Australian Council
for Civil Liberties

Submission by the Joint Councils for Civil Liberties

to

The PJCIS statutory review of the Mandatory Data Retention Regime

15th July 2019

PJCIS REVIEW OF THE MANDATORY DATA RETENTION REGIME

1. INTRODUCTION

The councils for civil liberties across Australia (the joint CCLs)[1] supported the need for an early review of the operation of the mandatory data retention regime established under the Data Retention amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act 1979) in 2015- although we argued that the importance of the legislation was such that these reviews should be annual.[2] We therefore welcome the opportunity to make a submission to this review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) as required by Section 187N of the TIA Act 1979.

We note the Committee has resolved to focus on nine aspects of the legislation:

i. the continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill;
ii. the appropriateness of the dataset and retention period;
iii. costs, including ongoing costs borne by service providers for compliance with the regime;
iv. any potential improvements to oversight, including in relation to journalist information warrants;
v. any regulations and determinations made under the regime;
vi. the number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security;
vii. security requirements in relation to data stored under the regime, including in relation to data stored offshore;
viii. any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the Telecommunications Act 1997; and
ix. developments in international jurisdictions since the passage of the Bill.

We will comment on these areas to the extent that they engage civil liberties/rights issues and where useful new information is publicly available. While we understand the parameters of this statutory review, we think it necessary to place our specific comments on the mandatory data retention regime in the context of our wider concerns about the cumulative impact of overreach in Australia's uniquely large body of national security and counter-terrorism legislation.

2. THE BROAD POLITICAL AND LEGISLATIVE CONTEXT OF THIS REVIEW

The AFP raids

This statutory review of the mandatory data retention regime comes at a timely moment. The recent, very public post-election raids by the Australian Federal Police (AFP) on the ABC and a news limited journalist in search of information relating to their sources and, as we now know, evidence of criminal activity by the journalists[3], have rightly caused a public furore.

[1] New South Wales Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australia Council for Civil Liberties and the Australian Council for Civil Liberties.

[2] Joint Councils for Civil Liberties Submission to PJCIS Inquiry Into The Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2014 Joint Committee On Intelligence And Security Inquiry Into The Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2014.[Joint CCLs submission PJCIS Data Retention Bill 2015] Recommendation 4

[3] Multiple media coverage including Canberra Times (AAP) 9/7/19

While others have recently been charged for secrecy offences, these media raids have made visible to a wider public the extent to which fundamental aspects of democracy that we have long accepted as given in Australia, are being progressively undermined by our expansive national security and counter terrorism legislative framework. These raids, whether or not journalists and/or whistle-blowers are charged, will clearly have an immensely intimidating effect on journalists and media organisations and would-be whistle-blowers. This is what they are meant to do.

Democracy is absolutely dependent on the public's right to know what Government is doing - with limited and non-permanent exceptions. The mandatory data retention regime is a major and controversial element in Australia's complex secrecy and surveillance legislative framework. The CCLs have consistently opposed it as seriously disproportionate legislation which, as well as unwarrantedly undermining the right to privacy of all Australians, directly threatens the capacity of journalists and media organisations to investigate and report on Government activity.

It does so despite credible evidence that less harmful means of effective investigation and surveillance are equally effective.

This review presents an opportunity to address the over-reach in the data retention legislation by amendment or repeal of provisions. This would not solve the wider issues raised by the AFP raids but it would be a good start.

National security and the cumulative surveillance and secrecy regime

The protection of public safety is a central responsibility of government. The CCLs appreciate the increased pressures of the seemingly permanent terrorist threat in the Australian, as well as international, context and the need for the Government and the Parliament to provide adequate powers and resources for the best possible protection of Australia's national security.

This support is always subject to the critical caveat that any exceptional powers granted to Government or its agencies are necessary, proportionate and compatible with the maintenance of a robust Australian democracy.

While the CCLs acknowledge that some of the post 9/11 specific counter-terrorism/national security laws have been necessary and positive, we have been concerned from as early as 2003[4] that numbers of provisions in the now exceptionally large and complex body of national security/counter terrorism law are excessive and incompatible with a well-functioning democracy.

The chilling significance of expanded surveillance powers has been progressively amplified by the equally excessive expansion of secrecy offences relating to government activity - especially encompassing areas of intelligence, national security and immigration/refugee activities.

Cumulatively, these surveillance and secrecy laws have changed the legal landscape with real and increasingly visible consequences for our democratic processes and values.

The joint CCLs were deeply disturbed - but not surprised - by the recent deliberately public AFP raids on the ABC and a news limited journalist in search of information relating to their sources and,

[4] Most notably in relation to the extraordinary Questioning and Detention Powers in the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 – which although amended remain excessive. The initial Bill included many excessive provisions leading the then Parliamentary Joint Committee on ASIO, ASIS and ASD to describe it as "*one of the most controversial pieces of legislation considered by the Parliament in recent times'*…which "*undermine key legal rights and erode the civil liberties that make Australia a leading democracy'* Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) bill 2002. May 2002

according to the AFP, evidence of criminal activity by the journalists[5].

These actions were not only predictable but inevitable. This is precisely the logical consequence of this expanded suite of surveillance and secrecy laws. Notwithstanding Ministerial assurances to the contrary and the insertion of limited 'fixes' to protect journalists and whistle-blowers[6] when faced with public outrage to particularly contentious provisions, the intention of existing laws is clearly to intimidate the media and would be whistle-blowers from reporting on a wide range of Government activity-regardless of whether or not it is in the public interest to do so.

It is abundantly clear that Australia now has in place an extensive and complex suite of laws which will greatly constrain journalists and legitimate whistle-blowers, greatly inhibit the public's right to know and discuss what Government and its agencies are doing and seriously undermine our already weak capacity to hold the Government accountable for its actions.

In the process these laws have also excessively undermined Australians right to reasonable privacy and security for their personal data.

The CCLs have repeatedly argued that that this is a dangerous trend for a democracy – all the more so because we lack the underpinning protection afforded by a National Human Rights Act.

In our view there is an urgent need for Government and Parliament to pause their hyper-legislating response to national security/counter terrorism issues and reflect on the cumulative implications of the existing large body of law with the view of winding back excessive and/or unnecessary laws which are incompatible with a robust democracy.

Freedom of the press inquiry

The CCLs note Attorney-General Christian Porter has given the PJCIS a reference to inquire into the '*impact of the exercise of law enforcement and intelligence powers on the freedom of the press*'[7]. We welcome the Government's recognition that an inquiry is needed and will be making a submission.

However, we consider the terms of reference too limited. A much wider review of the cumulative impact of the large body of national security/counter-terrorism legislation on the fundamentals of Australia's democracy is needed –a meaningful and potentially effective review must engage with the implications of excessive secrecy laws as well as the data collection and surveillance laws – and their interaction.

It must also engage with the depressing and dangerous culture of secrecy that increasingly permeates governments and agencies. The demolition of an effective open government regime at the national level is an integral dimension of the problem.

Recommendation 1

While noting that the Attorney-General has established a review relating to freedom of the press ***the CCLs recommend*** *that Government or Parliament initiates a broad and independent review of Australia's extensive body of national security/counter terrorism related laws to identify the cumulative impact on Australia's democratic values and repeal or amend provisions which are not compatible with robust democratic principles.*

[5] SMH article by Bevan Shields 6/6/19

[6] Eg: In relation to the impact on journalists of 35P of the ASIO Act ; the journalists defence included in the Security Legislation Amendment (Espionage and Foreign Interference) Act 2017

[7]

The review should be conducted by an independent entity such as the Australian Law Reform Commission with the requirement that it seeks public input by submissions and public hearings.

3. THE MANDATORY DATA RETENTION REGIME

The CCLs made a number of submissions in relation to the mandatory data retention regime over the period 2012-2015.[8] In those contexts we strongly opposed the central concept of a mandatory telecommunication metadata collection and retention scheme encompassing almost all Australian residents -suspect and non-suspect - which approved authorities would be able to retrospectively access without a warrant for a period of two years.

It was our view that such an indiscriminate data retention regime would not only constitute a major and unwarranted intrusion on the right to privacy of individuals but would also have major flow-on negative implications for other freedoms and democratic values. The chilling impact on journalists and whistle-blowers was a major concern.

Although some positive amendments were made to the original Bill – notably, although inadequately, in relation to special protections for journalists - our central reason for opposing the legislation remains. We are not aware of any development or operational outcomes which would cause us to change this position.

There have, however, been developments which have strengthened the grounds for some of our concerns in 2015.

Indiscriminate metadata collection and retention

The proportionality of the legislation depended on a controversial distinction between 'metadata' and 'real' content data that would have different collection, retention and access provisions. The validity of this distinction was strongly disputed by telecommunications experts and civil society bodies at the time. The CCLs noted:

> *The data retention proposal will capture far more private information about all aspects of individuals' lives than is currently done under the provisions of the TIA Act. Credible experts argue that the range and extent of telecommunications metadata provide such rich information about individuals and groups that it no longer makes sense to distinguish metadata from telecommunication content data.*
>
> *The Government's description of telecommunications 'metadata' as being like 'the information on the outside of the envelope' cannot be viewed as a serious contribution to the debate*[9]

This technical view was supported by the European Court of Justice in in the case of *Digital Rights Ireland* which involved elements similar to the proposed Australian scheme:

> ..'such data *taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained'*.[10]

[8] Submissions to the PJCIS Inquiry into Potential Reforms if National Security Legislation 2012 And to PJCIS Review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

[9] .[Joint CCLs submission PJCIS Data Retention Bill 2015] P5

Technical and behavioural developments over the last four years have further blurred any meaningful distinction between telecommunications metadata and content data. Technical developments and powerful data analytics software, greatly increased use of telecommunications across all aspects of life and the high-level use of multiple mobile devices, especially by younger people, have exponentially expanded the richness of the information about individuals lives that will be collected and can be extracted from 'metadata'.

The CCLs note that the European Court of Justice has subsequently found that European Union Law does not permit legislation which:

> *a. mandates general and indiscriminate data retention*
>
> *b. grants access to data in circumstances where access is not solely for the purpose of fighting serious crime, and where access is not subject to prior review by a court or an independent administrative authority.*[11]

All these unacceptable elements are included in the mandatory data retention regime.

In summary The CCLs consider the arguments we advanced in opposing the mass database regime in 2014 remain persuasive. They encompassed the disproportionate impact on:

- the right to privacy of non-suspects and the flow-on implications
- a free media and legitimate whistle-blowers and the ability to hold Government accountable and
- the lack of appropriate safeguards
- reasonable doubt as to whether a mass data collection regime will be significantly more effective in keeping Australians safe from terrorism or other serious crime than a more appropriately targeted scheme. [12]

We maintain our view that the current indiscriminate collection and retention of telecommunications data of all Australians is inappropriate and should be repealed and replaced with a more targeted regime as set out in our 2014 submission to the PJCIS.[13] This is more so the case as the weak distinction between metadata and content data is even less sustainable than it was in 2014.

Recommendation 2

The CCLs recommend that the current statutory requirement for telecommunication service providers to collect and retain prescribed telecommunications metadata of their clients for two years so that authorities can access such data without warrant be repealed - because of its disproportionate impact on the important right to privacy and its chilling impact on a free media and overall incompatibility with robust democratic values.

Alternative targeted data collection regime

The CCLs do not oppose appropriately targeted data collection and surveillance by our intelligence

---

[10] *Digital Rights Ireland and Ors* (C-293/12) *and Kärntner Landesregierung and Ors* (C-594/12), 8 April 2014. At [27] and [37]

[11] Tele2 Sverige AB (C-203/15) and Secretary of State for the Home Department (C-698/15) v Post-och telestyrelsen and ors (21 December 2016) ('Tele2 Sverige AB'). Quoted in ALRC submission …..

[12] .[Joint CCLs submission PJCIS Data Retention Bill 2015] pp4-12

[13] Ibid Recommendation 2 p12.

and security agencies with appropriate safeguards as to access. We previously noted the global discussion in relation to use of alternative targeted data preservation schemes which are less invasive of the citizenry's privacy but still responsive to the needs of intelligence, security and police agencies.[14]

We also noted that such schemes were in in use in Austria, Belgium, The Czech Republic, Germany, Romania and Sweden.[15]

We are not aware of evidence that these less intrusive schemes provide less effective surveillance than the indiscriminate data retention regime established by this legislation.

Access to a targeted metadata should require prior judicial warrant approval.

Recommendation 3

The CCLs recommend consideration be given to replacing the existing mass metadata collection and retention regime with a targeted scheme encompassing only individuals or groups for whom there is reasonable suspicion that they may be, or have been involved in terrorist or other serious criminal activity.

4. DETAILED RECOMMENDATIONS TO AMEND THE CURRENT MANDATORY DATA REGIME

If it is decided to maintain the current indiscriminate metadata regime encompassing all Australians the CCLs wish to reiterate amendments, we proposed amendments 2015.

Prior warrant approval for metadata access

The CCLs maintain our 2015 recommendation that prior warrant approval should be required for agencies access to telecommunications metadata[16]. The current legislation only provides for a warrant in the special context of a Journalist's Information Warrant.

Our argument in 2015 was based on the extensive rich personal information retrievable from metadata and the unknown number of agencies potentially having access to this metadata for a wide range of purposes. The huge growth in the volume and richness of retained metadata since 2015 and the increased technical capacity to analyse this metadata, as well as the increasingly meaningless distinction between metadata and other telecommunications content gives greater weight to this view.

The CCLs had previously been of the view that the prior access to telecommunications metadata under the TIA should also have been on the basis of a judicial warrant authorisation.

It is increasingly clear that access to two years of retained telecommunications metadata does constitute a very significant invasion of privacy for effected individuals with significant flow-on implications. Prior warrant approval is therefore essential in ensuring that the access to this data is not only lawful but proportionate and necessary.

[14] Ibid p13
[15] ibid
[16] Ibid Recommendation 6 p16

It is argued that requiring prior warrant access would introduce a range of problems - including slowing down an investigation, over-burdening judicial officers and adding costs. While we accept some of these outcomes will occur, we do not consider them sufficient reason for by-passing a well understood independent process of prior approval to ensure access is only given if there are appropriate, lawful and necessary grounds.

Such inconvenience and administrative burden that may result is a reasonable and necessary trade-off for such significant intrusion into the privacy rights of the community. The Government must take responsibility for adequately resourcing the courts to accommodate the additional workload arising from these warrant applications.

A significant impact is likely to be fewer applications for access being made on dubious grounds-– given the probability that they would not gain independent approval. This would not be a bad outcome.

An appropriate procedure can be put into place to cope with serious emergencies requiring immediate access to the data.

Recommendation 4

The CCLs recommend that access by enforcement agencies, criminal law enforcement agencies and ASIO to retained telecommunications metadata should require prior approval by judicial warrant.

Data retention period.

The legislation requires the prescribed data to be held by the telecommunications supplier for two years. This was debated in 2015 and the CCLs agreed with the Parliamentary Joint Committee on Human Rights that the Government had not provided a convincing justification for the such a comparatively lengthy period.[17] We held the view that the proposed 2 years may reflected an ambit claim from ASIO and the law enforcement agencies given that it was not substantiated by the operational data they provided at the time.

While we appreciate the reasons the agencies seek a lengthy retention period, there are real consequences for effected individuals.

The longer period provides access to more extensive data for each individual. This has major implications for the extent to which their right to privacy is breached. It also means more extensive data is vulnerable to any security breach of the data base. As we argued in 2015, the right to privacy is an important, though not absolute, right and it should only be curtailed on proportionate grounds.

There are also cost factors which are increased for lengthier retention periods.

Recommendation 5

The CCLs recommend that the legislation be amended to reduce the period of mandatory data retention from the current 2 years to 6 months consistent with available usage information and proportionality relating to the invasion of the right to privacy.

[17] Ibid p21

Notification of access to retained metadata

Unwarranted secrecy provisions are not compatible with a healthy democracy. The CCLs accept that Government and agencies- and particularly intelligence and security agencies - must be able to keep information secret for appropriate and reasonable periods of time.

In this context the appropriate balance between agencies' need for secrecy to protect ongoing investigations must be balanced against the individuals - including innocent individuals and third parties- right to know their data has been accessed by government agencies and for what purpose.

The absence of any surety that this information will be provided leaves everyone with the uncertainty that their private metadata may have been accessed. This is likely to create considerable concern for persons who have legitimate reasons for wanting to keep aspects of their life and professional and personal interactions private.

This concern will be exacerbated with the recent passing of the Telecommunications *and Other Legislation Amendment (Assistance and Access) Act 2018* which has removed from Australians their prior capacity to ensure the privacy of their telecommunications by use of encrypted applications.

The CCLs consider that in a democracy it is appropriate that persons- and particularly persons who are not suspected of any unlawful activity – are entitled to be informed within a reasonable period if their private metadata has been accessed by any agency under this legislation. A period of no more than two years is reasonable in the context.

Provision for the rare context where providing this information within the 2 year time frame will have serious implications for national security or the safety of individuals can be included.

Recommendation 6

The CCLs recommend that the legislation be amended to require the notification of all persons whose telecommunications metadata has been accessed by criminal law enforcement agencies, enforcement agencies or ASIO within a specified period of no more than two years.

Agencies able to access stored content and metadata.

As part of the mandatory data retention regime it was intended that the number of agencies authorised to access both content and metadata would be reduced. The CCLs strongly supported this given the significant privacy implications involved - but argued that the proposed provisions were not sufficient to guarantee this would be the case.

The CCls consider this remains an issue and reaffirm our recommendations that the legislation should exhaustively list or more precisely define the agencies who can access stored content and retained metadata.

Recommendation 7

The CCLS recommend that any additions to agencies on the basis of declaration by the Attorney-General should be limited to agencies investigating serious offences and serious threats to national security

Recommendation 8

The CCLS recommend that agencies given access to stored telecommunications content should be exhaustively listed within the legislation.

Effectiveness of the regime

The CCLs note the relevant Government agencies at state and federal level argue strongly that easy access to stored metadata for the whole population and warrant based access to targeted telecommunications content are indispensable investigative tools. Clearly these data provide a huge amount of information about the lives of individuals of which some would be highly relevant to investigations.

But the CCLs are not able to make any informed assessment of the effectiveness of the access to these data in increasing public safety or in gaining convictions or generally improving investigative capacity. The available data reported by the agencies is far too limited to provide a basis of any assessment of how useful and effective access to the data has been on these fronts.

We know from the one available annual report from the Department of Home Affairs that there is a high level of access. In the 2016-2017 year stored data was accessed 300,224 times by enforcement agencies. This data was used in a relatively small number of convictions - 442. The data was used most often in relation to a criminal law offence. – 293,069 times mainly in relation to unlawful drug offences, homicides and fraud related offences. There is no information in relation to 176,326 requests for access.[18]

This provides some interesting -but predictable – information as to the kinds of offences for which the data is sought. But it provides no information as to effectiveness on any relevant front.

We know that a journalist's telecommunications data was accessed unlawfully without warrant a number of times by the AFP and that this arose from inadequate knowledge of the requirement for a journalist's information warrant – itself the result of inadequate training. The identity of the journalist is unknown. [19]

These are inherent problems in relation to civil society having an informed perspective on the operational impact of much national security/counter terrorism legislation. The inbuilt secrecy provisions and the resulting limited public reporting information seriously restrict the useful information about relevant agency community's.

We can only say we see no evidence that suggests the current indiscriminate data retention scheme is more effective than a less intrusive scheme targeted at suspects would have been.

Journalist Information Warrant

The requirement for a special Journalist Information Warrant[20] for access to journalists' metadata was a significant amendment to the Bill - as was the inclusion of a scrutineering role in the process for a Public Interest Monitor. This was one of several 'fixes' to national security and counter

[18] Department of Home Affairs, Telecommunications (Interception and Access) Act 1979 (Cth). Annual Report 2016-2017 pvi.
[19] Commonwealth Ombudsman Report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979. 2017 p3
[20] TIA Act Div 4C Chapter 4.1

terrorism legislation in recent times in response to negative media and community responses to excessive legislation which directly (if not exclusively) threatened journalists and their sources[21].

While we welcomed this protection for journalists, we do not think it in any way solves the major privacy issues with this legislation. Even if this provided sure protection for journalists and the media - which it does not – they are not the only professionals affected by this legislation.

The limitations of relying on an individual Minister's opinion as to whether a warrant to access a journalist's data can be sought -or a prosecution proceed – are obvious. In recent days we have witnessed extraordinarily divergent understandings and views from the Attorney-General and Minister for Home Affairs in relation to the purpose and desirable flow-on actions from the recent AFP raids.[22]

This is an important but complex issue. On consideration we think it is more appropriate and possibly more constructive to explore the limitations of, and alternatives to, these one-off fixes for an undeniable major problem in the context of the wider -even if not wide enough- concurrent PJCIS ***Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.***

CONCLUDING COMMENT

The Joint Councils for Civil Liberty hope this brief submission is of assistance to the PJCIS and the Government. We would be willing to provide further comment and clarification directly to the Committee if that is desired.

This submission was written by Dr Lesley Lynch, Vice-President NSWCCL on behalf of the Joint CCLs and builds on the prior work of herself and other CCL colleagues in our earlier submissions relating to the mandatory data retention regime.

Therese Cochrane
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission
Dr Lesley Lynch
Vice President NSW Council for Civil Liberties
0416497508; email: lesley.lynch@nswccl.org.au

[21] Eg: In relation to the impact on journalists of 35P of the ASIO Act ; the journalists defence included in the Security Legislation Amendment (Espionage and Foreign Interference) Act 2017
[22] Most recent source: John Lyons ABC News 16/7/2019