Access to Retained Data in Civil Proceedings

Submission by the Australian Communications Consumer Action Network to the Attorney-General's Department

27 January 2017

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation

PO Box 639, Broadway NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

Jeremy Riddle
Policy Officer

ACCAN
PO Box 639,
Broadway NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
Contact us through the National Relay Service

Contents

1. Introduction 4
 1.1. Background to the consultation 4
 1.2. Recommendations 5
2. Access to retained data should not be allowed in civil proceedings 6
 2.1. Government commitments and scope creep 6
 2.2. Cost considerations 6
 2.3. Increased privacy risks 7
  2.3.1. Risks posed by metadata to personal privacy and security 7
  2.3.2. Risks of wrongful association and accusation 8
 2.4. A mandatory data breach notification scheme 8
 2.5. Potential impact on the effective operation of the civil justice system? 9
 2.6. A breach of Australian Privacy Principle 3 9
 2.7. Introduction of a Privacy Tort 9
3. Answers to targeted questions 11

1. Introduction

As the national peak body for Australian telecommunications consumers, ACCAN welcomes the opportunity to make a submission on the prohibition of the disclosure of retained data for the purpose of civil proceedings under the *Telecommunications Act 1997* (Cth) (the TA).[1]

This submission will include ACCAN's comments regarding:

- Cost considerations.
- Potential for increasing privacy risks.
- The need for a mandatory data breach notification scheme.
- Potential for adverse impacts on the operation of the civil justice system.
- The need for government to investigate the introduction of a statutory cause of action for serious breaches of privacy in Australia (a privacy tort).
- The perception of scope creep.

ACCAN would like to acknowledge that its submission has been informed to a large extent by consultation with ACCAN members Electronic Frontiers Australia (EFA)[2] and the Australian Privacy Foundation (APF).[3]

The Consultation Paper[4] included three questions for submitters. ACCAN is providing a response to the third question only.

1.1. Background to the consultation

The *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) was amended by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) so that telecommunications service providers are required by law to retain specified data for a period of two years.[5]

The original purpose and justification for the mandatory data retention regime was to support Australian law enforcement and national security.[6] For this reason the Parliamentary Joint Committee on Intelligence and Security (PJCIS) noted specifically in its February 2015 report on the 2014 Data Retention Bill that "it would be inappropriate for the data retained under the regime to be drawn upon as a new source of evidence in civil disputes."[7] The PJCIS therefore recommended

[1] *Telecommunications Act 1997* (Cth), s 280(1B); ss 281(2) and (3).
[2] Electronic Frontiers Australia, Metadata Access for Civil Cases, https://www.efa.org.au/privacy/metadata-civil/
[3] Australian Privacy Foundation, Submission to Attorney-General's Department on Access to Retained Data in Civil Proceedings, January 2016, https://www.privacy.org.au/Papers/DOCA-DataRet-170113.pdf
[4] Attorney General's Department, Consultation Paper – Access to Retained Data in Civil Proceedings, December 2016.
[5] The types of data required to be retained are set out in s 187AA of the TIA Act.
[6] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Revised Explanatory Memorandum at [25].
[7] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, at [6.115].

that parties in civil proceedings should be prohibited from accessing data retained by a service provider only for the purposes of complying with the data retention regime.[8]

The PJCIS also recommended that the 2014 Bill be amended to include regulation-making powers to allow the creation of exclusions to the prohibition, citing family law proceedings involving violence or international child abduction as examples of when such exclusions could be made. The PJCIS suggested that the Minister for Communications and the Attorney-General review and report on this measure to Parliament by the 13 April 2017.[9] The focus of the current consultation is whether there is a case for such regulations to be made.

1.2. Recommendations

Recommendation 1: That there is no expansion of access to retained telecommunications data for any civil proceedings.

Recommendation 2: That the Government instigates an urgent review into the efficacy of the Mandatory Data Retention Scheme as soon as possible.

Recommendation 3: That the Government ensures a comprehensive and adequate Mandatory Data Breach Notification Scheme is introduced as soon as possible.

Recommendation 4: That the Government instigates a Parliamentary Committee to consider the introduction of a statutory cause of action for serious invasions of privacy (a privacy tort) as a matter of urgency.

[8] Ibid, Recommendation 23.
[9] Attorney General's Department, Consultation Paper – Access to Retained Data in Civil Proceedings, December 2016.

2. Access to retained data should not be allowed in civil proceedings

2.1. Government commitments and scope creep

The Attorney-General's Department will be well aware of Attorney-General George Brandis' comments on the ABC's *Q&A* program in 2014 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, only as a tool, only to crime and only to the highest levels of crime. *Breach of copyright is a civil wrong.* ***Civil wrongs have nothing to do with this scheme.***"[10] [emphasis added]

The APF outlined its concerns about scope creep in its submission to the PJCIS inquiry into the Data Retention Bill.[11] It noted the likelihood that there would be "immense pressure for the data to be used in both civil and criminal legal proceedings by parties who are not authorised to access the data under the TIA Act". In relation to civil proceedings it wrote that the large amount of data to be retained by service providers under the data retention regime would be highly attractive to multiple actors, including "parties to disputes in family law, and in all manner of commercial disputes (involving, for example, trade secrets, intellectual property, and defamation)."

ACCAN would like to echo the APF's concerns surrounding the Government's apparent commitment in 2014 not to extend access to parties in civil proceedings, and surrounding scope creep. Extending access in this way is entirely against the initial justifications of the data retention regime, and would represent another step in the gradual narrowing of individuals' privacy rights in Australia.

2.2. Cost considerations

An additional consideration is who would need to bear the costs of requiring service providers to process requests for data in certain civil proceedings, given that in each case they will need to differentiate between the data they are retaining only under the requirements of the data retention regime and the data they are retaining for operational purposes. If the costs of processing such requests are to fall with the service providers, there is a possibility that they will flow down to consumers.

Another cost to be borne is that of creating the management and operational systems and procedures to grant access to retained metadata. If service providers are required to grant access to

[10] Australian Broadcasting Corporation, *Q&A*, 'National Security: Finding a Balance', 3 November 2014, http://www.abc.net.au/tv/qanda/txt/s4096883.htm

[11] 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, at 15-16.

civil litigants automated systems and staff procedures will likely need to be created, at a potentially high cost that could also disadvantage consumers.

It is also worthy to note that civil litigation is undertaken for a range of reasons whereas crime and terrorism prevention are expected by the community to only be undertaken in the case of serious risk. By extending access to retained data the amount of access requests would likely increase significantly, with the associated costs likely borne by consumers.

Therefore it is in the interests of telecommunications consumers that data retained only for the purposes of the data retention regime is not made available in civil proceedings.

2.3. Increased privacy risks

Extending access to retained data in civil proceedings would increase the risk of privacy breaches and of detriment to consumers. The service providers required by the mandatory data retention regime to hold data have sophisticated data security and privacy measures in place. Opening access to civil cases would likely increase the frequency at which this data is released to third parties, who may not hold the data in an equally secure environment. Once data is released into the public sphere it is notoriously difficult to contain.

Given that the data in question is likely to be exchanged in a digital form, the risks are exacerbated further: the closed systems that exist to exchange data between the high-trust realms of law enforcement and service providers do not exist between the potentially large number of civil litigants and service providers. Interconnecting these systems may undermine law enforcement systems.

2.3.1. Risks posed by metadata to personal privacy and security

In its submission to the current consultation the APF notes the importance of recognising the legal and policy challenges arising from the recent massive increase in the proliferation of telecommunications metadata.[12] Its submission provides a number of quotations on the ways in which telecommunications metadata can be used to paint a very clear picture about an individual, and notes that the constantly growing amount of metadata:

> "…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."[13]

Extending access to the data in question to parties in civil cases and thus increasing the likelihood of a data breach can have serious consequences for parties in family law disputes. Take for example a victim of domestic violence who for their own safety needs to keep their location private. Metadata released about a mobile service could identify the victim and their location to the offending party, potentially allowing the perpetrator to track the movements of the victim. This risk was described by

[12] APF, above n 3, at 4.
[13] Ibid, at 5.

President of the Law Council of Australia, Fiona McLeod, on the ABC's *7.30* show on 6 January 2017.[14]

2.3.2. Risks of wrongful association and accusation

With the increasing scarcity of Internet Protocol version 4 (IPv4) addresses, internet service providers are implementing systems that cause IPv4 addresses to be cycled quickly between end users. As a result during any daily interval a significant number of end users may separately use the same IPv4 address, without any of them actually being connected at the same physical location. Unless appropriate levels of proof are required to ensure that the request is for the metadata relating to a named individual at a specific location (and potentially more information) the risk of wrongful association with any particular piece of metadata is potentially high. The responsibility of using and interpreting such data should remain solely with law enforcement agencies and not with lawyers in civil cases.

2.4. A mandatory data breach notification scheme

In its 2013 *Report of the Inquiry into potential reforms of Australia's National Security Legislation* the PJCIS recommended that any data retention legislation should include 'a robust, mandatory data breach notification scheme.'[15] This recommendation was not included in the Data Retention Bill.

At the time the Australian Privacy Commissioner noted that data retention would lead to increased risks of data breach, and that a mandatory data breach notification scheme would be one way of managing this risk.[16]

ACCAN submitted to the Attorney-General's consultation on the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* and maintains the position that a mandatory data breach notification scheme should be introduced as soon as possible.[17] However, if such a scheme is introduced, the APP entity concerned should not be allowed the discretion to decide when there is a 'real risk of serious harm' as proposed by the Bill.

The introduction of such a scheme would reduce the potential for serious data breaches and the loss that these breaches can cause to consumers. Mandatory notification also plays an important role in giving consumers an opportunity to mitigate the potential negative effects a data breach may have on them.

---

[14] Australian Broadcasting Corporation, *7.30,* 'Data retention laws: Experts warn against opening up metadata to civil cases as telcos renew bid to change laws', http://www.abc.net.au/news/2017-01-05/telco-industry-pushes-for-metadata-collection-changes/8162896

[15] PJCIS, *Report of the Inquiry into potential reforms of Australia's National Security Legislation,* Canberra, May 2013, at 192.

[16] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, at p 293.

[17] ACCAN, Submission to Attorney-General's Department on the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015, http://accan.org.au/files/Submissions/ACCAN%20Submission%20Serious%20Data%20Breach%20Notification.pdf

2.5. Potential impact on the effective operation of the civil justice system?

The Consultation Paper states that the PJCIS' recommendation to include a regulation-making power to create exceptions to the prohibition was designed "to mitigate the risk that restricting parties to civil proceedings' access to such data could adversely impact the effective operation of the civil justice system, or the rights or interests of parties to civil proceedings."

As stated by EFA, the data in question has not been retained before and therefore has not been available to the civil justice system. As such ACCAN agrees that:

> "…continuing with the prohibition on using such data for civil cases would simply maintain the status quo, and would therefore, by definition not adversely or otherwise impact the effective operation of the civil justice system, or the rights or interests of parties to civil proceedings."[18]

2.6. A breach of Australian Privacy Principle 3

Another important factor identified by EFA is that data retained *only* due to the requirements of the mandatory data retention scheme is by definition in breach of Australian Privacy Principle 3 from the *Privacy Act 1988*.[19]

Australian Privacy Principle 3 sets out that an Australian Privacy Principle Entity "…must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities."

The principle above includes exemptions for law enforcement and intelligence agencies, which as EFA points out, are the basis of the mandatory data retention scheme. However, these exemptions are not justifiable in relation to civil proceedings. Allowing access to such data in civil cases would therefore represent a blatant breach of Australian privacy law.[20]

2.7. Introduction of a Privacy Tort

The Australian Law Reform Commission in 2006 recommended the introduction of a right to sue for a serious breach of privacy,[21] and subsequently published a 2014 report on how a privacy tort could be implemented.[22] In spite of this, Australia still lags behind other developed countries in allowing its citizens to seek redress when their privacy is breached.

As ACCAN has stated in the past, and as recommended by a multitude of Australian privacy advocates, the Government should increase the privacy protections afforded to Australians through

---

[18] EFA, above n 2.
[19] *Privacy Act 1988*, Australian Privacy Principle 3.
[20] EFA, above n 2.
[21] Australian Law Reform Commission, 'Privacy Law and Practice', https://www.alrc.gov.au/inquiries/privacy
[22] Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era' (ALRC Report 123), 3 September 2014, https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123

the creation of a privacy tort. The NSW Attorney-General is leading a working group and calling for Federal Government action on the introduction of such a tort.[23]

[23] Sydney Morning Herald, ''Only one piece of the puzzle': Baird government calls for national privacy laws', December 10 2016, http://www.smh.com.au/nsw/only-one-piece-of-the-puzzle-baird-government-calls-for-national-privacy-laws-20161207-gt6ibl (accessed 24 January 2017).

3. Answers to targeted questions

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?

No Response.

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?

No Response.

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?

No, the prohibition in 280(1B) should always apply.