Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
Phone: +61 2 6277 2360
Fax: +61 2 6277 2067
pjcis@aph.gov.au

28 June 2019

SUBMISSION TO REVIEW OF THE MANDATORY DATA RETENTION REGIME PRESCRIBED BY PART 5-1A OF THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979* (CTH) ('*TIA ACT*')

Monika Zalnieriute and Genna Churches
UNSW Faculty of Law
Sydney, Australia

About Us

We are researchers working at the intersection between law & technology, human rights and legal theory, collaborating under the *Technologies and Rule of Law* research stream at the UNSW Sydney Faculty of Law.

Dr. Monika Zalnieriute is a Research Fellow at the Allens Hub for Technology, Law & Innovation at the UNSW Sydney Faculty of Law, where she leads an interdisciplinary research stream on *Technologies and Rule of Law*. Monika's research explores the interplay between law, technology, and politics, and focuses on international human rights law Internet policy in the digital age.

Genna Churches is a PhD candidate at UNSW Law. Her thesis, 'The Evolution of Metadata Regulation in Australia: From Envelopes and Letters to URLs and Web Browsing', focuses on the access to and retention of telecommunications metadata, questioning if historical parliamentary debates and legislation of analogous technologies, such as the post and the telephone, have informed the balance between privacy protections and other social objectives in current telecommunications legislation.

The opinions expressed in this submission are the views of the authors, and do not necessarily reflect or present the views or positions of the UNSW Law or Allens Hub.

About this Submission

This submission seeks to respond to the terms of reference raised by Parliamentary Joint Committee on Intelligence and Security in its Review of the Mandatory Data Retention Regime prescribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (CTH) ('*TIA Act*').

As scholars working at the intersection of law and technology, we are somewhat comforted to see the review of the Data Retention Regime, led by the Joint Committee and mandated by legislation,[1] as we believe that reform in this area is important for Australia.

In this submission, we draw upon some of the research conducted by Technologies and Rule of Law stream researchers to make suggestions on how we think the current data retention regime should be reformed. We also seek to provide comparisons with the recent developments in other jurisdictions.

We note that our research does not relate to all questions raised in the terms of reference, and we only set out answers in relation to those matters where our research may be relevant.

We are grateful for the opportunity to present our views and hope this submission will assist the Committee in their important work on this subject. The opinions expressed in this submission are the views of the authors, and do not necessarily reflect or present the views or positions of the Allens Hub or UNSW Law.

---

1 *Telecommunications (Interception and Access) Act* 1979 (Cth) s 187N.

Submission

Introduction

In 2015, the Australian Government amended the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIA Act*') to introduce a statutory obligation for telecommunication and internet service providers ('carriers/CSPs/ISPs') to retain a specific dataset of metadata relating to their subscribers for a period of two years.[2] This data retention scheme was the culmination of rumour and inuendo surrounding a proposed scheme beginning in 2010. Data retention schemes have been part of five different inquiries,[3] four of which questioned the necessity of a data retention scheme and the types of data proposed to be retained[4] and one review which recommended a data retention scheme.[5] The *Amendment* made specific data which once would have fallen under the *Privacy Act 1988* (Cth) retainable for a period of two

---

2 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) ('*DR Act 2015*').

3 Senate Environment and Communications References Committee, Parliament of Australia, *Adequacy of Protections for the Privacy of Australians Online* (2010); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013); Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report to the 44th Parliament* (2014); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) and the Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015).

4 Senate Environment and Communications References Committee, Parliament of Australia, *Adequacy of Protections for the Privacy of Australians Online* (2010); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013); Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report to the 44th Parliament* (2014); and the Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015).

5 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015).

years. This retained data enables agencies to create a comprehensive digital picture of individuals' movements, contacts, interests and associations.[6]

The 2015 *Amendments*[7] made changes to the range of agencies who can access metadata. Initially there were over 80[8] agencies (many not concerned with matters of national security or law enforcement) that could access this information, however, those agencies beyond criminal law enforcement agencies must now be declared an 'enforcement' agency by the Minister.[9] Agencies who can make a request for data are criminal law enforcement agencies including the Australian Federal Police (AFP), and other federal, state and territory agencies.[10] These bodies can still access an individual's metadata without a judicial warrant.[11]

Australia's current data retention regime does not sit comfortably with recent developments in other jurisdictions, such as the EU and USA, and has been described as being 'off with international precedent'.[12] In particular, in the aftermath of Snowden revelations,[13] the Court of Justice of the European Union delivered several ground-breaking judgements related to metadata and data retention, which have resulted in a reform of the data retention regime in the

---

6 Rick Sarre, 'Metadata retention as a means of combating terrorism and organised crime: A perspective from Australia' (2017) 12(3) *Asian Journal of Criminology* 12(3) 167 <https://link.springer.com/article/10.1007/s11417-017-9256-7>; see also Genna Churches 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>.

7 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) ('DR Act 2015').

8 *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2015 Revised Explanatory Memorandum, 3.

9 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 176A.

10 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 110A.

11 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 178-180.

12 Kat Lane, David Lindsay and David Vaile, Australian Privacy Foundation, Submission to Department of Communications and the Arts and Attorney-General's Department (2016) *Review of Access to Retained Data in Civil Proceedings*, 13 January 2016, 15.

13 For an explanation of the Snowden documents in relation to Australia, see, eg, Genna Churches, 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>.

EU.[14] The European Court of Human Rights have also recently ruled that metadata constitutes personal information, and thus is covered by the general proportionality requirement under the rights to privacy jurisprudence and data privacy laws.[15]

Similarly, in the USA, *Carpenter v United States*[16] has found that law enforcement agency access to location data requires a warrant as it is a Fourth Amendment[17] search. The US Constitution now protects location data as it is of the highest level of interference with the individuals' rights, particularly to the expectation of privacy. Location data has reached the same levels of protection as content[18] in the USA, leaving Australian law deficient.[19]

---

14 Monika Zalnieriute, 'Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' (2018) 81(6) *The Modern Law Review* 1046.

15 *Big Brother Watch and Others v The United Kingdom*, 58170/13 62322/14 24960/15.

16 *Carpenter v United States* 585 US 1 (2018).

17 *United States Constitution*, Amendment IV.

18 Such as 'wire-taps' see *Katz v United States*, 389 US 347 (1967).

19 For an explanation of the development of the expectation of privacy from an Australian and US jurisprudence perspective, see, eg, Genna Churches, 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>.

Summary of Recommendations

In this submission, we draw on developments in other jurisdictions and the historical underpinnings of 'telecommunications data' access to respectfully make recommendations to the Committee with respect to the Australian Data Retention and Access regime.

First, we suggest that the Australian bulk data retention for two years is incompatible with the right to privacy and should be reformed. We note the international movements with respect to data retention and access and urge the Committee recognise the shift towards metadata protection, recommending appropriate protections for metadata in line with this international shift.

Second, we suggest a re-definition of 'personal information' under the *Privacy Act 1988* (Cth) to include an explicit acknowledgement that metadata is 'personal information' and thus should be governed/covered by the same protections as any other personal data.

Third, with respect to the inclusion of location data within the retained dataset and access more generally, we urge the Committee to re-consider the current 'non-contents' status of location data, in line with recent US jurisprudence, and recommend that it be excluded from the data set, and prohibited from access without a warrant.

Fourth, with respect to the exclusion of 'web browsing history' from the retained dataset, we acknowledge the historical difficulties with interpretations of such terms and recommend that the Committee consider technologically accurate wording, providing a definition with the inclusion of the acronym 'URL' and potentially destination IP addresses to avoid doubt as to what must *not* be retained.

Fifth, given the historical acceptance that 'URLs' (or 'web browsing history') are content and that a warrant should therefore be required to access 'URLs', we urge the Committee to specifically exclude access to URLs and other data revealing 'web browsing' without a warrant

under the *TIA Act* and *T-coms Act*. Currently, access to URLs and destination IP addresses as part of 'telecommunications data' is not specifically excluded.

Sixth, we recommend that the secondary disclosure provisions be strengthened to prevent the flow of data from declared 'enforcement agencies' to agencies without such status. Further, secondary disclosures should form part the of the annual *TIA Act* reporting measures, including the disclosing agency and the body/agency to which the disclosure was made. Reporting measures should also include a breakdown of the types of data accessed and/or disclosed.

Seventh, we recommend abolishing the content/non-content definition of 'telecommunications data' as it is outdated and unworkable. The legislation should be explicit, stating the type of data to be retained, and mandate deletion after the applicable retention period. It should define the terms 'contents' and 'telecommunications data' and should clearly state what types of data can be accessed without a warrant.

Eighth, we echo the calls for a complete revision of the access to and retention of data and more generally, a complete revision of the *TIA Act* as per Recommendation 18 of the *Inquiry into Potential Reforms of Australia's National Security Legislation*. The revision should also include the *Telecommunications Act 1997* ('*T-coms Act*'). Calls for re-writes, reviews and revisions have been ignored since 2005.

Overall, we urge the Committee to consider the importance of the right or expectation to privacy. We recommend that to protect this vital human right, access to metadata should be permitted only under a judicial warrant, not dissimilar to a Telecommunications Interception Warrant under the *TIA Act*. Further, that data retention should only be considered if there is a demonstrated and proportional need relating to the investigation of the most serious crime and/or national security matters similar to the threshold of offences for the interception of telephone calls under the *TIA Act*.

Recommendation 1 — Indiscriminate Data Retention Regime Should be Recognised as Incompatible with the Right to Privacy

First, we highlight that Australian data retention legislation permitting indiscriminate retention of metadata by communication service providers is incompatible with the right to privacy and especially the information sub-set of it, widely known as data protection or 'data privacy'.[20] This is especially in light of international developments, and in particular, the invalidation of Data Retention scheme in the EU.

On 8 April 2014, the Court of Justice of the European Union ('CJEU'), following numerous earlier judgements by the constitutional courts in Member states, Czech Republic, Germany and Romania, declared the Data Retention Directive[21] retroactively invalid in the *Digital Rights Ireland* case.[22] As explained by Monika Zalnieriute,[23] the CJEU made this declaration based on the disproportionate interference with the European citizens' right to private life and protection of personal data enshrined in Articles 7 and 8 of the *European Union Charter of Fundamental Rights* ('*EUCFR*').[24] The judgment was praised as a victory for fundamental human rights over mass-surveillance in Europe.[25] While the CJEU did not rule on the validity

---

[20] For the differences between privacy and data privacy, as well as definitional issues, see, eg, Monika Zalnieriute, 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 23(2) *International Journal of Law and Information Technology* 99.

[21] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54.

[22] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* [2014] ECR I-238.

[23] Monika Zalnieriute, 'Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' (2018) 81(6) *The Modern Law Review* 1046.

[24] See, Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger*; Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the Directive entered into force.

[25] See, Toumas Ojanen, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance' (2014) 10 *European Constitutional Law Review* 528; Orla Lynskey, 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*' (2014) 51(6) *Common Market Law Review* 1789.

of national laws implementing the invalidated directive in the *Digital Rights Ireland* case,[26] some Member States invalidated their domestic rules[27] and others have amended or introduced new data retention laws.[28] However, they are still in place in some EU countries,[29] and harmonised data retention legal framework has thus been unavailable at EU level since the date of the *Digital Ireland* judgment.

As outlined by Monika Zalnieriute,[30] in 2016, the CJEU delivered in *Tele2 Sverige* judgment where it evaluated the national data retention laws of Sweden and the UK,[31] and extended the *Digital Rights Ireland* reasoning to national legislation[32] by holding that domestic data retention legislation permitting indiscriminate retention of metadata by communication service providers is incompatible with the *EUCFR*.[33] The decision is important not only for addressing the legal status of metadata, which was not explicitly addressed in *Digital Rights Ireland* but on political level it is also predicted to 'exert a lasting impact' for the countries beyond EU, such as USA.[34] In *Tele2 Sverige* the CJEU build on previous judgements in *Digital Rights Ireland* and *Schrems*, as well as constitutional orders from Member States to forge a consensus on data retention, and mass surveillance more generally, in the EU with data privacy at its core.

---

26 European Commission (2015) Statement/15/5654 on national data retention laws, 16 September 2015.

27 For the Netherlands see: ECLI:NL:RBDHA:2015:2498 Rechtbank Den Haag 11 maart 2015 (Stichting Privacy First and others de Staat der Nederlanden); for France see: Arr^et no 84/2015 du 11 jeun 2015.

28 For the UK see: *Data Retention and Investigatory Powers Act 2014* (UK); for Germany see: Corinne Reichert, 'Germany Moves Closer to Data Retention', *ZDNet* (online), 19 October 2015 <https://www.zdnet.com/article/germany-moves-closer-to-data-retention/> (last accessed 11 February 2016).

29 EDRI (2015) Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling (last accessed 11 February 2016).

30 Monika Zalnieriute, 'Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' (2018) 81(6) *The Modern Law Review* 1046.

31 Joined cases C-203/15 and C-698/15 *Tele2 Sverige* [2016].

32 Joined cases C-203/15 and C-698/15 *Tele2 Sverige* [2016] nyr, para 112.

33 Joined cases C-203/15 and C-698/15 *Tele2 Sverige* [2016] nyr, para 112.

34 Isabella Buono and Aaron Taylor, 'Mass Surveillance in the CJEU: Forging A European Consensus' (2017) 76(2) *The Cambridge Law Journal* 250.

Based on these developments, we suggest that bulk data retention regimes are also incompatible with Australia's international obligations to provide domestic laws which protect the right to privacy and more specifically data privacy. Bulk data retention regimes are incompatible with international obligations under the *UDHR*,[35] *ICCPR*[36] and advice from UN Special Rapporteurs[37] and the Office of the High Commissioner.[38] Data retention also stands in contrast to Australia's existing warrant-based system for accessing or recording content,[39] despite metadata being more pervasive.[40]

Further, the retention of individuals' data who have no connection to any investigations concerning serious crime or national security is unnecessary. We suggest that the Australian government would be better served utilising targeted investigation techniques rather than bulk-surveillance. We recommend that the data retention scheme be abolished, and that metadata is treated as 'personal information' as outlined in Recommendation 2.

---

35 *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948) ('*UDHR*').

36 *International Covenant on Economic, Social and Cultural Rights*, opened for signature 16 December 1966, 993 UNTS 171 (entered into force 3 November 1976) ('*IPPCR*').

37 Joseph Cannataci, United Nations Special Rapporteur on Privacy <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx> and Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and Fundamental freedoms while countering terrorism <https://www.ohchr.org/EN/Issues/Terrorism/Pages/SRTerrorismIndex.aspx>.

38 Office of the High Commissioner of Human Rights, 'The Right to Privacy in the Digital Age' (online) < https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>; Office of the High Commissioner for Human Rights, 'Dangerous practice of digital mass surveillance must be subject to independent checks and balances – Pillay' (Media Release, 16 July 2014) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14875&LangID=E**>

39 *Telecommunications (Interception and Access) Act 1979 (Cth)*, eg s 7 not intercepted except by warrant for a serious offence s 5D.

40 Will Ockenden, 'How your phone tracks your every move', *ABC News* (online), 16 August 2015 <https://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152>.

Recommendation 2 — Definition of Personal Data Should Include Metadata

Second, we recommend the *Privacy Act 1988* (Cth) be amended to include an explicit acknowledgement that metadata is 'personal information' and thus should be governed/covered by the same protection as any other personal data. Similar to CJEU in *Tele 2 Sverige*, the status of metadata was recently interrogated by the European Court of Human Rights in *Big Brother Watch v UK*[41] where it held that metadata is just as important as the actual communications content in relation to the right for privacy. As explained by International Association of Privacy Professionals, metadata can be used to identify a person their location and other identifying information.[42]

Therefore, we respectfully suggest that the definition of 'personal information' should to be amended to expressly acknowledge that metadata is capable of being used to identify an individual.

Recommendation 3 — Location Data in Dataset of Retained 'Telecommunications Data'

Third, if the Committee recommends that the data retention scheme continues, location data should be omitted from the data set and assessed as content requiring a warrant to access.

Location data reveals the location of a device through different methodologies based on the connection type of the device. For a mobile phone, location data is automatically generated

41 *Big Brother Watch and Others v The United Kingdom*, 58170/13 62322/14 24960/15.

42 Katelyn Burgess and Towhidul Islam, 'Unpacking Big Brother Watch v UK' (2018) International Association of Privacy Professionals <https://iapp.org/news/a/unpacking-big-brother-watch-v-uk/>; see also Genna Churches, 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>, 9-12.

through cell or tower information as a function of the service.[43] Location data is retainable under s 187AA (item 6) of the *TIA Act*.

Location data associated with a mobile phone can be particularly pervasive, tracking the device from location to location.[44] For example, in *Carpenter v United States*,[45] a suspect's location data was obtained by court order in 2011 from his cell phone provider for a period of 127 days. This data revealed 12,898 data points or an average of 101 data points per day.[46] A data point is a location generated by the cell or tower which the mobile phone has, or is, connecting to. Chief Justice Roberts explained the technology:

> Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI).[47]

The technology works in a similar fashion in Australia and is far more refined now than it was in 2011.[48] The Court found that the accuracy of CSLI was approaching 'GPS-level precision',[49] but was overall more pervasive as: the cell phone is carried with the user, perhaps

---

43 Other types of location data may also be retainable such as for devices connected to the Internet, the IP address can reveal more limited location data, particularly when matched with subscriber data. Devices with Bluetooth capabilities can be logged by MAC address to a location.

44 See especially Will Ockenden, 'How your phone tracks your every move', *ABC News* (online), 16 August 2015 <https://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152>.

45 *Carpenter v United States* 585 US 1 (2018).

46 *Carpenter v United States* 585 US 1, 3 (2018).

47 *Carpenter v United States* 585 US 1, 1-2 (2018).

48 Will Ockenden, 'How your phone tracks your every move', *ABC News* (online), 16 August 2015 <https://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152>.

49 *Carpenter v United States* 585 US 1, 14 (2018).

even into the shower;[50] the phone automatically carries out the surveillance;[51] and the surveillance is retrospective, that is, at any point law in time enforcement bodies can go back through a person's location record retrospectively — that is prior to the person becoming a person of interest. Conversely, a GPS tracker, under US[52] and Australian law,[53] generally requires a warrant and is therefore only prospective.[54]

The Court found that CSLI (location data) was so pervasive that a search warrant based on 'probable cause' was required to access it as it was found to be a Fourth Amendment[55] search. This means that the court order originally obtained by law enforcement agencies based on 'reasonable grounds' that Law Enforcement Agencies believed the records or other information sought were 'relevant and material to an ongoing criminal investigation' was insufficient to protect the expectation of privacy the accused had in his location data.[56] As a result, access to location data has attained the same protections as access to content[57] in the United States. To be clear, prior to this judgement, the US *Stored Communications Act* still required a court order

50 *Carpenter v United States* 585 US 1, 13 (2018).

51 *Carpenter v United States* 585 US 1, 17 (2018).

52 See, eg *United States v Knotts*, 460 US 276 (1983); *United States v Jones* 132 US 945 (2012); for an explanation of these cases see, eg, Genna Churches, 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>.

53 *Surveillance Devices Act 2004* (Cth) s 39; the exception/s being: where there is no interference with the item or property (not generally including installation in a vehicle); recovery of a child; protection from/prevention of terrorism; control orders. See also Revised Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (Cth), 38 [216].

54 For clarity, prospective means from the date of warrant forward in time until the warrant ends, ie data which has not yet been created or generated.

55 *United States Constitution* Amendment IV.

56 *Stored Communications Act* — Required disclosure of customer communications or records, 18 US Code § 2703(d).

57 Such as 'wire-taps' see *Katz v United States*, 389 US 347 (1967); see also Genna Churches 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>.

for the disclosure of non-content and subscriber information (metadata), a substantial increase in the threshold for access compared to Australia.

Location data in Australia has quite an exceptional history. Despite the technology being available and enforcement bodies and other agencies accessing it, there was no specific legislative basis for access prior to 2007.[58]

In 2005, the *Report of The Review of The Regulation of Access to Communications* ('*Blunn Review*')[59] found that:

> Mobile telephones provide location data and the precision of that data can be expected to improve. That data is generated without any specific intervention. The use of that data for Security and Law enforcement purposes is obvious. *The privacy implications are equally obvious. However it is far from clear whether access is subject to any regulation.*[60]

The *Blunn Review* recommended that the privacy implications of access to location data and the lack of legislation surrounding access to it be reviewed 'in the context of the requirement for comprehensive and over-riding legislation dealing with the general issue of access to telecommunications data', and that the entire scheme for access to data be re-written as a separate Act.[61] To date this has not occurred.

---

58 *Telecommunications (Interception and Access) Amendment Act 2007* (Cth).

59 Anthony Blunn AO, Attorney Generals Department, *Report of The Review of The Regulation of Access to Communications*, August 2005 ('*Blunn Review*').

60 Anthony Blunn AO, Attorney Generals Department, *Report of The Review of The Regulation of Access to Communications*, August 2005, 20 [1.1.25] (emphasis added).

61 Anthony Blunn AO, Attorney Generals Department, *Report of The Review of The Regulation of Access to Communications*, August 2005, 20 [1.1.26]

We argue that location data has been wrongly categorised as non-content information or 'telecommunications data' since access to this source of information began. We recommend it be removed from the retention dataset.

We recommend that a warrant be required to access location data, similar to the requirement for a warrant[62] required to install a GPS tracker/locator under the *Surveillance Devices Act 2004* (Cth), removing the current inconsistency between the *TIA Act* and the *Surveillance Devices Act 2004* (Cth). Alternatively, we recommend that the warrant for access be based upon the requirements of the *TIA Act* for a Telecommunications Interception warrant.[63]

Recommendation 4 — URLs or 'Web Browsing History'

Fourth, whilst 'web browsing history' is excluded from the dataset at s 187A(4) of the *TIA Act*, we question the definition of 'web browsing history', particularly as there is no definition provided in the *TIA Act*. Historically, the use of terms such as 'web browsing' and 'URL' has caused confusion with different parties applying their own, at times incorrect, interpretations. For example, 'web address'[64] and 'web pages'[65] have been classified as 'telecommunication

---

62 *Surveillance Devices Act 2004* (Cth) s 39; the exception/s being: where there is no interference with the item or property (not generally including installation in a vehicle); recovery of a child; protection from/prevention of terrorism; control orders. See also Revised Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (Cth), 38 [216].

63 *Telecommunications (Interception and Access) Act 1979 (Cth)*, eg s 7 not intercepted except by warrant for a serious offence s 5D.

64 Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, Friday, 2 November 2012, 14-5 (Catherine Lucy Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department).

65 Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 41 (Catherine Lucy Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department).

data', URLs *were not* contents,[66] URLs *were not* 'telecommunications data',[67] and at other times 'telecommunications data' has included '*Uniform Resource Locators (URLs)* to the extent that they do not identify the content of a communication'.[68] With such inconsistency, we recommend 'Web Browsing History' be defined in the *TIA Act*, specifically including URLs and potentially destination IP addresses.

Recommendation 5 — URLs are already Accessible, with or without Data Retention

Fifth, of further concern is existing access to URLs outside the dataset under Part 5-1A. Despite s 172 of the *TIA Act* prohibiting access to 'contents', in 2013 the Parliamentary Joint Committee on Intelligence and Security were informed that Telstra were providing URLs 'to the extent that they do not identify the content of a communication'[69] and the Attorney-General's Annual reports stated a similar access regime.[70] URLs are content and throughout many years of debate over telecommunication data they have generally been considered as such.[71] The *TIA Act* and '*T-coms Act*' contain no prohibition on access to URLs or 'web browsing history'. To permit access to this form of content is in contravention of s 172, is

---

66 Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 42 (Lionel Wayne Markey, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department).

67 Replacement Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), 8.

68 Attorney-General, Telecommunications (Interception and Access) Act: Report for the year ending June 2008-2011, Commonwealth of Australia.

69 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013), Appendix H.

70 Attorney-General, Telecommunications (Interception and Access) Act: Report for the year ending June 2011, Commonwealth of Australia, 2011, 10.

71 Exceptions relate to debate in 2007: Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), 6; subsequently revised to exclude 'URL/URI' Replacement Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007 (Cth), 8; Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, Canberra, 16 July 2007, 42 (Lionel Wayne Markey, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department).

inconstant with the retained dataset[72] and the privacy concerns raised in Committee reports from 2010 onwards.[73]

We recommend that URLs or 'web browsing history' be specifically prohibited from access without a warrant through amendments to the *TIA Act* and *T-coms Act*.

Recommendation 6 — Secondary Disclosures and Access Reporting Obfuscation

Initially there were over 80[74] agencies (many not concerned with matters of national security or law enforcement) who could access 'telecommunications data', however, with the passage of the *TIA Act Amendment*, those agencies beyond criminal law enforcement agencies must be declared an 'enforcement' agency by the Minister.[75] While the *Amendment* restricts permission to access 'telecommunications data' to enforcement agencies,[76] the *TIA Act* permits those same agencies to access data for imposing a pecuniary penalty or the protection of the public revenue, as well as the enforcement of the criminal law.[77] This may have the effect of obfuscating the true spectrum of access to metadata as requests from agencies not declared enforcement

---

72 *Telecommunications (Interception and Access) Act 1979* (Cth) s 187A(4).

73 All have raised concerns regarding access to URLs, web browsing etc, but most have been comforted by an exclusion of such data in a retained dataset: Senate Environment and Communications References Committee, Parliament of Australia, *Adequacy of Protections for the Privacy of Australians Online* (2010); Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Estimates* (2012); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013); Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report to the 44th Parliament* (2014); Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) and the Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015).

74 Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth), 3.

75 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 176A.

76 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 176A.

77 *Telecommunications (Interception and Access) Act 1979 (Cth)* ss 178 and 179.

agencies could now be made through declared enforcement agencies for a range of different non-criminal law reasons. The data would be passed on through secondary disclosure provisions, which offer little protection to the data.[78] Although a record is required to be kept,[79] secondary disclosures are not part of annual reporting measures.[80] It is therefore unclear what, if any, reduction in access has occurred. We also note that the Annual report to be prepared by the Attorney Generals Department has not yet been released for the period 2017-2018, meaning that valuable reporting information is unavailable for public submissions.[81]

We recommend that secondary disclosures be strengthened to disclose data only for the investigation of serious crime and/or national security[82] matters or may only be disclosed if the same threshold for access under which the data was originally obtained is met. Further, we recommend that all secondary disclosures be reported in the Attorney-General's Annual Report, along with a breakdown of the type/s of data accessed.[83]

Recommendation 7 — Specific Definitions

Seventh, the strained definition of 'telecommunications data' being everything that is *not* 'contents', which is also not defined, does not, has not and cannot work.[84] Technology has

---

78 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 182(3)(a); see, eg, Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report to the 44th Parliament* (2014), 17.

79 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 186A.

80 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 186.

81 <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance> (accessed 21 June 2019); latest report available is for the year ending 30 June 2017.

82 Similar to a Telecommunications Warrant under the *Telecommunications (Interception and Access) Act 1979 (Cth)*, eg s 7 not intercepted except by warrant for a serious offence s 5D.

83 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 186; Attorney-General, Telecommunications (Interception and Access) Act Annual report.

84 Difficulties acknowledged by the Attorney-General's Department; Attorney-General's Department, Submission 26 to Senate Legal and Constitutional Affairs References Committee, *Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, 2015, 45.

moved far beyond the 'letter' and the 'envelope', a time when distinguishing between contents (the letter) and metadata (the envelope) was easy. Today, the new ways in which people communicate generates types of data which, if accessed, grant insights into their movements, interactions and daily activities which could not have been contemplated by legislators from previous generations.

Further, the argument that 'technology neutral' definitions have prevented constant revisions to the *Act/s* has been shown to be a fallacy with the *TIA Act* being amended 68 times since the *Cybercrime Act 2001* (Cth) (3.77 times per year for 18 years) and the *T-coms Act* 57 times since the *Communications and the Arts Legislation Amendment Act 2001* (Cth) (3.16 times per for year for 18 years). In fact, the inclusion of provisions in the *TIA Act* to permit changes to the dataset[85] and the declared enforcement agencies[86] appears to provide an avenue for rapid inclusion of changes without waiting for a sitting of Parliament.[87] We argue that there is now no barrier to providing specific data types and definitions of terms such as 'telecommunications data' and 'contents'.

We recommend that 'telecommunications data' and 'contents' be defined, omitting the current negative descriptor of 'non-contents' information. If the data retention scheme is to continue, then the dataset should specifically state the data to be retained, along with definitions of that data, and the date after which the data *must* be deleted.[88] Only with factual understandings of the precise data retained and accessible can the interference with the right to privacy truly be measured.

---

85 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 187AA(2)

86 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 176A.

87 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 Revised Explanatory Memorandum 8, [39].

88 The exception to the deletion date must only be where the data is required to be retained under a different act, such as for taxation compliance.

Recommendation 8 — Access to Data and/or *TIA Act* and *T-coms Act* should be Re-written

Eighth, copious revisions to both the *T-coms Act* and the *TIA Act* have resulted in a miscellany of provisions which create duplication, confusion, conflict and issues with interpretation. In fact, the *Blunn Review* in 2005;[89] the Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice Report 108* in 2008,[90] the *Inquiry into Potential Reforms of Australia's National Security Legislation* at Recommendation 18;[91] the minority report of the *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979*[92] and a plethora of submissions to inquiries held in 2010, 2013 and 2015 have called for the *Act/s* to be reviewed, revised and/or rewritten.

We concur with the above Reports and Inquiries, and recommend that Recommendation 18 of the *Inquiry into Potential Reforms of Australia's National Security Legislation* be actioned, with a full revision of the *TIA Act* undertaken immediately. We recommend that this revision also include the *T-Coms Act*.

---

89 Anthony Blunn AO, Attorney Generals Department, *Report of The Review of The Regulation of Access to Communications*, August 2005, Recommendations, 10; Recommendation (i) 'comprehensive and over-riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established' amongst other recommendation for review.

90 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice Report 108 (2008) Recommendation 71-2.

91 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) Recommendation 18.

92 Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (2015) Minority Report (Senator Ludlam).

Recommendation 9 — Recognise the Importance of the Right to Privacy

Legal academics, UN special rapporteurs, and jurisprudence in Europe and the USA have recommended protections for metadata to protect the right or expectation of privacy or data protection.[93] It is difficult to understand why Australia is moving against the tide of international recognition of the right to privacy and failing to recognise the ability of retention and/or warrantless access to metadata to erode that right.

All jurisdictions, including Australia, recognise that the right to privacy is proportional to the safety, security and protection of citizens and society. The Explanatory Memorandum stated:

> Telecommunications data is central to virtually every counter-terrorism, organised crime, counter-espionage and cyber-security investigation, as well as almost every serious criminal investigation, such as murder, rape and kidnapping. Telecommunications data is increasingly important to Australia's law enforcement and national security agencies, allowing agencies to determine how and with whom a person has been communicating.[94]

There are further remarks throughout the Explanatory Memorandum[95] regarding telecommunications data access by law enforcement and security agencies and the proportionality of that access with the pressing need to address crime. However, when access to metadata occurs for minor offences or even fines, the balance of access versus privacy should be weighted in favour of privacy. Access to metadata for minor offences, fines, and other non-

---

93 See, eg, Monika Zalnieriute 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 23(2) *International Journal of Law and Information Technology* 99; Genna Churches, 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <https://espace.cdu.edu.au/eserv/cdu:46190/Churches_46190.pdf>. There are many publications and judgements espousing these views, far too many to list here.

94 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill (2014) (Cth) 5, [5].

95 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill (2014) (Cth).

serious matters should be strictly prohibited. There is no justification that anything less than serious offences[96] should infringe upon the right to privacy.

We therefore recommend that the Committee recognise the disproportionate interference with the right to privacy which exists under the *TIA Act* for the access of metadata. We recommend the Committee consider implementing similar thresholds for the severity of crime as contained within the *TIA Act* s 5D 'Serious Offences' as per the requirement for obtaining a Telecommunications Interception Warrant.[97] Further, in the same way that the contents of 'live'/'voice' communications are not stored or recorded for future access by enforcement agencies, metadata should not be retained. Metadata should be treated in the same manner that a telephone conversation is under the *TIA Act*.[98]

96 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 5D.
97 *Telecommunications (Interception and Access) Act 1979 (Cth)* s 7.
98 *Telecommunications (Interception and Access) Act 1979 (Cth)*, eg s 7 not intercepted except by warrant for a serious offence s 5D.