Access to Retained Data in Civil Proceedings

Submission to Government Consultation

Prepared by Adam Fletcher and Melissa Castan

January 2017

Introduction

The Castan Centre for Human Rights Law thanks the Australian Government for the opportunity to comment on s 280(1B) and ss 281(2) and (3) of the *Telecommunications Act 1997* (Cth). The explanatory material to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, which inserted these sections, states that their purpose is to ensure that data which has been collected under the data retention regime (and not for other purposes) cannot be disclosed by service providers to litigants in civil proceedings, subject to some exceptions.[1] This is consistent with other data retention regimes, such as those in many European countries.[2]

We have been invited to comment on the operation of the data release prohibition in the context of the 'effective operation of the civil justice system, or the rights or interests of parties to civil proceedings.' Given our expertise, we will focus on the question of how the rights of litigants may best be balanced with the rights of those whose data has been requested. In addition, we endorse the submission and recommendations of the Australian Privacy Foundation (Submission dated 13 January 2017).

In summary, our submission is that the prohibition should be maintained without exception. Personal data[3] being retained (and released) for national security and criminal investigation purposes may constitute a proportional limitation on the right to privacy under international human rights law if rigorously justified, but its release for other purposes would not be a proportional limitation. In addition, release for civil litigation purposes runs counter to the Government's assurances that the data would only be used for investigating the 'most serious crime.'[4] The Attorney-General specifically stated '[b]reach of copyright is a civil wrong. Civil wrongs have got nothing to do with this scheme.'[5] This was the basis on which the public consented to the data retention regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) ('TIA Act'). Expansion of the nature being considered would therefore be an unwarranted change.

---

[1] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, *Third Supplementary Explanatory Memorandum*, para 167.
[2] See eg Spanish *Law 34/2002 on information society services and electronic commerce* (*Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico*) of 11 July 2002, Article 12.
[3] See below for reasons why metadata should be considered 'personal data.'
[4] See eg '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>.
[5] See 'Brandis wrong on copyright and data retention: IP expert,' *Computerworld*, 4 November 2015: <http://www.computerworld.com.au/article/558798/brandis-wrong-copyright-data-retention-ip-expert>.

Rights of Litigants

International Covenant on Economic, Social and Cultural Rights

The International Covenant on Economic, Social and Cultural Rights (ICESCR), to which Australia is party, requires protection of the right of each individual '[t]o benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.'[6] This right finds its expression in Australia's intellectual property regime. In the case of digital content reproduction, the most relevant law is the *Copyright Act 1968* (Cth).

It is said that '[i]ntellectual property regimes seek to balance the moral and economic rights of creators and inventors with the wider interests and needs of the society.'[7] In the context of the present inquiry, this means considering the best balance between the rights of content creators and those of ISP subscribers whose data are being retained. This balancing consideration has already arisen in Europe, where content creators have attempted to use data retention regimes to access subscriber data to sue for copyright breaches.
In *Promusicæ v Telefónica* the European Court of Justice (ECJ) considered how article 17(2) of the *Charter of Fundamental Rights of the European Union,* which requires the protection of intellectual property, should be balanced against privacy rights in the *Charter* (articles 7 and 8). The Court found that article 17 does not:

> …require the Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings, in a situation in which a non-profit-making organisation of producers and publishers of musical and audiovisual recordings has brought proceedings seeking an order that a provider of internet access services disclose to the organisation the identities and physical addresses of certain subscribers, so as to enable civil proceedings to be brought for infringement of copyright.[8]

The ECJ reasoned that a 'fair balance' must be struck between the competing rights, taking into account the principle of proportionality. The Spanish law in question provided:

> 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.[9]

---

[6] ICESCR [1976] ATS 5, article 15(1)(c).
[7] See Chapman, *A Human Rights Perspective on Intellectual Property, Scientific Progress, and Access to the Benefits of Science*, Presentation to American Association for the Advancement of Science, Washington, 1998: <http://www.wipo.int/edocs/mdocs/tk/en/wipo_unhchr_ip_pnl_98/wipo_unhchr_ip_pnl_98_5.pdf>, 1.
[8] *Promusicæ v Telefónica,* Case C-275/06, Judgment of the Court (Grand Chamber), 29 January 2008, para 70.
[9] *Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico* of 11 July 2002, Article 12(3).

The proportionality of restricting privacy rights for those purposes was not questioned, but the ECJ implicitly found that requiring production of retained data to protect IP rights was a disproportionate restriction on other fundamental rights – to protection of personal data and to a private life.[10]

In Australia, the *Dallas Buyers' Club v iiNet* case demonstrated that parties attempting to enforce copyright claims are amongst those who would like access to data retained under the TIA Act regime.[11] The Federal Court noted that, despite privacy concerns, 'nothing…prevents this Court from ordering the ISPs to disclose the information in question.'[12] His Honour Justice Perram observed:

> [The relevant] provisions demonstrate that the privacy of account holders of ISPs is regarded by the Parliament as having significant value. Of course, the Parliament has also accorded significant value to the owners of copyright by enacting the Copyright Act and by giving them the right to sue for infringement.[13]

The court protected privacy, but not because of this legislation.[14] We acknowledge that the *Dallas Buyers Club* case was about access to regular data, not data under the mandatory regime, but believe it is still relevant.

The UN Committee on Economic, Social and Cultural Rights (CESCR) has also noted that IP rights 'are generally of a temporary nature, and can be revoked, licensed or assigned to someone else,' and that they 'primarily protect business and corporate interests and investments.'[15] Where this is the case, and it is not a question of, for example, an author's ability to maintain an adequate standard of living, it may be inferred from CESCR's reasoning that IP rights should not override fundamental human rights such as the right to privacy.

In our submission, and despite the lack of similarly binding privacy rights in the Commonwealth jurisdiction, similar reasoning should be applied in Australia. Further arguments in relation to proportionality and other rights are set out below.

<u>International Covenant on Civil and Political Rights</u>

Parties to civil litigation are entitled to some fair hearing guarantees under article 14 of the International Covenant on Civil and Political Rights ('ICCPR'). In particular, they are entitled

---

[10] *Promusicæ v Telefónica,* Case C-275/06, Judgment of the Court (Grand Chamber), 29 January 2008, para 70.
[11] See *Dallas Buyers Club LLC v iiNet* [2015] FCA 317.
[12] Ibid, para 84.
[13] Ibid, para 85.
[14] Ibid, paras 84-87.
[15] CESCR, *General Comment 17* (2005), UN Doc E/C.12/GC./17, para 2.

to respect for the principle of 'equality of arms,' so that they do not face structural or procedural disadvantages compared with their opponents.

Relevantly, at common law, parties to litigation are entitled to seek the production of documents and other data relevant to their case. The Consultation Paper refers to the 'longstanding power of the courts to order access to relevant telecommunications data in civil proceedings.'[16] However, the data in question has historically been retained by service providers for their own purposes, including customer tracking and network maintenance. The extra data collected under the TIA Act retention regime should not be accessible on the same basis, because it is only being collected by service providers for security purposes. This is data to which neither courts nor litigants would ever have had access without the retention regime, so it does not make sense to say that their proceedings or rights may be impaired if they cannot access it.

The explanatory material for the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 states:

> As the requirement for access depends substantially on the facts and circumstances of each individual civil proceeding, any limit on the availability of such information would have the potential to prejudice the legitimate rights and interests of claimants or respondents in such proceedings.[17]

With respect, any exception carved out under the Regulations to which this statement refers would actually alter the status quo with respect to equality of arms, which is inappropriate. A party's litigation strategy should not depend on access to data which has only been retained for national security purposes. In addition, the explanatory material itself notes elsewhere that the relevant telecommunications data is not currently 'available as an evidentiary source for either party,' and that 'precluding parties' access to a new source of information' does not reduce or limit their current access.[18]

Individuals also have the right to seek and receive information under article 19(2) ICCPR, including information held by public authorities.[19] The UN Human Rights Committee has stated that '[t]he designation of such bodies may also include other entities when such entities are carrying out public functions.'[20] Since the carriage providers are, under the TIA Act retaining data on behalf of the Government, it is probable that the data will come within the definition of 'data held by public authorities' for the purposes of article 19. However, the primary purpose of extending the coverage of article 19 to information held by public

---

[16] *Consultation Paper*, 2.
[17] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, *Third Supplementary Explanatory Memorandum*, para 404.
[18] Ibid, para 169.
[19] See Human Rights Committee, *General Comment 34* (UN Doc CCPR/C/GC/34), 12 September 2011, para 18.
[20] Ibid.

authorities is to give people access to their own information ('personal data; his or her files'), rather than information on opposing parties to litigation.[21]

Rights under article 19 ICCPR may be limited according to paragraph 3, which provides:

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
   (a) For respect of the rights or reputations of others;
   (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Clearly, it would therefore be legitimate under article 19(3)(a) to limit litigants' access to data for the purposes of protecting the privacy and/or reputation of those to whom the data relates. However, such a limitation (as s 280 of the Telecommunications Act effectively imposes) will only be justified if it achieves a proportionate balance between the competing rights.

Concerns have been raised by knowledgeable parties about a 'honey-pot' for litigants in 'Family Law cases and all manner of commercial disputes.'[22] One submission to the JCIS Inquiry noted that '[o]ne investigation of Polish data retention laws found that 'more and more often traffic and location data is requested by the parties in civil disputes such as divorce and alimentary disputes.''[23] This is not necessarily indicative of the Australian experience, but there is also anecdotal information on civil discovery requesting data disclosures from before the TIA Act retention regime was established.[24] The latest AGD report on the operation of the TIA Act does not mention civil proceedings or discovery.[25]

The submission of the Australian Privacy Foundation ('APF') that '[g]iven 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'[26] is compelling. As the APF notes, lawyers will have incentives to request access to potentially exculpate their clients'[27] – in fact, they might actually be negligent if they were to overlook such potential evidence.

---

[21] Ibid.
[22] See *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, Parliamentary Joint Committee on Intelligence and Security, February 2015, para 6.98.
[23] Ibid, para 6.101.
[24] See eg Grubb, 'Data retention a boon for private investigators,' *Sydney Morning Herald*, 4 November 2014
[25] See AGD, *TIA Act, Annual Report 2014-15*.
[26] See *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, Parliamentary Joint Committee on Intelligence and Security, February 2015, para 6.103.
[27] Ibid.

The fact that the Government, in drafting the relevant TIA amendment, chose not to restrict retained data access to investigations of criminal and national security offences (let alone the most serious category of offences) indicates that other reasons for access were foreseen, and tacitly accepted as legitimate. In our submission, this is consistent with article 19 rights. However, for the reasons given below, the threat to privacy presented by the release of personal data for the purposes of civil suits is likely to render it a disproportionate limitation on citizens' rights under article 17 of the ICCPR.

Rights of Individuals Whose Data is Retained/Requested

Commonwealth Law

The *Privacy Act 1988* (Cth) applies to ISPs, requiring them to comply with the Australian Privacy Principles (APPs) in relation to retained data.[28] They are also required to notify customers about the data collection/retention, and the purposes for it.[29] Penalties may be imposed for privacy breaches.[30]

APP 6, on the use or disclosure of personal information, provides that data collected for one purpose must not be disclosed for another purpose. The exceptions to this rule are consent of the person whose data it is, or where disclosure is 'required or authorised by or under an Australian law or a court/tribunal order.'[31]

As such, the Privacy Act is of no assistance to a person whose mandatorily-retained data is being requested (by order of the court) for use in proceedings, civil or otherwise.

International Covenant on Civil and Political Rights

At the outset of any discussion in relation to privacy effects, it must be noted that the new blanket data retention regime is likely a disproportionate response to the security threats faced by Australia. An even more sweeping regime in the US has proven relatively ineffective in averting such threats.[32] The EU Data Retention Directive was invalidated by the ECJ in 2014 due to the unjustified restrictions it placed on citizens' privacy and personal data protection rights.[33] In addition, the Australian Parliament's own Joint Committee on

---

[28] See AGD, *Data Retention: Frequently Asked Questions for Industry,* 33.
[29] Ibid.
[30] Ibid, 34.
[31] APP 6.2(b).
[32] See eg Nakashima, 'NSA phone record collection does little to prevent terrorist attacks, group says,' *The Washington Post*, 12 January 2014.
[33] See EU FRA, *Data retention across the EU*: <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention>.

Human Rights ('JCHR') found in 2015 that the new regime represented a disproportionate limitation on the right to privacy, even with legitimate law enforcement interests in mind.[34]

The retention regime may therefore be an unjustified limitation on Australians' article 17 ICCPR rights in its entirety.[35] However, this broader argument is outside the scope of the present consultation process, so we turn to access by civil litigants.

The data to be retained comes under six categories:

1. Information about the identity of the subscriber of, and accounts, telecommunications devices and other services relating to, the relevant service provided;
2. The source of a communication;
3. The destination of a communication;
4. The date, time and duration of a communication;
5. The type of communication; and
6. The location of the equipment or line used in connection with a communication.[36]

It is likely that all of this data would fall within the definition of either 'personal information' or 'correspondence' for the purposes of article 17 ICCPR.

For the purposes of civil litigation, such data pertaining to opposing parties may be sought to vindicate a certain legal claim. However, data on people who are not party to the litigation may also be sought, broadening the threat to privacy.

The risk of disproportionality when the regime is used for law enforcement purposes was identified by the JCHR after careful consideration. In our view the risk is far greater when the relevant data is used for civil litigation purposes. Given that safeguards, such as (a) limitations on the scope of data collected, (b) mandatory access notification and (c) limiting the period for which data must be retained, have not been bolstered since the JCHR's findings, it is very likely that permitting access for civil litigation purposes would breach Australia's obligation under article 17 of the ICCPR to protect privacy.

---

[34] See JCHR, *Twentieth Report of the 44th Parliament*, March 2015, 45-54.
[35] See further Molnar and Daly, 'What 'safeguards' are in Australia's data retention plans,' *The Conversation*, 5 March 2015: <https://theconversation.com/what-safeguards-are-in-australias-data-retention-plans-38237>.
[36] AGD, *Data Retention: Guidelines for Service Providers* (July 2015)

Conclusion

In summary, we submit that 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, and we do not support the reduction of those prohibitions by means of regulations made under s 280(1B)(v) and s 281(2)(v).

Further we endorse the submission and recommendations of the Australian Privacy Foundation (dated 13 January 2017). That is, it is recommended that further review of Part 13 of the *Telecommunications Act* be undertaken to ensure it is fit for purpose in the context of the mass collection of telecommunications metadata. It would also be appropriate to tighten the prohibitions on the disclosure of telecommunications data for the purpose of civil proceedings, beyond s 280(1B) and ss 281(2) and (3) of the *Telecommunications Act* in order to limit access to only a subset of the data set specified in s 187AA of the Telecommunications (Interception and Access) Act 1979 (Cth).