Submission

Telecommunications Data Retention Review

19 July 2019

David Vaile

Shavin Wijeyaratne

Genna Churches

Monika Zalnieriute

THE ALLENS HUB
FOR TECHNOLOGY, LAW & INNOVATION

About Us

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub adds breadth and depth to research on the diverse interactions among technological change, law, and legal practice. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, industry, government and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

David Vaile is a leader of the 'Data Protection and Surveillance' research stream, Allens Hub for Technology, Law and Innovation, UNSW Faculty of Law (Allens Hub). Shavin Wijeyaratne is an intern with the Allens Hub. Genna Churches is PhD candidate and a scholar at the Allens Hub. Monika Zalnieriute is a Research Fellow and a leader of the 'Technologies and Rule of Law' research stream at the Allens Hub. Assistance of other colleagues is gratefully acknowledged. The views expressed herein, and responsibility for any errors or omissions, are solely those of the authors.

About this Submission

This is a submission to the review in Section 187N of the *Telecommunication (Interception and Access) Act 1979* (Cth), about the data retention scheme in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* ('the Act'/ 'TIA Act').

The submission touches on issues of the proportionality of the scheme, especially in respect of privacy, personal or other information security of users, communications confidentiality and similar public interests affecting users, as well as governance, oversight and transparency.

THE ALLENS HUB
FOR TECHNOLOGY, LAW & INNOVATION

The continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill

The reference to 'continued' effectiveness may imply an assumption that past effectiveness has been demonstrated. However, there has been no robust, independent evidence-based scrutiny of claims and assumptions about the necessity of the scheme, its proportionality[1] or its effectiveness.

The history of the original proposal is illustrative. The original brief text of the proposal for the scheme in 2013 provided insufficient justification, leading to it not being accepted by the PJCIS.[2] The second version of the proposal in 2014, which resulted in the current scheme, made claims about necessity and expected effectiveness without providing sufficient evidence or referring to findings in the US and EU that their key data retention schemes were insufficiently effective or proportionate (see note below in 3. Costs for details).[3]

More critical scrutiny of effectiveness claims is required.

The appropriateness of the dataset and retention period

Data set

The final text of the Act is unclear as to the actual data items to be covered by the data set. [4] It is difficult for telecommunications consumers affected by the scheme to understand the Act's scope. While the term "metadata" is ambiguous and would thus need to be defined, it may help consumers understand what data is covered by the Act. There is also tension between a desire for technological neutrality (which contributes to longevity of terminology) and the need for readers to interpret statutory language in concrete contexts.

---

[1] Proportionality concerns remain critical in light of the significant ongoing intrusions into privacy, communications confidentiality, personal information security, commercial secrecy and other public interests created by the expanded framework for warrantless, suspicion-less mass surveillance that the retention scheme supports, in addition to traditional targeted and warrant-based investigation. The Department submitted on privacy and proportionality considerations to the 2014 PJCIS inquiry, but the concerns remain, given the limited constraint which these considerations appear to play in the final form of the scheme. See [3.57], 87, <https://www.aph.gov.au/~/media/02%20Parliamentary%20Business/24%20Committees/244%20Joint%20Committees/PJCIS/DataRetention2014/FinalReport_27February2015.pdf>.

[2] PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 2013, <https://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm>.

[3] 2015 PJCIS report, above; Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report to the 44th Parliament* (2014), 14-8.

[4] See s187AA of the Act, at <https://www.legislation.gov.au/Details/C2015A00039>.

Clarity and transparency, particularly as to scope, in granting powers in national security and law enforcement contexts is critical[5] for reasons including public accountability, preventing the retention of data outside the dataset, and enabling carriers, CSPs and ISPs to refuse access to data which is not specified as being 'telecommunications data' and subject to mandatory retention obligations.

Access to data set, as description and as sample

One way to enhance public understanding about which data is retained is to provide individuals with a right to access data retained about them, and to publish specific descriptions of retained data items (including technical terms for each item and indicative quantities retained for a period). *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 was triggered by a dispute by an individual regarding their right to access their 'personal information' retained under the retention scheme, in particular items like their IP address, under the pre-2014 version of s 6 *Privacy Act 1988*. While that case has been interpreted to exclude IP address and similar technical device-related data items from that earlier definition of 'personal information' because they are not 'about' a person, s 187LA(2) TIA Act now says information retained under Part 5-1A is 'personal information' where it relates to an individual or to a communication to which the individual is a party.

This useful provision should be supplemented by explicit rights for an individual to gain access both to those descriptions and also to substantial examples of the actual data retained about their online communications activity (see below for more detail).

Implications of CG-NAT etc.

The evolution of techniques to address developments and limitations in the changing telecommunications data environment means that the implications of telecommunications data retention, and the data set involved, requires review. One example is CG-NAT (Carrier Grade Network Address Translation, which enables re-use of IP numbers behind a carrier's firewall),[6] and related techniques required during the IPv4 to IPv6 transition. This includes rapid re-use of 'leases' for particular device identifiers like IP number, and 'multiplexing' enabling simultaneous sharing of scarce IPv4 numbers. To enable identification of a user's device behind the public facing IP address, the use of CG-NAT requires additional data

[5] Lyria Bennett Moses and Louis de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41 *Melbourne University Law Review* 530.

[6] For an example of the records created when CGNAT occurs, see, eg, 'Citrix how to for Netscaler' <https://www.citrix.com/content/dam/citrix/en_us/citrix-developer/documents/Netscaler/how-to-enable-compact-logging-for-cgnat-in-netscaler.pdf>.

(including the address of the server at the other end of each request) to be retained.[7] The retention of this type of data can reveal elements of browsing history and make it possible to reconstruct 'pattern of life' information about a user including their movements, browsing or communication habits. The Revised Explanatory Memorandum states that NAT records are permitted to be retained under s 187A(4)(b):

> does not exclude any provider from retaining information about the identifiers it assigns, on a permanent or transient basis, to an account, device or relevant service, such as *network address translation (NAT)* information. Such information can be required to be retained by Item 1(d) or Item 2, or both, of the table in 187AA.[8]

This blurs the boundary between 'contents' or 'web-browsing histories', and 'telecommunications data', permitting or even requiring the retention of data excluded by ss 172 and 187A(4)(a) or (b) of TIA Act.

Period

The appropriateness of the retention period remains a matter of concern. In particular, any chosen time period should be backed by evidence of sufficient usefulness of the information for that time period, as against risks and harms associated with extended retention.[9]

Submission 21. from Home Affairs Portfolio, is not persuasive on this issue.[10] At [56], it mentions that the two year period was based on European Union experience.[11] It does not mention the key reason the European Court of Justice ruled the *Data Retention Directive* of 2006 was disproportionately intrusive[12] and thus invalid: the scope or duration of retention

---

[7] See explanation by APNIC chief scientist Geoff Huston, 'What is Metadata, and Why Should I Care?', *The ISP Column* (online), August 2014 at <https://www.potaroo.net/ispcol/2014-08/metadata.html>. In contrast the Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) says in respect of s 187A(4)(b), 'retention obligation is explicitly expressed to exclude the retention of destination web address identifiers, such as destination internet Protocol (IP) addresses' at [55].

[8] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 Revised Explanatory Memorandum [242] 43 (emphasis added).

[9] See, eg, *Digital Rights Ireland Ltd* (C-293/12) v Minister for Communications, Marine and Natural Resources (2014) [64] ('*Digital Rights Ireland*').

[10] See <https://www.aph.gov.au/DocumentStore.ashx?id=c7b8eeb1-aa40-4612-8e36-a93173f5ddca&subId=668160>.

[11] Keeping in mind that the period of two years was the maximum time for retention. The minimum time was only six months with member states being able to determine the appropriate period of retention between six months and two years. Australia chose to implement the maximum period of time.

[12] The European Court of Justice, in *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (C 293/12 and C 594/12) [2014] ECR-SC, 8 April 2014, ruled the *Data Retention Directive* 2006/24/EC 'disproportionate' for lack of independent review on objective criteria to ensure retention is limited to what is strictly necessary. 'Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU,

obligations were not limited by strict necessity or a requirement to minimise them where possible. The EU-based precedent for a two year period in Australia should be discounted because of this direct rejection of its proportionality.[13]

Most Australian data disclosed in 2016-2017 was less than six months old and 80% was less than 3 months.[14] Only about 4% was older than 12 months, and less than 1% was 21-24 months old. A reduced retention period of say 6 months would, on these figures, have minimal effect, notwithstanding the other factors mentioned. This does not support an extension.

The anecdotal example at [62]-[63] given to support a longer retention period showed six of seven charges in a 2017 case were proven using data from the current two year retention period. To help prove the remaining charge, the retention period would have needed to go back to 2011, six or more years, or over than three times the present period (and the failure to convict was not attributed solely to lack of 2011 data so it may have failed in any event). About 86% of the offender's charges were proven within the existing framework. Although a single example is not a basis for proper analysis, in this instance it is arguably not proportionate to propose extending the period by 300% to address the remaining charge.

More comprehensive information is needed to assess the other examples in [64]-[78].

The uncritical or counterintuitive conclusions drawn in favour of extension of the retention period in the three instances above suggest a more independent and critical review is needed.

Costs, including ongoing costs borne by service providers for compliance with the regime

It should be recognised that the cost of the retention scheme is ultimately paid for by telecommunications customers and taxpayers.[15] Cost issues should therefore be made transparent by independent assessment. In the US, cost/benefit calculations using closely

---

without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary', [65]. <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN>. See also Explanatory memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), [60].

[13] In the terms used by *Digital Rights Ireland* [64], Australia's data retention scheme does not contemplate the retention of only data which is strictly necessary.

[14] Review of the mandatory data retention regime, Submission 21. Home Affairs Portfolio, undated, [58].

[15] See Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2016-17* (2018) 51.

scrutinised evidence of benefits resulted in a similar retention scheme being terminated.[16] As noted above, the European Court of Justice held the *Data Retention Directive* invalid because of a lack of proportionality, taking into account the efforts required and the benefits obtained.

Costs of the retention scheme are also likely to increase over time, given increased use of telecommunications networks, including due to video live-streaming services and the Internet of Things. The gradual incremental reduction in cost per byte of storage, bandwidth and processing power common in the IT industry is unlikely to fully offset this.

More critical scrutiny needs to be applied to claims about costs, and to whether these are proportionate to benefits obtained. One calculation compared costs against convictions: 'In 2015-2016, the 63 agencies allowed to request access to retained metadata made nearly 334,000 requests, nearly all of which were for criminal investigations. Those 334,000 requests and $200 million cost yielded 366 arrests and 195 convictions – a unit cost of more than $500k per arrest, and more than $1 million per conviction.'[17]

The US and EU assessments above also included non-financial costs borne by users, such as interference with communications confidentiality and rights to privacy and free speech, in

---

[16] See Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court*, US government, Washington DC, 23 January 2014, <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf>. The review of all evidence of benefit and 12 'success stories' found the Section 215 bulk telephone records program (the main US call metadata retention scheme) 'raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value', and recommended it be ended (at 8). Noting that 'an intelligence-gathering tool with significant ramifications for privacy and civil liberties cannot be regarded as justified merely because it provides *some* value in protecting the nation from terrorism' (at 145, emphasis in original), PCLOB saw 'little evidence that the unique capabilities provided by the NSA's bulk collection of telephone records actually have yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program', at 146. One instance of a donation to Al Shabaab in Somalia was 'the only time [in its 7 years] that the program has directly contributed to the identification of an unknown terrorism suspect' (at 152). The review also criticised logic of the FISA Court as 'circular and deprives the word "relevant" of any interpretive value'. 'The implication of this reasoning is that if the government develops an effective means of searching through everything in order to find something, then everything becomes relevant to its investigations', at [208].
The successor program in the US is inoperative and facing closure because 'the logistical and legal burdens of keeping it outweigh its intelligence benefits': C Savage, 'Disputed N.S.A. Phone Program Is Shut Down, Aide Says', *NYT*, 4 March 2019; Dustin Volz and Warren Strobel, 'NSA Recommends Dropping Phone-Surveillance Program,' *Wall Street Journal* (online), 24 April 2019.

[17] Richard Chirgwin, 'Australia's metadata retention scheme costs telcos $500k per cuffing', *The Register* (online), 14 August 2017 <https://www.theregister.co.uk/2017/08/14/australia_metadata_retention_report/>.

such considerations. Such non-financial costs should be included in analysis of Australia's scheme at both program level (including this review) and operational level.[18]

Any potential improvements to oversight, including in relation to journalist information warrants

With respect to journalist information warrants, one key problem has always been that these warrants only apply to one aspect of investigative journalist practice, namely journalists' metadata of communication with whistleblowers. However, it is also possible to access data of a cohort of potential whistleblowers, in other words, to avoid the barrier while reaching the same outcome. This issue of lack of protection for sources whose metadata is exposed to warrantless access is separate to the use of the journalist information warrants to pursue direct investigations of journalist sources, as brought to attention by questions over the recent raids on ABC and News Ltd journalists.

The protection offered to journalists should arguably be extended to a variety of others, including say whistle-blowers and sources; politicians and their staff; advocates; lawyers[19] and other advisers; researchers and investigators; human rights campaigners; political opponents of agencies or governments; religious and other community leaders; protesters and critics of projects or policies; active figures in unions, professional associations or political groups; and psychiatrists.

Any regulations and determinations made under the regime

This inquiry should review the extent of access to retained data for a wide range of relatively minor infractions, including access by councils.[20] The list of entities with access was initially reduced by the Act but there is a mechanism to expand this by regulation or declaration without the scrutiny of Parliament. Similarly, as noted in the Communications Alliance submission, access under s 280 of the *Telecommunications Act 1997* has seen a wide variety of agencies and bodies beyond 'criminal enforcement agencies' seek to access metadata.[21]

---

[18] Eg, insert '(da) interference with communications confidentiality, privacy and free speech' after cost issues in 187K(7) TIA Act.

[19] See, eg, *Digital Rights Ireland* [58], 'professional secrecy'.

[20] Harriet Alexander, 'Councils pry into residents' metadata to chase down fines', *Sydney Morning Herald* (online), 15 November 2018, <https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html>.

[21] Communications Alliance, Submission No 27 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Scheme*, 12 July, attachment A.

In the interests of proportionality, the extent of this list should be documented and reviewed, with a view to reducing access over time to apply a test of 'strict necessity' for only the most serious matters.[22]

The number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security

Given the opacity of the data set and the remoteness of the retention process from the awareness of most users of telecommunications services, whether business or individual, it is unlikely that the number of complaints will be a useful metric by which to judge the effectiveness, appropriateness or proportionality of the scheme. The lack of notification to the individual that their data has been accessed, further prevents complaints. Telecommunications intermediaries are not directly impacted by the privacy effects of the scheme.

Security requirements in relation to data stored under the regime, including in relation to data stored offshore

Perfect cyber security is impossible; at most one can strive for cyber hygiene, cyber resilience and minimisation of risk. As Bruce Schneier observed, the advantage presently lies with those seeking to obtain data rather than those seeking to defend it.[23] In this context, collecting data and storing it for longer than necessary itself poses a risk to data subjects, even where an organisation attempts to protect that data.

If data is to be retained (because the benefit outweighs these risks), then data subjects should arguably be given a right to legal redress for any resulting harm on a strict liability basis (given their inability to control or assess the security standards adopted).

Any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the Telecommunications Act 1997

The *TIA Act* does not prevent 'voluntary' retention of data for longer than the statutory period or of data outside the statutory scheme's retained dataset. Nor does it prevent 'voluntary' provision of access to retained data outside the mandatory scheme. Oversight requirements such as record keeping for inspection apply to mandatory disclosures but may

[22] See, eg, *Digital Rights Ireland* [57]-[61].
[23] See for instance 'Artificial Intelligence and the Attack/Defense Balance,' *IEEE Security & Privacy*, March/April 2018.

not apply to voluntary disclosures. The *Telecommunications Act 1997* also offers other mechanisms for access, and as with voluntary provision of access, these are not covered by oversight by the Ombudsman.[24] These factors expand the scope of retention and access, and reduce oversight. Consideration should be given to restricting these 'informal' aspects.

Developments in international jurisdictions since the passage of the Bill

Australia's current data retention regime sits uncomfortably with recent developments in other jurisdictions, such as the EU and USA. These developments may be of use in the context of the Australian review.

Firstly, following the Snowden revelations,[25] the Court of Justice of the European Union delivered several important judgments which resulted in invalidation of the data retention regime in the EU.[26] On 8 April 2014, it retroactively invalidated the EU Data Retention Directive[27] in the *Digital Rights Ireland* case (as noted above in 3. Costs).[28] As explained in detail by Monika Zalnieriute,[29] the CJEU found the data retention regime to be a 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'). In 2016, the CJEU delivered a further judgment in *Tele2 Sverige*[30] where it evaluated the national data retention laws of Sweden and the UK and held that domestic data retention legislation permitting indiscriminate retention of metadata by communication service providers is incompatible with the EUCFR.

Secondly, as already noted, the USA appears to be in the process of abandoning its section 215 call data retention scheme because the logistical and legal burdens of keeping it outweigh its intelligence benefits, but it is also creating precedent to protect sensitive

---

[24] See Submission 10. La Trobe University, 13, n 41. See also S Shanapinda, 'Privacy versus the Use of Location Information for Law Enforcement and Security in Australia' (2018) 6(4) *Australian Journal of telecommunications and the digital economy* 109-140, <http://doi.org/10.18080/ajtde.v6n4.167>.

[25] 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 <http://ssrn.com/abstract=3419937>.

[26] For more detail on these judgements, see 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.

[27] 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.

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

[29] 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.

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

information such as location data outside of retention schemes. Case law in the USA such as *Carpenter v United States*[31] demonstrates the sensitivity of retained location data.[32] In *Carpenter*, the Court found that location data was so sensitive that the original court order based on 'reasonable grounds'[33] which law enforcement bodies obtained to access Carpenter's location data was insufficient. The Court found that obtaining location data constituted a Fourth Amendment[34] search and required a warrant based on 'probable cause' further extending the US jurisprudence of the expectation of privacy.[35] Yet, in Australia, location data is retained and accessible through a certification of an authorised officer from the very body who seeks access to it.[36] There is no judicial intervention or oversight despite location data being so pervasive that, at the time of recording or retention, the individual in question may not even be a person of interest. Law enforcement can access location data and see the movements of every individual for the previous two years, if not more, since there is no obligation to delete this data.[37]

[31] *Carpenter v United States* 585 US 1 (2018).

[32] Location data retainable under s 187AA (item 6) of the TIA Act.

[33] *Stored Communications Act* (USA) — Required disclosure of customer communications or records, 18 US Code § 2703(d) this court order is only based on 'reasonable grounds' not the highest standard of 'probable cause'.

[34] United States Constitution, Amendment IV.

[35] See, eg, Genna Churches, 'Everybody Knows: Snowden's NSA Leaks, Metadata and Privacy Implications for Australia' (2013) Bachelor of Laws Honours Paper <http://ssrn.com/abstract=3419937>.

[36] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 178 and 179.

[37] *Telecommunications (Interception and Access) Act 1979* (Cth) s 187(c); see *Digital Rights Ireland* [67] that there must be deletion after the period of retention. The Australian scheme does not specify any requirement to delete.