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

11 March 2020

Supplementary 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*')

Genna Churches and Monika Zalnieriute
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.

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.

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.

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.

Supplementary Submission

This submission seeks to respond to the questions on notice taken during our oral evidence on 14 February 2020 and to respond to issues raised in evidence and supplementary submissions.

I Questions on Notice

A Question on the Cost of Data Retention Versus the Benefit

We took a question on notice regarding the costs of the data retention scheme versus the benefits. Allens Hub Submission 28[1] cited an article written in 2017 regarding the cost of the data retention scheme.[2] The article cites the 2015/2016 Attorney-General's Annual Report[3] and appears to incorrectly interpret the number of arrests and convictions for stored communications warrants as those applicable to telecommunications data access. This means the approximations of $500,000 per arrest and $1 million per conviction are based on an incorrect comparison of information as there is no publicly released information which would reflect the numbers of arrests or convictions made using telecommunications data.[4] This means that we do not know how much each arrest or conviction costs.

However, the inability to calculate these costs serves to highlight the insufficient reporting mechanisms for the telecommunications retention and access regime. It is not known what the cost per arrest or conviction is because those numbers are not released in annual reporting measures, making it impossible to judge if the cost of the scheme is proportionate to the results obtained. If each arrest did cost $500,000, would that money be better spent by employing more police officers or more technical officers for law enforcement agencies? These are questions which can only be answered by the release of information regarding the numbers of arrests and convictions. Therefore, the cost to the taxpayer for the data retention regime, which does not collect the metadata of those who seek to evade the scheme, must be shown to be a better investment than employing additional police resources.

---

[1] David Vaile et al, *Submission Telecommunications Data Retention Review* (Submission, The Allens Hub, 19 July 2019).

[2] 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/>.

[3] Australian Government, Attorney General's Department, *Telecommunications (Interception and Access) Act 1979 Annual Report 2015-16*.

[4] Australian Government, Department of Home Affairs, *Telecommunications (Interception and Access) Act 1979 Annual Report 2018-19*.

B Question on the Effectiveness of Data Retention

We also took a question on notice regarding the effectiveness of data retention. Allens Hub Submission 28 cites a report on the NSA's s 215 telephone records program, which states the collection of call records had 'shown only limited value' yet been a serious threat to privacy and civil liberties. The report states:

> 'we have not identified a single instance involving a threat to the United States in which the *telephone records program made a concrete difference in the outcome of a counterterrorism investigation*. Moreover, we are aware of *no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack*. And we believe that in *only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect*. In that case, moreover, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.'[5]

The above example questions the effectiveness of this particular aspect of metadata retention and analysis. However, a similar analysis of the Australian data retention regime is impossible as there is a lack of information reported to determine the effectiveness. Reporting mechanisms should include the arrest and conviction rate (and use as exculpatory data), clarity around the offences being investigated, the data types and volumes disclosed, and which data types were most useful/led to an arrest/conviction. This will enable an analysis on the effectiveness of the regime and may also determine which data types are more effective for law enforcement purposes, permitting a reduction in the retention of 'less useful' or unnecessary data. Further, the current varieties of metadata disclosed (ie the possibility of the disclosure of URLs and variations in the accuracy of location data) represent a difficulty in measuring the effectiveness of the scheme versus the incursion of the right to privacy.

[5] 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, 23 January 2014) 146 <https://www.pclob.gov/library/215- Report_on_the_Telephone_Records_Program.pdf>, 146.

II Further Responses

A Need for Retained Metadata

In principle, we agree that some uniformity of the retention periods across various providers may have been required. However, we take specific issue with the failure to address the proportionality of the scheme. The current regime mandates the retention of a broad data set, accessible by a wide range of organisations with a lack of threshold as to serious crime, and contains no mechanism for prior review such as a warrant. This makes the current regime disproportionate — it is not reasonable and necessary to fulfil the societal objectives of tackling serious crime including terrorism and paedophilia.

We note the failure of several safeguards enacted in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), namely:[6]

1. That the dataset is currently so broad that it includes the likely retention of URLs (web browsing)[7] and fails to adequately limit the number of data points for location data, particularly with increases in technology and adoption. Machine to machine communications and 5G adoption will/are causing further issues with the data set.
2. That the restrictions relating to enforcement agencies are meaningless when those enforcement agencies can access metadata for the investigation of breaches of laws, can make secondary disclosures which are not reported in the annual *Telecommunications Interception and Access Act 1979* (Cth) ('*TIA Act*') reports, and that other legislation such as s 280 of the *Telecommunications Act 1997* (Cth) ('*T-coms Act*') permits agencies beyond the definition of an 'enforcement agency' access to metadata.
3. We do not know if the *TIA Act* restricts data to only when it is 'reasonably necessary' for the investigation of a crime, enforcement of a pecuniary penalty or the protection of public revenue. The requirements under s 180F *TIA Act* do not apply to those agencies accessing data under ss 280 or 313 of the *T-coms Act* (or secondary disclosures). We note the concerns cited in the Commonwealth Ombudsman Reports 2016/17 and 17/18 regarding the application of s 180F of the

[6] This list is not exhaustive. For example, issues such as the storage of data offshore and entities not covered by a mandatory data breach regime have not been assessed in this submission. Nor have broader topics such as the ability to evade the data retention regime and the effect of newer technologies such as 5G and M2M communications.

[7] Noting destination IP addresses can also expose content in certain circumstances.

TIA Act.[8] In some instances, a request had taken *just a minute* to be authorised, clearly insufficient time to consider the requirements of s 180F of the *TIA Act*.[9]

4. Sections 280 and 313 of the *T-coms Act* undermine the data retention and access regime intended by legislators. In 2015 the scheme was envisaged as a system of retention of a limited dataset for access only by enforcement agencies for serious matters under an authorisation.[10] Concerningly, s 297 of the *T-coms Act* also permits secondary disclosures of information obtained under s 280 of the *T-coms Act* providing the disclosure is required or authorised by law.
5. The current regime contradicts statements made in Explanatory Memorandums such as:

> The Bill permissibly limits an individual's privacy in correspondence (telecommunications) in a way which is reasonable and proportionate by circumscribing the types of telecommunications data that are to be retained by service providers to the essential categories of data required to *advance criminal and security investigations, permitting access to telecommunications data only in circumstances specified in the TIA Act* and reducing the range of agencies who can access data under those provisions.[11]

6. This leaves a scheme which is essentially a blanket metadata retention regime, accessible by an unlimited number of agencies without prior independent review, and not limited to the investigation of serious crime.

---

[8] Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979 For the Period 1 July 2016 to 30 June 2017*; Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979 For the Period 1 July 2017 to 30 June 2018*.

[9] Commonwealth Ombudsman, 'A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979 For the Period 1 July 2017 to 30 June 2018' (n 7).

[10] See generally, *Revised Explanatory Memorandum Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 2015*; Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, Second Reading Speech, Malcom Turnbull, 12,561.

[11] *Revised Explanatory Memorandum Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 2015* [67].

B Datasets to be Retained

We note the evidence provided by the Commonwealth Ombudsman and the Australian Federal Police ('AFP') with respect to the disclosure of URLs on Friday 28 February 2020. The AFP explained that browsing histories occupy a 'grey space' between content and metadata.[12] Similar issues were raised before the PJCIS during the 2014/15 review.[13] As we stated in our submissions, there are serious definitional issues with the dataset which means it does not serve to prevent the mandatory retention of URLs, and the disclosure regimes under the *TIA Act* and the *T-coms Act* also do not prevent the disclosure of URLs retained outside of the data retention regime. We concur with the Commonwealth Ombudsman and the AFP in calling for clarity with definitions provided for the contents or substance of a communication, and specific prohibitions on the retention and disclosure of URLs.[14]

C Threshold of Access

Despite concerns being raised during 2014/15 during the PJCIS hearings, no threshold of criminal activity is specified in the data retention and access regime. Instead, s 180F was hoped to provide a threshold of 'proportionality' as to the seriousness of the offence and, of course the list of agencies able to access the data was restricted to enforcement agencies.[15] The types of offences shown in the annual Reports show metadata is being accessed for trivial matters in addition to the serious criminal offences intended suggesting a threshold of access is required. Note, limited or no data is available for access under s 280/313 of the *T-coms Act* or for secondary disclosures.

We note the Law Councils' suggestion in Submission 29 that s 15GE of the *Crimes Act 1914* (Cth) is an adequate threshold for access to metadata.[16] While we would agree that a threshold of this type is appropriate, we question the addition of further complexity to the *TIA Act*. Instead, it may be prudent to keep the definition of a serious offence to one already contained within the *TIA Act*, and suggest that s 5D of the *TIA Act* may be an appropriate alternative.

---

[12] Commonwealth of Australia, *Official Committee Hansard, Parliamentary Joint Committee on Intelligence and Security*, 28 February 2020, 49.

[13] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Parliament of Australia, February 2015), 103-4.

[14] Note that some destination IP addresses are also content.

[15] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Parliament of Australia, February 2015), 245-51.

[16] Law Council Submission #29, 13.

D Prior Review of Access

Given recent unlawful access to over 3000 telecommunications users data, we recommend the implementation of a form of independent prior review.[17] We have suggested that it may be appropriate to permit access to less invasive metadata without a warrant (perhaps only subscriber data), but sensitive data such as location and URLs should be subject to a judicial warrant. A perfect system would require prior judicial review for all metadata access as subscriber data can be subject to abuse[18] and may also, under current dataset definitions, contain content such as URLs or destination IP addresses.[19]

However, we note opposition to a warrant-based system by the Department of Home Affairs and other enforcement agencies,[20] who flagged the time needed to obtain a warrant and the intensive resources involved in preparing warrant applications, as being inimical to the enforcement of criminal law. A compromise could be the implementation of a warrant system to obtain location data, with strict reporting mechanisms, such as the amount of time taken to prepare the warrant, and how many hours/days/weeks it takes to obtain it. This data could be used to justify a further warrant rollout across metadata types if the 'burden' to law enforcement agencies proves to be manageable. Similarly, if reporting measures for existing warrants under the *TIA Act,* such as telephone interception and stored communications warrants, had mandated reporting on how long a warrant takes to obtain, it may be instructive on how a warrant system for metadata access may affect law enforcement agencies.

E Access to telecommunications data under s 280 *T-coms Act*

Section 280 of the *T-coms Act* is a loophole which permits largely unregulated access to metadata. It originates from provisions enacted in 1975 which permited the disclosure of content without a warrant

---

[17] Paul Karp, 'ACT Police Admit They Unlawfully Accessed Metadata More than 3,000 Times', *The Guardian* (online at 26 July 2019) <https://www.theguardian.com/australia-news/2019/jul/26/act-police-admit-unlawfully-accessed-metadata-more-than-3000-times>.

[18] 'Queensland Police Officer Allegedly Took Photo of Family Violence Victim's Private Details | Australia News | The Guardian' <https://www.theguardian.com/australia-news/2020/mar/08/queensland-police-officer-allegedly-took-photo-of-family-violence-victims-private-details>; 'Queensland Police "breached Privacy" of Domestic Violence Victim by Leaking Her Details | Australia News | The Guardian' <https://www.theguardian.com/australia-news/2019/mar/27/queensland-police-breached-privacy-of-domestic-violence-victim-by-leaking-her-details>; 'Queensland Police Charge Officer with Hacking after Domestic Violence Victim's Details Leaked | Australia News | The Guardian' <https://www.theguardian.com/australia-news/2018/dec/14/queensland-police-charge-officer-with-hacking-after-domestic-violence-victims-details-leaked>.

[19] This may also be due to the use of CG NAT, the ability for some destination IP addresses to disclose content and the retention of information outside the data set.

[20] Home Affairs Supplementary Submission # 21.1.

'in pursuance of the requirements of a law of Australia or a Territory'; or in circumstances in 'which the doing of the thing was in the public interest'.[21] There was no prohibition on the disclosure of metadata.

In 1989, the *Australian Telecommunications Corporation Act 1989* (Cth) prevented the disclosure of content and metadata by current carrier employees except 'under a law of the Commonwealth' or in situations prescribed in the Regulations. The Regulations prescribed that disclosure could occur 'where the disclosure is *authorised by or under a law of the Commonwealth*, *or required or authorised by or under a law of a state or territory*; or where the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.'[22]

In 1997, s 280 of the *T-coms Act* provided an exception to the prohibition on disclosure where 'the disclosure or use *is required or authorised by or under the law*'. The provision does not specifically prohibit the disclosure of content:

> (1) Division 2 does not prohibit a disclosure or use of information or a document if:
>
> (a) in a case where the disclosure or use is in connection with the operation of an enforcement agency—the disclosure or use is required or authorised under a warrant; or
>
> (b) in any other case—the disclosure or use is required or authorised by or under law.[23]

This leaves telecommunications data exposed to a regime which was outside the contemplation of legislators when the data retention regime was enacted in 2015.[24] Disclosures under s 280 of the *T-coms Act* numbered 11,526 and 13,106 for 2013/14[25] and 2014/15[26] and have maintained similar numbers since 2005/06,[27] with some exceptions for example; a spike at over 21,000 requests in

---

[21] *Telecommunications Act 1975* (Cth) s 82.

[22] *Australian Telecommunications Corporation Regulations 1989* (Cth) reg 3.

[23] *Telecommunications Act 1997* (Cth) s 280 (as made).

[24] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Parliament of Australia, February 2015) 220-222.

[25] Australian Government, *Australian Communications and Media Authority Annual Report 2013-14*, 210.

[26] Australian Government, *Australian Communications and Media Authority Annual Report 2014-15*, 95.

[27] Australian Government, *Australian Communications and Media Authority Annual Report 2005–06*, 98.

2006/07[28] and a drop to 7,725 during 2010/11.[29] These are not insignificant numbers and should have been a known alternative for access outside of the *TIA Act*.

As evidence of 28 February 2020 revealed, there are no reporting mechanisms for s 280 which show which specific agencies asked for access, what laws they sought access under or even whether that access was legitimate under those external laws. Further, protections such as s 180F of the *TIA Act* do not apply to disclosures made under the *T-coms Act*. This means that it is unnecessary to consider the privacy of the individual (unless the enabling *Act* directs such considerations) when requesting disclosure under provisions such as s 280 of the *T-coms Act*.

Discussions surrounding the ability of States to make legislation which permits access to telecommunications data under s 280 of the *T-coms Act* are fundamentally flawed as without the legislative exceptions permitting disclosure under provisions such as s 280, State laws would be ineffective in gaining access to this information.

F Legislative Requirement to Protect Data and Communications — Secondary Disclosures

While s 182 of the *TIA Act* does contains a criminal offence for the unlawful disclosure telecommunications data, it also provides a wide range of exceptions, namely, the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or the protection of public revenue. This means that as a secondary disclosure can be made in relation to a suspected breach of almost any law to an unlimited number of agencies. Evidence at the hearings has suggested that agencies do not delete obtained telecommunications data and draw upon it for future investigations and make secondary disclosures to other agencies in case of a suspected breach of the law.[30]

G International Context

In January 2020, findings in *Digital Rights Ireland*[31] and *Tele2 Sverge*[32] were reinforced by the Opinion of Advocate General Campos Sánchez-Bordona (who provides non-binding opinions on EU law to the

---

[28] Australian Government, *Australian Communications and Media Authority Annual Report 2006–07,* 128.

[29] Australian Government, *Australian Communications and Media Authority Annual Report 2010-11*, 78.

[30] Commonwealth of Australia, *Official Committee Hansard, Parliamentary Joint Committee on Intelligence and Security*, 7 February 2020, 29-30.

[31] 'Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General' (2014) Joined Cases C-293/12 and C-594/12 *Court of Justice of the European Union* <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=firstð=1&cid=8886631> ('Digital Rights Ireland').

[32] *Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson C 203/15 and C-698/15* (Court of Justice of the European Union, 21 December 2016).

Court of Justice of the European Union ('CJEU')) on three national data retention schemes in the UK, France and Belgium. The Opinion clarifies existing case law; reaffirming that only limited and discriminate retention may occur within the EU, with prior independent authorisation by a court or independent authority for accessing that data; that affected parties have to be informed (unless it would compromise the effectiveness of the measures); and that domestic laws must be enacted to prevent unlawful access or misuse of the data.[33] We anticipate the principles outlined in the Advocate General's opinion will be adopted in the binding decision to be handed down by the CJEU later this year. Without change to the current Australian metadata retention and access regime, this decision will put Australia further at odds with international counterparts and the protection of fundamental human rights.

[33] *Advocate General's Opinions in Case C-623/17 Privacy International, Joined Cases C-511/18 La Quadrature du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others* (Court of Justice of the European Union, Advocate General Campos Sánchez-Bordona).