on 17/08/2016 5:02:20 PM AEST and has been accepted for filing under the Court's Rules. Details of filing follow and important additional information about these are set out below.

Details of Filing

Document Lodged:	Outline of Submissions
File Number:	VID38/2016
File Title:	Privacy Commissioner v Telstra Corporation Limited
Registry:	VICTORIA REGISTRY - FEDERAL COURT OF AUSTRALIA



Dated: 17/08/2016 5:02:30 PM AEST

A handwritten signature in blue ink that reads 'Warwick Soden'.

Registrar

Important Information

As required by the Court's Rules, this Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date and time of lodgment also shown above are the date and time that the document was received by the Court. Under the Court's Rules the date of filing of the document is the day it was lodged (if that is a business day for the Registry which accepts it and the document was received by 4.30 pm local time at that Registry) or otherwise the next working day for that Registry.



**IN THE FEDERAL COURT OF VICTORIA
AT MELBOURNE
GENERAL DIVISION
COMMERCIAL COURT**

No VID 38/2016

PRIVACY COMMISSIONER

Applicant

And

TELSTRA CORPORATION LTD ABN 33 051 774 556

Respondent

SUPPLEMENTARY OUTLINE OF SUBMISSIONS BY AMICUS CURIAE

Legal Principles: Amicus Applications

1. This is an exceptional case. It requires ‘the elucidation of complex questions of legal principle and legal policy, as well as of decided authority’¹ both domestically² and internationally. The determination of the scope of ‘*personal information*’³ in the digital environment, and in the context of not only digital data but metadata, is both the most difficult and important legal issue in information privacy law and carries with it economic and political implications for Australia and Australian ‘organisations’.⁴
2. It is not contended by the Potential Amicus Curiae (**Amicus**) that the parties are unable or unwilling to adequately protect their own interests, but rather that it may not be necessary for the parties to ventilate the broader domestic and international policy considerations in order to protect those interests.⁵ Indeed, in Telstra’s submissions filed in this Appeal areas of legal policy and international precedent have not been traversed in detail, while those of the Privacy Commissioner deal with overseas jurisprudence peripherally to its substantive submissions⁶.
3. The Amicus seeks to assist the Court in its task of resolving the issues by drawing attention to only those aspects of the case (and potential ramifications) that have not been dealt with by the parties, and that might otherwise be overlooked.⁷ The Amicus is equipped to offer the specialist knowledge of the domestic and international framework necessary to assist the Court

¹ *Levy v Victoria* (1997) 198 CLR 579 at 650-651 per Kirby J.

² The definition of "Personal Information" is an intrinsic part of State information privacy legislation including the *Privacy and Data Protection Act 2014* (Vic) s. 3, the *Health Records Act 2000* s.3, the *Information Privacy Act 2009* s 12 (Qld) and the *Privacy and Personal Information Protection Act 1998* (NSW) s.4. The definition of "personal information" is substantially similar to that found in the Commonwealth *Privacy Act 1988*. The scope, and possible limitation, of the definition of personal information will impact on the administration of those Acts.

³ Known in some jurisdictions as ‘personal data’

⁴ Discussed in detail below.

⁵ *Kruger v Commonwealth* (HCA, Full Court, 12 February 1996, unreported).

⁶ See Applicants submissions at paragraphs 23 - 26 and submissions in reply at paragraph 13.

⁷ *Bropho v Tickner* (1993) FCR 165 at 172 per Wilcox J; *Lange v* (1997) 189 CLR 579 at 604-605 Per Brennan CJ; see also *Wilson v Manna Hill Mining Co Pty Ltd* (2004) 51 ACSR 404; [2004] FCA 1663 at [87]–[89].

in this complex Appeal.⁸

4. The application made by the Australian Privacy Foundation and the New South Wales Council of Civil Liberties for leave to appear as amicus curiae should be granted.

Australia's International Commitments

5. The *Privacy Act 1988* (the '**Act**') embodies the Commonwealth's commitment to, *inter alia*, Article 17 of the International Covenant on Civil and Political Right (**Covenant**)⁹ and the Organisation for Economic Co-operation Council Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.¹⁰ It is human rights legislation,¹¹ an express object of which is to implement Australia's international privacy obligations.¹²
6. The way in which signatory states to the Covenant and OECD member states deal with identification issues is therefore relevant. Conflicting approaches in defining '*personal information*', and to the issues of 'identity' and 'identification', have potential economic and political consequences by impeding the international free flow of information and data.¹³
7. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (**OECD Guidelines**)¹⁴ were developed as a result of concerns about the consequences of inconsistent or competing national data protection laws that had arisen in response to new and automated means of processing data.¹⁵ The preamble to the *Privacy Act 1988* acknowledges that the Council of the OECD (the "**Council**") 'has recommended that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in Guidelines annexed to the recommendation', and that 'Australia ... will participate in the recommendation concerning those Guidelines'.¹⁶
8. The Council updated the OECD Guidelines in 2013 in the Recommendation of the Council

⁸ The objects of the Australian Privacy Foundation and the NSW Council of Civil Liberties is outlined in paragraphs [4] – [8] of the Affidavit of Stephen Joseph Blanks sworn 19 July 2016.

⁹ As outlined in the Preamble in the *Privacy Act 1988*; see also s. 2(A) (a).

¹⁰ The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data considered a key international instrument for data protection standards worldwide since they were agreed in 1980. The Privacy Act 1988 explicitly references them in its language and in the preamble.

¹¹ It is remedial or beneficial legislation that "should be construed so as to give the fullest relief which the fair meaning of its language will allow": *Re Comb* [22], Warren J citing Issacs J in *Bull v Attorney-General (N.S.W.) (1913) 17 C.L.R. 370 at 384*.

¹² Section 2A (h).

¹³ As contemplated by s. 2 (A) (f) of the *Act*. For example, Article 25 of Directive 95/46/EC states that a European Union member should, as a general rule, only transfer personal data to third countries that ensure an 'adequate' level of protection: Directive 95/46/EC of the European Parliament and Council of 24 October 1995 [1995] OJ L 281 (the DPD). This is outlined in further detail below.

¹⁴ First introduced On 23 September 1980.

¹⁵ Recommendation of the OECD Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013) at page 69.

¹⁶ The 1980 OECD Guidelines recognise the need for regulation concerning the processing of data in a privacy context to be considered in an international context: Article 6 - 8

Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013) (**2013 Guidelines**). ‘Personal Data’ is defined as ‘any information relating to an identified or identifiable individual (data subject)’¹⁷ For the purposes of whether the individual is identifiable, the 2013 Guidelines acknowledge the process of linking of information or data to ascertain the identity, stating:¹⁸

Data can be combined with other data and in the process may make individuals identifiable – sometimes to a high degree of statistical probability. For example, although currently there is some debate about whether IP addresses are personal data, there is an argument to be made in favour of considering it personal data in certain contexts when it is possible to identify an individual by linking an IP address to other information, such as web searches. Information garnered by web searches can also reveal very sensitive information about an individual’s practices, preferences and beliefs. The volume of next generation IP addresses, IPv6, will allow greater use of static IP addresses, thereby potentially increasing the ease with which individuals can be identified.

International jurisprudence

9. The AAT finding that ‘it does not matter whether the information or opinion could be married with other information to identify a particular individual’,¹⁹ and therefore be ‘personal information’, is inconsistent with the approach adopted in foreign jurisdictions.²⁰
10. Internationally, the legal emphasis is upon the capability or potential of identification rather than the actual achievement of identification. A person may, for example, be “identified” when, within a group of persons, he or she is "distinguished" from other members of the group, known as "unique combinations".²¹
11. In determining whether information is ‘about’ an individual, overseas regulation²² and decisions²³ consider whether information can be used alone or in concert with other information as a means of identification.²⁴ In the United Kingdom ‘personal data’ includes data which can lead to possible ‘direct and ‘indirect’ identification.²⁵ Segregating information

¹⁷ Annex clause 1 (b) page 13.

¹⁸ Ibid page 40 – General background; page 69 Transborder data flows; page 81 Current trends in the processing of personal data

¹⁹ Reasons [95]; see also the findings in relation to whether the information was “about an individual” at Reasons [111], - [113].

²⁰ This approach is also inconsistent with the AAT definition is inconsistent with personal information under Part 5 of the Telecommunications (Interception and Access) Act.

²¹ For example: Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136, 20 June 2007.

²² Subsection 2(1) of the Personal Information Protection and Electronic Documents Act (PIPEDA)

²³ *Gordon v Canada (Health)* (2008) FC 258. See also *R. v. Spencer*, 2014 SCC 43 and *R v Cole* [2012] 2 SCR 34

²⁴ A person might still be “identifiable” because that information may be combined with other pieces of information, an approach that has been adopted in Canada: Booth and others, *What are ‘Personal Data’?—A Study Conducted for the UK Information Commissioner* (2004)

²⁵ The UK law implements the EU DPD Directive and article 8 of the Charter of Fundamental Rights of the European Union which guarantees the protection of personal data: *Consolidated Information Services Limited (Formerly Viagogo Limited) (In Liquidation) v The Rugby Football Union* [2102] UKSC 55

into different databases is irrelevant where linkage is possible.²⁶ The fact that the result is identification is the key.

12. Other jurisdictions have incorporated the constant advances in data aggregation and mining capabilities, rather than artificially considering data's "identifiability" in the abstract.²⁷ In that context the Canadian Federal Court stated in *Gordon v Canada (Health)*²⁸:

"...information will be information about an individual where there is a serious possibility that an individual could be identified through the use of that information alone or in combination with other information"²⁹

13. The New Zealand Complaints Review Tribunal interpreted the phrase "about a person" broadly, looking at the "capacity" of information to identify a person, rather than asking the narrower question of whether the individual is identified by the information on its face.³⁰ In *Israel v. Bank Ha'Po'alim*, the Supreme Court of Israel found that, for purposes of privacy law, "the term information... should include data that can be derived from a database which is not indexed according to individual names."³¹
14. In *ACLU v. Clapper*³², the U.S. government argued in its brief that the plaintiffs did not have standing to challenge the NSA's bulk telephone metadata collection program because the possibility that their particular data would be connected to their identities was "speculative."³³ The Second Circuit Court of Appeals disagreed. It found the NSA searched through the files to identify individuals regularly, meaning that plaintiff's records were also "searched" even if they were not the targets of the search.
15. Article 2(a) of the Directive 95/46/EC of the European Parliament and Council of 24 October 1995 [1995] OJ L 281 (the **DPD**) defines 'personal data' to mean:

" any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

16. While the European definition uses the term 'relates' rather than 'about' it is functionally equivalent to the definition of 'personal information' in the *Privacy Act 1988*.

²⁶ *Vidal - Hall & ors v Google* [2015] EWCA Civ 311, [115] and [122] – [124]

²⁷ See *ACLU v. Clapper*, 785 F.3d 787, 794 n1 (2nd Cir. 2015) (considering recent scientific studies which suggested that anonymized metadata could be easily re-identified).

²⁸ (2008) FC 258)

²⁹ at [34]

³⁰ *Proceedings Commissioner v. Commissioner of Police*, [2000] NZAR 277 <http://www.austlii.edu.au/cgi-bin/LawCite?cit=%5b2000%5d%20NZAR%20277>

³¹ EU Data Protection Working Party, *Opinion 6/2009 on the level of protection of personal data in Israel*, (2009), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf

³² Case 14-42, Document 168-1

³³ Brief of Defendants-Appellees, *ACLU v. Clapper*, at 54 (2014).

17. Article 4(1) of the DPD states that a person is one who can be identified ‘directly or indirectly’ by reference to an identifier such as name, an identification number, *location data*, *an online identifier...*”.
18. Recital 26 of the European Data Protection Regulation provides that even information that has undergone pseudonymisation should be considered information on an identifiable natural person and to determine whether a natural person is identifiable, regard is had to all the means reasonable likely to be used such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. Recital 30 specifies that ‘natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifier.
19. The recent opinion of Capos Sánchez-Bordona in the case of *Patrick Breyer v Bundesrepublik Deutschland*³⁴ stated that for data to be considered ‘personal data’ it is not necessary for means of identification to be held by a single entity. The issue was whether ‘dynamic’ IP addresses which a service/content provider stores when their website is accessed constitute personal data if a third party, in this case a service provider, has the additional knowledge required in order to identify the data subject. The Opinion stated that even if a single entity is subjectively incapable of identifying a person from a particular IP address, that does not eliminate the risk for the data subject and should not exclude that data from the definition of personal data. In that context the third party must be a party that could ‘reasonably’ be approached by the entity holding the data in question for the purpose of seeking data to facilitate identification. A telecommunications provider such as Telstra would similarly satisfy that threshold, being a party that may be required or requested to lawfully provide that data.³⁵
20. The definition of ‘reasonableness’ is determined by the existence of an accessible third party having the means necessary to facilitate identification of a person, not the possibility that an approach would be made to that third party³⁶. The Opinion specifically considered the potential of data being warehoused separately in order to avoid being defined as personal data.
21. In the United Kingdom the *Data Protection Act 1998* (UK) (the ‘**DPA**’) is intended to implement the DPD. Section 1(1) of the DPA provides:
- “ personal data” means data which relate to a living individual who can be identified—
- (a) from those data, or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the

³⁴ C-582/14 the full CJEU decision is forthcoming

³⁵ *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* s. 187 C.

³⁶ [76]

data controller...”

22. In *Google Inc. v Vidal-Hall*³⁷, the English Court of Appeal considered whether Browser Generated Information (BGI) collected by the Apple Safari Browser was ‘personal data’ under section 1(1) of the DPA. The BGI allowed Google to recognise the particular browser used by the Internet user and, accordingly, to personalise advertising. The Court found there was a serious question to be tried as to whether BGI amounted to personal data. It was immaterial that the BGI did not identify an individual in the sense of naming them. What was important was that the data “ ‘individuates’ the individual, in the sense that they are singled out from all others’.³⁸ It was arguable that the BGI singled out individual Internet users. The fact that the entity holding the information segregated the data in question from any other databases that could be used for linking in order to facilitate identification was irrelevant.³⁹ The issue is whether ‘the defendant has “other information” actually within its possession which it could use to identify the subject of the [Browser Generated Information], regardless of whether it does so or not.’⁴⁰
23. In *Vidal-Hall* the BGI included two forms of metadata: detailed browsing histories, including the websites visited and the dates and times the websites were visited and a unique identifier in the form of a ‘cookie’. By combining that metadata, the Court held, Google could to single out individual users as it allowed it to determine:
- (i) the unique ISP address of the device the user is using i.e. a virtual postal address; (ii) what websites the user is visiting; (iii) when the user is visiting them; (iv) and, if geo location is possible, the location of the user when they are visiting the website; (v) the browser’s complete browsing history; (vi) when the user is online undertaking browser activities.⁴¹
24. The European Union Article 29 Working Party (**Art 29 WP**), an expert advisory body established under Article 29 of the DPD, published *Opinion 4/2007 on the concept of personal data*,⁴² (“**Art 29 Opinion**”) which considered whether or not an Internet Protocol address (**IP address**) amounts to ‘personal data’. An IP address is a 32-bit⁴³ or 128-bit⁴⁴ number that identifies a computer or device connected to the Internet. An IP address can be either static or dynamic. Where the same IP address is allocated each time a computer accesses the Internet it

³⁷ [2015] EWCA Civ 311

³⁸ Para [115].

³⁹ Ibid [122] – [124].

⁴⁰ Ibid [124].

⁴¹ Ibid.

⁴² Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, Adopted on 20 June 2007, 02148/07/EN, WP136.

⁴³ The IP address scheme used in Internet Protocol Version 4. It is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. It is designed for use in interconnected systems of packet-switched computer communication networks.

⁴⁴ The IP address scheme used in Internet Protocol Version 6 (IPv6), also called IPng (*Internet Protocol next generation*). It is the newest version of the Internet Protocol IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons

is known as a static IP address. A dynamic IP address is where a new IP address may be assigned each time a computer accesses the Internet.⁴⁵ Although it is easier to establish a link between an IP address and an Internet user with a static IP address, it is possible to identify a user from combining a dynamic IP address with other information.⁴⁶

25. The Art 29 Opinion determined that individual Internet users were reasonably identifiable from IP addresses, stating:

Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically “log” in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive ...).⁴⁷

26. The Art 29 Opinion considered that where a third party, such as a copyright holder, processes an IP address for the purpose of identifying an Internet user, there would be “means reasonably likely to be used” to identify the relevant persons. Notwithstanding there are circumstances which would make identification more difficult, all IP addresses should be treated as personal data.⁴⁸

27. In 2008 the Art 29 WP concluded⁴⁹ that dynamic IP addresses should be treated as personal data where a user was reasonably identifiable from the IP address together with other accessible data, stating:

Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.⁵⁰

28. It found that a dynamic IP address in the hands of a search engine operator should *a fortiori* be considered personal data where it is processed by an ISP or mobile carrier.
29. European Union Jurisprudence has already established in *Scarlet Extended v Societe belge des auteurs, compositeurs et editeurs* (SABAM)⁵¹ that IP addresses were personal data when

⁴⁵ The assigning, reassigning and modification of dynamic IP addresses is managed by a Dynamic Host Configuration Protocol (DHCP) server. One of the primary reasons behind having dynamic IP addresses is the shortage of static IP address on IPv4. Dynamic IP addresses allow a single IP address to be moved between many different nodes to circumvent this problem.

⁴⁶ For example where identification can be made by an Internet Service Provider or mobile carrier a dynamic IP address.

⁴⁷ Ibid. p 16.

⁴⁸ Ibid. p 17.

⁴⁹ Article 29 Working Party, *Opinion 1/2008 on data protection issues relating to search engines*, Adopted on 4 April 2008, 00737/EN, WP148.

⁵⁰ Ibid. p 8.

⁵¹ Case C-70/10 [2012] ECDR 4

coupled with other information within the same entity's possession. The French Constitutional Court found IP addresses to be personal data⁵².

30. The principles behind the international authorities and approaches to IP addresses are applicable to telecommunications data, including meta data, the subject of this appeal. It illustrates that the determination of what is 'personal information' for the purposes of the *Privacy Act 1988* must be to a technological neutral interpretation. This is an approach not adopted by the AAT.

Technical identification issues

31. Database aggregation techniques permitting identification from any particular data point were ignored by the AAT.⁵³ An individual subjectively incapable of identification from a single data point, such as a particular IP address, can be identified by reference to other data points.⁵⁴ It is in this context that the relationship between meta data and privacy must be understood.⁵⁵
32. The comparison of multiple systems of records used to aggregate data about an already identified subject by means of a computer had been described as "data matching"⁵⁶ The means of re-identifying an anonymous database by linking identified databases with anonymous databases has been described as data linking.⁵⁷
33. There are a number of learned articles which may assist the Court's understanding on the technical process of database aggregate and the privacy issues and considerations it raises.⁵⁸
34. This is not a theoretical analysis, as recently there have been high-profile instances where "anonymised" databases were released publicly and researchers were able to link the data back to individuals by combining the anonymised data with information contained in other databases.⁵⁹ These techniques have also been applied on a smaller scale, for example as a way

⁵² Décision n° 2009-580 DC du 10 juin 2009 however not in Ireland Ireland: EMI & Ors v Eircom Ltd[2010] IEHC 108

⁵³ Example: The PII Problem: Privacy and a New Concept of Personally Identifiable Information *New York University Law Review*, Vol. 86, p. 1814, 2011, Radio Frequency Identification and Privacy Law: An Integrative Approach *American Business Law Journal*, Vol. 46, No. 1, Spring 2009

⁵⁴ *Canada (Information Commissioner) v Canada (Transport Accident Investigation and Safety Board)* [2006] FCA 157

⁵⁵ References include Office of the Privacy Commissioner of Canada, *Metadata and Privacy: A Technical and Legal Overview*, October 2014, Available at: https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.pdf. See also AOL Breach from aggregation referred to in Michael Barbaro and Tom Zeller Jr, A Face is Exposed for AOL Searcher No:4417749 (9 August 2006) *New York Times* http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&. See also Stanford Study: Jonathan Mayer, Patrick Mutchler and John Mitchell, "Evaluating the privacy concerns of telephone metadata (2016) 113 *Proceedings of the National Academy of Sciences* 20, 5536.

⁵⁶ Daniel Steinbock 'Data Matching, Data Mining, and Due Process' (2005) 40 *Georgia Law Review* 1, 10.

⁵⁷ Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review* 1701, 1724.

⁵⁸ See articles in footnotes 56 and 57 above. See also Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets', (2008) PROC. OF THE 2008 IEEE SYMP. ON SECURITY AND PRIVACY 111, 119; and Bradley Malin, 'Betrayed by my Shadow: Learning Data Identity via Trail Matching' (2005) *Journal of Privacy Technology* 1.

⁵⁹ See page 97 2013 OECD Recommendations and "A Face Is Exposed for AOL Searcher No. 4417749", www.nytimes.com/2006/08/09/technology/09aol.html ; Latanya Sweeney, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy Working Paper, LIDAP-WP4 (2000); Arvind Narayanan and Vitaly Shmatikov, How to Break the Anonymity of the Netflix Prize Dataset, 16 October, 2006, <http://arxiv.org/abs/cs/0610105>. Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review* 1701,

to identify various types of data, including anonymous social network data.⁶⁰

Data Retention Laws

35. Under s. 187LA (2) of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* information that is kept under Part 1 of that Act, is taken for the purposes of the *Privacy Act 1988*, to be personal information about an individual if the information relates to an individual, OR is a communication to which the individual is a party.
36. Under s 187 AA the information that must be kept includes:
 - (a) “any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service;
 - (b) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device
 - (c) Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred;
 - (d) The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service
 - (e) The type of communication i.e. voice, sms, email, chat ...
37. The meta data the subject of this appeal is data that must be kept for the purposes of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. It is deemed to be ‘personal information’ for the purposes of the *Privacy Act 1988*. This is consistent with the way in which international jurisdictions deal with data of this nature. The approach adopted by the AAT is, however, inconsistent.

Political and Economic Consequences

38. A failure to apply an approach to the definition of ‘personal information’ consistent with international guidelines and jurisprudence, may have significant legal and economic consequences. For example, under Article 25(1) of the EU Directive 95/46/EC (also known as the ‘Data Protection Directive’ (“DPD”))⁶¹ transfers of personal data from European Union member states to a third country may take place only if the recipient ensures an adequate level of protection. Article 25(6) establishes a mechanism for the European Commission to

1718; Paul Schwartz and Daniel Solove, ‘The PII Problem: Privacy and the New Concept of Personally identifiable Information’ (2011) 86 *NYU Law Review* 1815, Arvind Narayanan and Vitaly Shmatikov, ‘Robust De-Anonymization of Large Sparse Datasets’, (2008) PROC. OF THE 2008 IEEE SYMP. ON SECURITY AND PRIVACY 111, 119.

⁶⁰ Arvind Narayanan and Vitaly Shmatikov, ‘De-Anonymizing Social Networks’, available http://userweb.cs.utexas.edu/~shmat/shmat_oak09.pdf.

⁶¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [1995] OJ L 281.

determine that a third country ensures an adequate level of protection.

39. In *Maximillian Schrems v Data Protection Commissioner* Case⁶² the Court of Justice of the European Union held that, to comply with the adequacy test, a third country must ensure a level of protection ‘essentially equivalent’ to that conferred by European Union members. The adequacy standard is preserved by Article 45 of the recently enacted General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).
40. An overly restrictive approach to the definition of ‘personal information’ in the Act, such as the definition given by the AAT, may jeopardise the Australia information privacy regime being considered adequate, and therefore be a catalyst for bans on data flows between the EU and Australia. Such a restriction would have economic consequences for Australian organisations that operate in digital commerce and the digital economy.

Interpretation of Remedial Legislation

41. The *Privacy Act 1988* is remedial or beneficial legislation.⁶³ It should be interpreted liberally and in a way that will not only promote the purpose and objects of the *Act*,⁶⁴ but “should be construed so as to give the fullest relief which the fair meaning of its language will allow”.⁶⁵ It is to be given a fair, large and liberal interpretation rather than one which is ‘literal’ or ‘technical’.⁶⁶
42. The objects of the *Privacy Act 1988* include to promote the protection of privacy of individuals⁶⁷ and to implement Australia international obligations in relation to privacy.⁶⁸ These objects will be achieved through an interpretation being given the term ‘personal information’ which is consistent with the realities of modern technology and consistent with the approach adopted internationally by signatory states to the Covenant and member states of the OECD.

Michael Rivette

Peter A Clarke

Counsel for the Prospective Amicus Curiae

17 August 2016

⁶² (C-362/14, 6 October 2015)

⁶³ *A remedial or beneficial statutory provision is one that gives some benefit to a person and thereby remedies some injustice: Re Comb* [1999] 3 VR 485, [22] per Warren J (As her Honour then was).

⁶⁴ *S. 15AA Acts Interpretation Act 1901*. The objects of the *Privacy Act 1988* are

⁶⁵ *Re Comb* [22], Warren J citing Isaacs J in *Bull v Attorney-General (N.S.W.) (1913) 17 C.L.R. 370 at 384*.

⁶⁶ *I W and the City of Perth* (1997) 191 CLR 1 at 12 per Brennan CJ and McHugh J.

⁶⁷ S. 2A (a)

⁶⁸ S. 2A (h)