JOINT COMMITTEE ON INTELLIGENCE AND SECURITY INQUIRY INTO THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014

20th January 2015

A combined submission from:
NSW Council for Civil Liberties
Liberty Victoria
Queensland Council for Civil Liberties
South Australian Council for Civil Liberties
Australian Council for Civil Liberties

SUBMISSION OF CIVIL LIBERTIES COUNCILS ACROSS AUSTRALIA TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY INQUIRY INTO THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014

The councils for civil liberties across Australia[1] (The CCLS) welcome the Government's referral of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for review and for the opportunity to provide our considered views on the Bill.

1. THE BILL

This bill has been a long time coming having been floated by the Rudd Labor Government as a generalised proposal in the context of overall reform of national security legislation in 2012. The proposal – and the Government's cavalier approach to the issue including the lack of crucial defining detail – generated much controversy and criticism- including from the PJCIS in its report on the national security reform proposals[2].

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the bill) proposes amendments to The Telecommunications (Interception and Access) Act 1979 (TIA Act). The main purpose is to introduce a statutory obligation on telecommunication service providers to retain prescribed telecommunications data of their clients for two years so that authorities can access such data.

The proposed amendments are contained in three schedules to the bill. The first schedule sets out the provisions requiring service providers to retain the telecommunications data of clients for two years. The data to be retained is to be prescribed by regulation; however, s 187A(2) sets out the data types that service providers will have to retain. Such data will not include the contents of communications and it will not include a client's browsing history.

The second schedule deals with access to the retained data. Under the provisions of the bill criminal law-enforcement agencies as defined in s 110A and enforcement agencies as defined in s 176A will have access to telecommunications data. The Bill lists those agencies that will be a "criminal law-enforcement agency", and provides a power to the Minister to declare any additional authority or body to be a criminal law-enforcement agency. The Bill does not list who will be an "enforcement

[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] Parliamentary Joint Committee on Intelligence and Security Report on the Inquiry into Potential Reforms of National Security Legislation June 2013

agency". An enforcement agency will be a criminal law-enforcement agency and any authority or body, which the Minister has declared, by legislative instrument, to be an enforcement agency.

The third schedule sets out the role of the Ombudsman in providing oversight regarding compliance with the provisions of the Act.

2. THE CONTEXT

This is the fourth significant bill over the last 12 months[3] encompassing national security and counter-terrorism matters and the second inquiry relating specifically to the TIA Act 1979.[4] It has been an extraordinarily intensive period of legislative activity in this complex and sensitive area – possibly unrivalled within any other liberal democratic nation. The cumulative volume and the short timeframes for consideration of each element (or tranche) of this hugely important legislation has placed a heavy burden on the Australian parliament and on civil society organisations wishing to understand and assess the proposed legislation and the implications for our nation's security and our democratic values, civil liberties and human rights.

Like others the CCLS have done our best to meet this challenge around each review process.

We appreciate the increased pressures of the very real terrorist threat in the Australian, as well as international, context - and the need for the Government and the Parliament to ensure adequate laws and resources for the best possible protection of Australia's national security, consistent with a robust democracy. This complex but absolutely essential balance between security and democratic values is at the heart of the necessary and proportionate test that we accept as defining how far we are willing to go as a nation in encroaching on rights and liberties to protect national security.

As is clear from our submissions on counter-terrorism and national security matters across 2014[5], the CCLS are concerned that some of the new laws fail the necessary and proportional tests in relation to important rights. In part this has resulted from the haste with which legislation has been drafted and moved through the parliament.

There have been disturbing indications that senior members of parliament did not understand key aspects of the laws they were endorsing. In at least one instance a senior and experienced member of parliament has acknowledged that the passage of a particularly controversial –and in our view very dangerous law - was a mistake.[6]

---

[3] National Security Legislation Amendment Bill 2014; Counter-Terrorism Legislation Amendment Bill (No.1) 2014; Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014.

[4] Comprehensive revision of the Telecommunications (Interception and Access) Act 1979 (the Act), Senate Standing Committees on Legal and Constitutional Affairs

[5] Joint CCLS submission to PJCIS inquiry into Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 - October 2014; Joint CCLS submission to PJCIS inquiry into Counter-Terrorism Legislation Amendment Bill (No.1) 2014 - August 2014; Submission of the Civil Liberties Councils across Australia to the Parliamentary Joint Committee On Intelligence And Security inquiry into the National Security Legislation Amendment Bill (no 1) 2014; NSWCCL Submission: The Comprehensive Revision Of The Telecommunications (Interception And Access) Act 2014

[6] Anthony Albanese MP statement in relation to the creation of a new offence of unauthorised disclosure by any person of information relating to a Special Intelligence Operation by ASIO as part of the counter-terrorism package in the National Security Legislation Amendment Bill (No.1) 2014- S 35P. MPS Kate Ellis (ALP) and Kelly O'Dwyer (Liberal) appeared to have inaccurate understanding of the

We are concerned that this bill represents another example of unnecessary (last minute) haste, loose drafting, serious disparity between what the Government says about the proposals and what the bill actually requires - with the attendant risks of a bad and unintended (or at least unacknowledged) legislative outcomes.

The issue of mandatory retention of telecommunications data is not new. It has been on the Australian Government's agenda since 2012 and has been the subject of two PJCIS reviews, an ongoing comprehensive review of the TIA and a review of the current Bill by the Parliamentary Joint Committee on Human Rights. In that sense, it cannot be seen as rushed policy. The Government has been working on the detail of this policy for over two years. It is highly controversial and contended policy globally, as well as in Australia.

The CCLS regard it as very significant legislation for a democracy.

It is, therefore, totally unacceptable that the long awaited draft legislation before Parliament is, as it has been widely described, little more than a legislative shell[7]. Numbers of absolutely central matters, including the detailed definition of the telecommunications data that is to be mandated for collection and retention and clear specification as to which bodies will be given access to this data are not included in the bill and will be determined by later regulation and ministerial declaration.

RECOMMENDATION 1

The CCLS register their strong condemnation of the Government's failure to include clear definitions of central elements of the proposed telecommunications data retention and access regime in the bill and recommend the bill not be considered further by Parliament until these matters have been addressed within the bill.

Although the data retention issue has been on the agenda for three years, and the Government has followed good process by referring the bill for parliamentary committee review - once again, with no visible justification, civil society and the parliament are required to respond to this important and contentious bill in a very tight timeframe - which also happens to incorporate the Christmas and New Year holiday period. Few civil society organisations are able to engage their expert members and supporters over this period. Our concern is that many groups wanting to respond will not have been able to do so because of the timing.

The CCLS register concern at the difficult timing of this review process.

3. THE CORE POLICY ISSUE OF MASS DATA RETENTION

To legislate for the mandatory collection and retention of mass telecommunications data for the bulk of Australia's population to enable retrospective access by authorities is a major step for a democracy. It constitutes a major intrusion into the right to privacy of all citizens including those who are not suspected of any participation in unlawful activity. This will have major flow-on negative implications for other freedoms and democratic values.

---

controversial S 35P provisions and the powers of ASIO to add, copy, delete or alter' a citizens computer. ABCTV Q&A October 2014 Transcript

[7] For example Professor George Williams *Holes in Metadata bill make it unacceptable* SMH opinion piece 29/12/14

The CCLS consider it to be a step too far. We oppose the proposed data retention regime for a range of reasons.

3.1. The scope and significance of telecommunications meta-data

It is wilfully misleading of Governments to suggest that the current proposal relating to the retention and access to meta-data amounts to nothing more than an updating of existing laws and practices to accommodate new technologies and communications devices.

The proposed regime will give authorities access without warrant to an unprecedented range of rich personal information for a majority of the residents of Australia. The use of digital technologies such as the Internet, mobile and smart phones and WiFi-enabled devices, have become part of everyday life for Australians generating extensive meta-data. There is an abundance of material that establishes how extensive and informative telecommunications meta-data is and how it provides a comprehensive profile of all aspects of a person's life.

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 meta-data provide such rich information about individuals and groups that it no longer makes sense to distinguish meta-data from telecommunication content data.

The Government's description of telecommunications 'meta-data' as being like 'the information on the outside of the envelope' cannot be viewed as a serious contribution to the debate.

3.2. Data retention and the right to privacy

The mass collection and retention of large quantities of telecommunications data generated by this everyday use of such devices constitutes a serious interference with the right to privacy. It makes it possible to conduct retrospective surveillance, throughout the data retention period, of the private lives of ordinary Australians. As recently observed by the European Court of Justice 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'.*
>
> and
>
> *The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.* [8]

The Government does in fact recognise that the proposal will have a significant impact on the right to privacy but argues that this is justified by the benefits of more effective crime prevention and national security capacity that will be enabled by the data retention. Thus the bill's objective is stated as:

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

'*the protection of national security, public safety, addressing crime, and protecting the rights and freedoms by requiring the retention of a basic set of communications data required to support relevant investigations'* [9]

3.3. Proportionate and necessary

Given the curtailment to the right of privacy that the mass retention of telecommunications data represents, there is a heavy onus on the Government to show that such interference is proportionate and necessary.[10] The Government argues that it does substantiate these tests.

To the extent that the right to privacy is impinged, the interference corresponds to a 'pressing social need', that is the need for law enforcement agencies to effectively investigate and prosecute crime. The limitation is proportionate because the measures are precisely directed to the legitimate aim being pursued. [11]

This statement misconstrues the test for proportionality under human rights law. The objective to allow law enforcement agencies to effectively investigate and prosecute serious crime is a perfectly legitimate one. There is little doubt that this objective may be a legitimate reason for limiting the right to privacy. However, for such a limitation to be proportionate and necessary under human rights law, the Government must use the least intrusive means that will achieve the desired result.[12] The CCLS are of the view that the data retention regime proposed in this bill fails the proportionate and necessary tests on multiple counts.

We offer some examples.

First, the threshold of access to telecommunications data is much lower than what is needed to effectively investigate serious crime. Access to telecommunication data can lawfully be obtained by enforcement agencies, if an authorised officer within such an agency is satisfied that the information is 'reasonably necessary' for the enforcement of a criminal law, a law imposing a pecuniary penalty, or for the protection of the public revenue. No threshold with respect to the seriousness of the crime being investigated is required. Moreover, access can be lawful if nothing more is being investigated than a law imposing a penalty or a tax.

Second, no guidance is provided in the TIA Act as to the meaning of "reasonably necessary". There is no requirement that the interference with an individual's privacy be proportionate to the subject matter of the investigation.

Third, Chapter 4 does not require that there be any nexus between the person whose information is being accessed and the subject matter of the investigation. Accordingly, the private information of individuals who are under no suspicion of wrongdoing may be accessed if such information is reasonably necessary with respect to the suspected wrongful conduct of another.

Fourth, the Bill and the provisions of Chapter 4 do not provide adequate safeguards to ensure the right to privacy of Australians is protected. A number of standard safeguards are not utilised. These

---

[9] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum (EM) at P 6

[10] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014 at [20].

[11] EM p 11 [35].

[12] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014 at [25] and *Digital Rights Ireland and Ors* (C-293/12) *and Kärntner Landesregierung and Ors* (C-594/12), 8 April 2014, at [46].

include: the requirement for prior oversight by judicial authorities or other independent authorities which require a case-by-case assessment of requests for access to telecommunications data;[13] the requirement that enforcement agencies that have accessed telecommunications data destroy such data once its usefulness has been exhausted and notify the person whose information had been accessed, at least retrospectively;[14] limiting the use and sharing of the accessed data between agencies[15] and limiting the period of time for which the data is to be retained to the shortest possible period[16].

None of these measures would be unduly burdensome on authorities, but together, would provide more effective safeguards for the protection of privacy than are contained in the bill. We will make further comment on some of these safeguard measures in a later section.

3.4. The importance of privacy

This mandatory retention of extensive meta-data amounts to a gross invasion of the right to privacy which, while not an absolute right, is an important right with very real significance for the nature of society.

Privacy is no trivial matter. It matters and its status has significant implications for the nature and quality of personal life, family life and the wider society. Intrusions on it have effects. They harm the individuals whose privacy is invaded. But even more importantly, society suffers.

Privacy is a fundamental human right, in that it is central to the maintenance of democratic societies and is essential to human dignity. In its absence, there is no freedom of expression and information, and no freedom of association.

Privacy gives us the freedom to define ourselves and our relations with others. It is essential for human development.

But this is not only a psychological necessity. Privacy is necessary for the development of dissent, for the formation of challenges to orthodoxy.

It is for such reasons that privacy is recognised under international human rights law.

3.5. Impact on a free media

A major concern of the CCLS about the proposed mass data retention regime is the flow on effects on other freedoms. Most significantly this regime will create a real threat to our free media. It will make it extremely difficult for any sensitive information to be provided to journalists as it will not be possible to guarantee confidentiality of any kind of telecommunication.

It will also threaten the capacity for legitimate whistle-blowers to bring important information about official or corporate misbehaviour or corruption to public notice and this does not augur well for any democratic society.

---

[13] Opinion of the Advocate-General Cruz Villalón of the Court of Justice of the European Union in joint cases C-293/12 and C-594/12 at [127].

[14] Ibid at [129].

[15] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, at [27].

[16] Opinion of the Advocate-General Cruz Villalón of the Court of Justice of the European Union in joint cases C-293/12 and C-594/12 at [149].

Cumulatively the effect of this proposal will be very bad for robust democratic values and practice. Ordinary people will be more cautious about many kinds of communications knowing they can be retrospectively accessed by authorities for up to two years- and without the knowledge of the person.

3.6. Will it make us safer?

The Government bases its support for the regime on the argument that telecommunications data is an essential investigative tool for intelligence, security and police organisations:

> *'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.'*[17]
>
> *Access to historical data and analysis of inter-linkages with other data sources is vital to both reactive investigations into serious crime and the development of proactive intelligence on organised criminal activity and matters affecting national security*[18]
>
> *The data retention measures contained in the Bill will ensure the retention of the basic telecommunications data that is essential to support Australian law enforcement and security agencies in the performance of their functions*[19]

The CCLS accept that telecommunications data is an important investigative tool and that law enforcement and security agencies should have appropriate access to it. What we do not accept is that appropriate access should extend to the compulsory collection and retention of mass telecommunications information (meta-data) of virtually the whole population.

Apart from the central civil liberties concern about the serious impact on the right to privacy and other freedoms, we share the scepticism of many experts, parliamentarians, legal and civil society groups that the mass collection and retention of telecommunications data of non-suspect citizens for retrospective access will significantly increase Australia's (or any nation's) safety from terrorism and serious crime.

The recent tragedies in Sydney and Paris have generated reasonable comment around the fact that the perpetrators were well known to police and intelligence agencies but had been allowed to drop from active surveillance.

Such focussed research as exists on this central issue of necessity and effectiveness is not conclusive- but it certainly does not support the unequivocal claims of the Government on this matter.

The experience of Europe during the period between when the European Data Retention Directive came into force in 2005 and its being ruled invalid in various courts and ultimately by the European Court of Justice on 8 April 2014, provides rare evidence (other than anecdotal) on the effectiveness or otherwise of mandatory data retention. The evidence from this experience is that mandatory mass data retention makes no difference. Between 2007 and March 2010 there was no discernable change in the outcomes of investigations as a result of the mandatory data retention regime.

[17] EM Para 5, p.5
[18] EM Para 7, p6
[19] EM para 8, p6

The Scientific Services Section of the German Parliament analyzed the effects of data retention on

crime clearance rates in a number of EU member states and concluded that "In most states client clearance rates have not changed significantly between 2005 and 2010."[20]

According to the European Digital Rights Organisation, a German study showed that blanket data retention would have made a difference in only .002% of criminal investigations.

The Digital Rights group argues that while blanket data retention may be helpful in some cases, that has to be balanced against the negative effect of encouraging people to move to the use of internet cafes, unregistered pre-paid mobile phones, VPNS and similar devices to avoid detection. [21]

More recent reviews of the effectiveness of mass data collection and retention regimes from the USA –where the debate on this issue has been intense since the Snowden revelations in 2013- have divergent findings. Both reviews were in response to President Obama's search for alternatives to the NSA's bulk data collection programs.

The most recent report by US National Research Council and sponsored by the Office of the Director of National Intelligence found:

"*There are no technical alternatives that can accomplish the same functions as bulk collection and serve as a complete substitute for it; there is no technological magic,*"

According to the Reuters, the reviewers did however, find it might be possible to develop techniques that improve targeting and provide a viable substitute for bulk collection. [22]

An earlier review by the Privacy and Civil Liberties Oversight Board set up by President Obama following Snowden's revelations reported it could find no evidence that sweeping collection of the telephone metadata of Americans led to a single major counter-terrorism breakthrough.[23] It also expressed the view that there was no information obtained that couldn't have been procured through a more conventional, court-ordered search.

At best, the available, evidence-based research suggests a high degree of uncertainty as to the effectiveness of mass telecommunication data retention regimes in preventing terrorism and other serious crimes.

[20] Quoted in German police statistics prove telecommunications data retention superfluous (6 Jun 2011) Working Group on Data Retention http://www.vorratsdatenspeicherung.de/content/view/455/79/lang,en/

[21] European Digital Rights Shadow evaluation report on the Data Retention Directive (2006/24/EC) 17 April 2011 https://edri.org/files/shadow_drd_report_110417.pdf page 14 and see also German police statistics prove telecommunications data retention superfluous (6 Jun 2011) Working Group on Data Retention http://www.vorratsdatenspeicherung.de/content/view/455/79/lang,en/ and 'Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics ' Arbeitskreis Vorratsdatenspeicherung, 19 February 2011, at http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

[22] National Research Council of the National Academies:Bulk Collection of Signals Intelligence Technical Options Washington 2015. Reported in SMH 16/1/15 "No substitute to gathering bulk communications intel'.

[23] Privacy and Civil Liberties Oversight Board: Report on the Telephone Records Program January 23, 2014

This uncertainty strengthens the CCLS view that the serious infringement on ordinary persons' privacy and the flow-on cost to other liberties and democratic values in our community that will result from the implementation of the proposed data retention regime, are not justified.

But it should be noted that, even if the claims of the Government and intelligence and police agencies in relation to effectiveness and necessity could be demonstrated to have more certain legitimacy, in our view the cost to privacy, liberties and democratic values would still be too great to justify the proposal.

3.7. The global trend

Government ministers in their public statements supporting the proposal have on occasions suggested that mass data collections and mass surveillance programs are clearly the way of the future. This is not an accurate world view. The disturbing and dramatic move in recent years towards greater mass surveillance and mass data retention in liberal democracies around the world is highly controversial and tightly contended.

It is a profoundly important and defining debate for liberal democratic societies and it is a long way from being over.

Liberal democrats have historically been opposed to any form of mass surveillance and mass data retention by governments or their agencies. The heightened and more dangerous political context post 9/11 opened the door for movement on this front and there was a major expansion of mass surveillance programs utilising the rapidly developing telecommunication surveillance technologies. Some of this expansion was open and debated; a considerable amount was done secretly and even unlawfully.

The revelations by Edward Snowden in 2013 as to the scope, volume, analytic capacity and international sharing of systemic telecommunications surveillance by NSA and other intelligence agencies through a variety of programs were astonishing and have generated an ongoing global fight back.

One manifestation has been the growing international profile of the global alliance of civil liberties and human rights organisations that has worked very successfully to develop necessary and proportionate principles to address global developments in surveillance. *The International Principles of the Application of Human Rights to Communications Surveillance* were launched at the 24th Session of the United Nations Human Rights Council in Geneva on 20 September 2013.[24]

The debates in Europe and the United States have been particularly intense and opposition among politicians, lawyers, academics and civil society groups has been strong and growing. The courts and parliaments in Europe and the USA have also been active players.

The European Court of Justice has ruled that blanket retention of meta-data is disproportionate.

There is currently no proposal in the United States for a mandatory data retention law. Two Bills introduced in the Congress in 2009 which would have required all internet providers and operators of Wi-Fi access points to keep records on internet users for at least two years to assist police in investigations lapsed.

[24] https://en.necessaryandproportionate.org/ Now known as 13 principles.

It would appear that any such legislation in the US is likely to face significant constitutional obstacles. On 11 June 2014, the 11th Circuit of the United States Court of Appeals held in the decision of *US v Davis* that a warrant was required for police to obtain access to cellular phone location data. The Supreme Court of Florida in the decision of *Tracey v Florida* (16 October 2014) held that that State's constitution also prohibited access to cell phone location data without a warrant. The same result was reached by the Supreme Court of Massachusetts in *Commonwealth v Augustine* (18 February 2014) and by the Supreme Court of New Jersey in *State v Earles* (18 July 2013).

Whilst these decisions only relate to cellular phone location data it is difficult to see how the same principles do not apply for example to internet metadata.

Since these decisions, Kansas, Massachusetts and Utah have passed laws requiring police to obtain warrants before obtaining access to what would broadly be described as metadata:. Other states including Colorado, Maine, Minnesota, and Montana have passed laws requiring the police to obtain a warrant to access cell phone location data.

James Ball assessing current recent trends in the battles around surveillance in the US and UK suggests that while 2014 was 'the year the administration struck back' *'both sides of the Atlantic might find next year* [2015] *a closer fight than they would think'.* [25]

Two key pieces of legislation are coming up for renewal.

There will be a highly contended debate around the scheduled expiry of provisions in the USA Patriot Act on 1 June 2015 which provide the legal basis for the Government's bulk data collection. There was an attempt last year to get them extended until 2017 in Sen. Pat Leahy's USA Freedom Act, but the bill could not overcome the scepticism of some intelligence watchdogs and the party-line opposition of Republicans.[26]

Similarly in the UK, the major parties have pledged to re-examine the critical Regulation of Investigatory Powers Act which authorises most UK mass-surveillance programmes and allows police and other authorities to access journalists' telephone records after the election. The UK also has to renew the controversial Data Retention and Investigatory Powers (Drip) legislation by the end of 2016. The other key site to watch will be the courts: there are multiple challenges in UK tribunals, the Organisation for Economic Cooperation and Development, the European court of justice, and several cases attempting to get the US Supreme Court to make its first surveillance rulings since Edward Snowden's leaks.

This important debate about mass surveillance and data retention has been more muted in Australia than in Europe, the UK or the US. The level and intensity of debate lifted last year when it was realized how extensive and invasive of privacy some of the provisions in the first tranche of counter terrorism laws were and what a devastating effect the new offence of unlawful disclosure of

[25] James Ball: *When it comes to surveillance , there is everything to play for.*Guardian Australian edition 1/1/15

[26] Gregg Levine: 'Government data-collection report favors government data collection' The Scrutineer 15/1/15 http://america.aljazeera.com/blogs/scrutineer/2015/1/15/bulk-data-collectionstudy.html

Information relating to ASIO Special Intelligence Operations would have on journalists.[27] Hopefully that belated level of interest will be reignited by the issues raised by this mass data retention proposal.

The point of this brief diversion is that the issue is not decided globally.

There is no clear and uncontentious policy pathway for Australia to follow. There is a real and profoundly important debate underway about the safe balance in a democracy between the relative value of privacy, freedom of the press, legitimate whistleblowers and the competing value of mass surveillance and data retention in the interests of security and safety.

Members of Parliament, the media and civil society in Australia need to give careful and informed consideration to where the line should be drawn in a democracy.

RECOMMENDATION 2

The CCLS strongly oppose the central proposal in the bill to introduce a statutory obligation on telecommunication service providers to collect and retain prescribed telecommunications meta-data of their clients for two years so that authorities can access such data without warrant. We urge Parliament to reject this proposal on the grounds that it is a disproportionate, unnecessary and inappropriate policy which will undermine important rights and democratic values long held as fundamental to our democratic way of life in Australia.

The CCLS consider the option of a more targeted data surveillance scheme is more compatible with liberal democratic values even in the current context where Australians –along with citizens in many parts of the world- are confronted with heightened threat of terrorist actions – than any mass surveillance scheme that would allow government and its agencies access to deeply private data about the lives of most of the community.

Collection retention and access to modern telecommunications data should be targeted to persons who are suspected of involvement in serious wrong doing.

A central aspect of the current global debate about mass data retention and government surveillance is the exploration of alternatives which are less invasive of the citizenry's privacy but still responsive to the needs of security and police agencies. These schemes incorporate quite familiar elements such as:

- quick response preservation of data of persons who have been identified as posing a real and immediate serious threat and designated vulnerable groups;
- requiring persons convicted of specified crimes released on licence to register their means of electronic communication for data preservation for a prescribed period;
- case by case judicial authorization for preservation targeted at those reasonably believed to have engaged in criminal activities (with emergency procedures).

[27] The notorious S 35P amendment as part of the National Security Legislation Amendment Bill (No 1) 2014 amendments. TAs part of this package, Parliament also gave ASIO extraordinarily wide access to (undefined) networks of computers of both suspects and non-suspects

- targets to be notified afterwards where suspicious proved unfounded in the absence of compelling reasons not to do so
- access to the data on judicial authorization.

The CCLS consider this a less dangerous (to our privacy and liberal democratic practices, and possibly an equally effective surveillance regime as an alternative to the indiscriminate mass data collection proposed in the bill.

The CCLS understand that such targeted data preservation schemes are in use in Austria, Belgium, The Czech Republic, Germany, Romania and Sweden.[28]

RECOMMENDATION 3

The CCLS do not oppose the prospective surveillance of, mandatory retention of and access by prescribed authorities to telecommunications data in relation to persons or groups for whom there is reasonable suspicion that they may be, or have been involved in terrorist or other serious criminal activity as long as such surveillance and access to retained data is on the basis of a prior warrant approval.

4. PRAGMATIC IMPROVEMENTS

The CCLS hold strongly to their principled opposition to any mass telecommunications data retention regime for retrospective access by government and its agencies. This is our policy position and we will continue to argue for it in the public interest.

Nonetheless, we accept that it is obviously possible the PJCIS and the Parliament may accept the core data retention proposal as a necessary and proportionate infringement on privacy and other liberties in the interest of national security and serious crime prevention.

If this option is taken, it is imperative that major problems with key elements of the proposal as set out in the bill are addressed.

As the Parliamentary Joint Committee on Human Rights (JCHR) points out[29], because the proposal clearly limits the right to privacy *'the scheme must be sufficiently circumscribed to ensure that limitations on the right to privacy are proportionate (that is, are only as extensive as strictly necessary)* '[30]

As it stands the bill clearly fails to achieve this. If the proposal as currently drafted were to proceed, it is difficult to see how the Government's claim to have established necessity and proportionality wherever rights are impinged upon, could withstand any fair and reasonable analysis.

The rest of this submission addresses some of the major issues that would have to be addressed to limit as much as possible the infringements on privacy and the flow-on impacts on other liberties and democratic values.

5. OVERSIGHT AND ACCOUNTABILITY

[28] This information has not been directly checked.
[29] EM 7
[30] Parliamentary Joint Committee on Human Rights report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Fifteenth Report of the 44th Parliament, Nov 2014.(PJCHRC report 2014) para 1.31, p13.

The Government makes much of the stronger safeguards and oversight mechanisms it has included in the bill. While these are welcome, the CCLS join other commentators in arguing the safeguards are far from adequate for such an intrusive surveillance power- which captures non-suspects as well as suspects - and must be strengthened by additional and more effective mechanisms.

5.1. The Commonwealth Ombudsman

Schedule 3 provides for oversight by the Commonwealth Ombudsman of the mandatory data retention scheme and the extent of compliance with Chapter 4 by enforcement agencies and the extent of compliance by criminal law-enforcement agencies with Chapter 3. In order to facilitate this oversight, agencies must keep records of authorisations made for access to telecommunications data and must co-operate with investigations by the Ombudsman. Each year the Ombudsman must report to the Minister in writing about the inspections conducted with respect to compliance with the TIA Act. The Minister must cause a copy of the report to be laid before each House of the Parliament. If as a result of an inspection the Ombudsman is of the opinion that an officer has contravened a provision of the TIA Act, the Ombudsman may report on the contravention in its report to the Minister.[31]

This role for the Ombudsman is a welcome addition to the general oversight of the scheme. The NSWCCL recommended such a role in its submission to the comprehensive revision of the TIA last year but argued that 6 monthly reports to Parliament were appropriate. [32]

In the context of the proposed mass data retention regime however, the Government should provide for effective oversight which will ensure accountability for arbitrary or unlawful interference by enforcement agencies with the right to privacy as required by the International Covenant on Civil and Political Rights (**ICCPR**) [33] Moreover, the ICCPR states that parties must ensure victims of violations of the Covenant have an effective remedy.[34]

The Ombudsman's oversight role will neither provide for effective oversight nor provide any remedy or sanction for unlawful access. Under the provisions in Schedule 3, unlawful conduct on the part of enforcement agencies in accessing telecommunications data may never come to light, because the Ombudsman is not required to report on any contravention of the TIA Act. Moreover, there is no requirement to inform a person whose telecommunications data had been accessed. In fact, to do so would be an offence punishable by 2 years imprisonment pursuant to s181B of the TIA Act.

In the circumstances, unlawful access to telecommunications data will likely go unknown and even if the Ombudsman reports on such conduct, there is no provision for any sanction.

The Commonwealth Ombudsman's Office is not well resourced. This is a significant and important new role. It is obviously important that the Government provides additional resources to the

---

[31] s 186J of the Bill.

[32] NSWCCL Submission Comprehensive Revision Of The Telecommunications (Interception And Access) Act 2014, (NSWCCL Submission TIA 2014) P10 .

[33] *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, at [37]. Article 17 of the International Covenant on Civil and Political Rights provides that: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honour and reputation' and that "Everyone has the right to the protection of the law against such interference or attacks

[34] Article 2(3).

Ombudsman to allow this role to be implemented effectively.

RECOMMENDATION 4

a) **The CCLS welcome the detailed provisions in the bill for post-access oversight by the Commonwealth Ombudsman of the data retention and access regime, however in our view this will not prevent violations of the process nor guarantee appropriate remedies for any violations.**
b) **To ensure that this role can be carried out effectively the CCLS recommend the Ombudsman's Office be provided with adequate additional resources.**

5.2. PJCIS Review

The Government has made provision for the PJCIS to review the scheme three years after its commencement. This is a welcome provision for a post hoc comprehensive and open review of the regime. We have two reservations about this provision.

Obviously it will not address the need for prior oversight and protection against unwarranted violations of privacy. That will need to be addressed by an additional process.

Given the significance of the proposed regime, the CCLS consider an earlier review schedule is necessary and recommends the PJCIS review the scheme annually.

RECOMMENDATION 5

The CCLS recommend that the proposal for the PJCIS to review the data retention scheme be amended to provide for annual reviews.

5.3. IGIS

The role of the Inspector General of Intelligence and Security in oversighting ASIO's processes and access to telecommunications data has not changed. It is to be hoped that the promised additional resources for her office will give her greater capacity to fulfil her now quite extensive oversight role adequately.

5.4. Warrant only access

The CCLS greatest concern about the proposed safeguards is the lack of prior oversight of the operation of enforcement agencies access to telecommunications meta-data.

As it stands, the as yet unknown number of 'enforcement agencies' to be given access to meta-data will not require a warrant to do so. They will be able to authorise service providers to provide the information on their own say-so as long as the access 'is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or a law protecting the public revenue'. 'Criminal law enforcement agencies' may also authorise disclosure of prospective meta-data if the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of a serious offence (as defined in the TIA Act) or an offence which is punishable by imprisonment for at least 3 years. The authorisation allowing access to prospective telecommunications data may be valid for up to 45 days. [35] ASIO will be able to access all meta-data as long as the data is 'in connection with the performance of the agencies functions'[36]

[35] TIA 1979 ss 171-186
[36] TIA 1979 ss 175-176

The CCLs have always been of the view that the current access to telecommunications meta-data under the TIA should have only been on the basis of a judicial warrant authorisation. Given the extensive personal information which is retrievable from the extended range and quantity of meta-data accessible through the proposed scheme, this issue moves into sharper relief. This was noted by the PJCHR in its report:

> *Under the TIA Act, access to communications (content) requires a warrant while access to telecommunications data (metadata) does not. However, technology has significantly developed since the TIA Act was enacted with the development of new forms of communications technologies and, consequently, new forms of metadata. In this respect, the committee notes that the assessment of this bill brings into sharper focus potential inadequacies of the TIA Act in terms of specific safeguards around access to telecommunications data and content.* [37].

It is clearly unacceptable for the 'enforcement agencies' or ASIO to be their own authorisers of access to such personal information. Any oversight of their processes and detection of any abuse of the legal parameters could only be detected post hoc.

There is an obvious and well tested, traditional safeguard that should be included in the bill. Access to both retrospective and prospective meta-data under the proposed scheme should only be on the basis of a prior warrant authorisation from a judicial authority.

The CCLS do not accept the argument that having to access a warrant will impose an unmanageable administrative burden on the agencies or ASIO. The warrant process provides an important procedural safeguard without any great inconvenience. Such inconvenience and administrative burden that does accompany it, is a reasonable and necessary trade-off for such significant intrusion into the privacy rights of the community.

RECOMMENDATION 6

The CCLS strongly recommend that access by enforcement agencies, criminal law enforcement agencies and ASIO to retrospective and prospective meta-data be subject to prior independent assessment on a case by case basis through a warrant issued by a judicial body

5.5. Public Interest Monitor

The NSWCCL has previously argued for the appointment of a Public Interest Monitor (PIM) in the context of the current review of the TIA[38]. The target person is not currently represented at the issuing of warrants for access to telecommunications content. Nor would they be represented at the issuing of warrants for access to meta-data under the proposed scheme.

In any kind of covert operation, the rights of the target need to be protected. Protection is needed to ensure that warrants are not being rubber stamped and that the impact of the invasion of privacy is properly evaluated - including the impact on the community and the public interest.

The CCLS are of the view that there is merit in considering such a role in relation to the issuing of warrants within the proposed data retention regime.

[37] The PJCHR report 2014 para 1.22 p11

[38] NSWCCL submission TIA 2014, Rec 16. For a more detailed argument in support of the PIM see pp12-14.

RECOMMENDATION 7

Noting that the warrants would be issued ex parte, the CCLS recommend an additional oversight mechanism of a Public Interest Monitor to represent the rights of the person whose data is being sought or, as proposed by the PJCHR, close ongoing oversight of the warrant process by the INSLM.

6. ACCESS THRESHOLDS

The CCLS do not accept that the proposed thresholds for access to the meta-data are stringent enough. They certainly are not aligned with the statements by Ministers that the regime is directed towards serious crime and terrorism and will not be able to be directed towards minor offences, or copyright infringements or online piracy.

This threshold problem manifests itself in both the loose definition of the agencies which can access the telecommunications data and in the provisions specified in the current Act to allow authorisation of the release of stored meta-data being requested by an agency[39].

6.1. Data Release provisions

The release of stored meta-data may be authorised when it is considered 'reasonably necessary' for the 'enforcement of a criminal law, a law imposing a pecuniary penalty, or for the protection of the public revenue'.

"Reasonably necessary' is not defined in the bill and is open to wide range of legitimate interpretations. The Government is sensitive to this and has a pre-emptive defence of the provision in the Statement of Compatibility in the Explanatory Memorandum:

> *'Enforcement agencies may only issue authorisations enabling access to data where it is 'reasonably necessary' for a legitimate investigation and must consider the privacy impact of accessing telecommunications data. 'Reasonably necessary' is not a low threshold. It will not be 'reasonably necessary' to access data if it is merely helpful or expedient'.*[40]

In our view it is too low a threshold. Given the serious privacy implications, proportionality and necessity would be better served by a stronger provision – access should be 'necessary'.

The provision for release of prospective telecommunications data to the criminal law-enforcement agencies is reasonably necessary for the investigation of a serious offence (as defined in the TIA Act) or an offence which is punishable by imprisonment for at least 3 years. While the weak 'reasonably necessary' is used, this provision does set a level of seriousness for the offence being investigated.

The lack any such threshold as to the seriousness of the offence being investigated when access to stored meta-data is authorised is not acceptable. When linked with the open-ended definition of requirements allowing the Minister to declare 'enforcement agencies' (see discussion below), it is obvious that the bill does not deliver the constraints that the Government has suggested will apply to access to this sensitive information.

[39] TIA chapter 4 ss171-186
[40] EM para p16

The bill must incorporate a provision which limits release of meta-data to investigation of serious criminal activity. In conjunction with an independent judicial warrant process, this will go some way towards limiting the potential for unwarranted invasion of privacy.

RECOMMENDATION 8

The CCLS strongly recommend that warrants for access to telecommunications meta- data should only be issued on the basis that it is: i) necessary to assist with the enforcement of a criminal law, a law imposing a pecuniary penalty or a law protecting the public revenue and ii) where it is necessary for the investigation of a serious criminal offence.

6.2. Criteria for declared agencies with access to data

The number and range of agencies that have been able to access telecommunications data under the current regime has long been a matter of public concern.[41] A review of the *Telecommunications (Interception and Access) Act* 1979 – Annual reports, published by the Attorney-General's Department, show that the agencies that use the provisions under the TIA Act to gain access to telecommunications data goes far beyond agencies that are responsible for investigating serious crime or protecting national security. They include non-government charities such as the RSPCA, statutory bodies such as Australian Post, professional regulatory bodies such as the Tax Practitioners Board and local councils such as the Wyndham City Council.[42]

Under the TIA Act enforcement agencies currently have access to stored communications (the 'content' e.g. emails and sms messages) by warrant and to stored telecommunications data (the meta-data) without warrant[43]. The Government has indicated that the bill will reduce the numbers and range of organisations which will have access to each of these categories of stored data.[44]

The bill creates two categories of authorised organisations: criminal law enforcement agencies and enforcement agencies (which incorporate the former).

6.3. Stored Communications (Content) access

Under the proposed regime, the bill will restrict access to stored communications (content) to '**criminal law** enforcement agencies' which will continue to be on the basis of warrant authorisation.[45] The bill's mechanism for achieving this by restricting access to a subset of the current 'enforcement agencies' category, implies that agencies responsible for 'imposing pecuniary penalties or protecting the public good' would be excluded from access to this personal information. Few would disagree that access to such 'content' data is very sensitive and access to it constitutes a very significant intrusion into a person's privacy. The Government's stated commitment to reduce the number and range of agencies able to have this access is therefore a very welcome one.[46] However, extraordinarily, the bill does not guarantee this outcome. The bill provides for the Attorney-General to declare additional 'criminal law enforcement agencies' beyond the 12 specified organisations (or groups of organisations- ie a police force of any state) .[47] On our close reading, the designated range of factors the Attorney-general must 'have regard to' are open-ended. While the first specified factor is very properly:

[41] Law Council of Australia's submission to the Senate Standing Committee on Legal and Constitutional Affairs inquiry into the Comprehensive Revision of the *Telecommunications (Interception and Access) Act* 1979, March 2014, at 27 – 29.
[42] See the Annual report for the year ending 30 June 2013 at 48 – 51.see also NSWCCL submissions……
[43] TIA chs 3,4
[44] EM 8, 21,
[45] Bill sch 2, item 3, cl110A(1)
[46] EM 21, , 2R speech. Media ??
[47] Bill sch 2, item 3, cl 110A(3)

(a) whether the functions of the authority or body include investigating serious contraventions;

the list also includes a range of less discriminating factors including the very open-ended:

'f) any other matter that the Minister considers relevant'.

The range of organisations able to be so declared is in fact only limited by the Attorney-General's discretion.

If the designation of a smaller grouping of agencies as '**criminal law** enforcement agencies' is to guarantee/deliver the Governments claimed policy objective of a substantial reduction in the number of agencies having access to sensitive stored communications warrants the bill must be amended to require a much tighter and more appropriate criterion for declaration of additional **criminal law** enforcement agencies'.

This can be achieved by making one of the factors already listed in the bill a limiting factor.

s110(4) (a) 'whether the functions of the authority or body include investigating serious contraventions' - should be a limiting factor. [48]

RECOMMENDATION 7

The CCLS recommend that any additions to the specified 'criminal law enforcement' agencies on the basis of declaration by the Attorney-General should be limited within the bill to those agencies whose functions include 'investigating serious contraventions.' (Sch 2, item 3, s 110A(4) (a))

6.4. Stored Meta-Data Access

In the Explanatory Memorandum the claim is made that the provisions in Schedule 2 of the Bill will limit the range of agencies that are able to access telecommunications data.[49] This is a welcome policy position. However once again the actual provisions in the bill itself do not ensure such an outcome.

Enforcement agencies will maintain their current access to meta-data. The only enforcement agencies actually specified in the bill are the specified criminal law enforcement agencies.

Other 'enforcement agencies' may be declared by the Attorney-General on the basis of listed factors to which he must 'have regard'. These include:

(a) whether the functions of the authority or body include:
  (i) enforcement of the criminal law; or
  (ii) administering a law imposing a pecuniary penalty; or
  (iii) administering a law relating to the protection of the public revenue;[50]

and a range of other factors included for the declaration of criminal law enforcement agencies- including the open-ended:

' (f) any other matter that the Minister considers relevant.'

As with the declaration of criminal law enforcement agencies, the Attorney-General's discretion to declare any authority or body an 'enforcement agency' and thereby have

[48] Recommended by Dr Kieran Hardy and Professor George Williams: Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,Submission 5, 9th December 2014, p4
[49] Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2014, Explanatory Memorandum at 8.
[50] Sch 2, 176A, 4 (a), (i) (ii) (iii)

access to stored telecommunications data under the bill's provisions remains at large.

The current list of factors and the fact that they only have to be considered and are not limiting on any declaration do not instil any confidence that the threshold to be applied by the Minister will be very high.
Clearly, depending on how the Minister decides to exercise his or her discretion, there is nothing in the Bill to prevent the range of agencies that are allowed to access telecommunication data from being increased rather than decreased.

There is nothing in the bill's current provisions which would prevent bodies with an interest in pursuing copyright infringement or online piracy being declared in either category – contrary to the assurances of the Government that data retention would not be accessible for this purpose.[51]

The issue of who will have access to stored telecommunications data of every internet provider customer in Australia is of great significance in the determination of the proportionality of this intrusion into the privacy rights of a persons who are not suspected of any involvement in unlawful activity.

In the view of the CCLS this is an absolutely unacceptable situation and the bill must include both a clear definition of and specification of enforcement agencies.

Given the wide agreement that the number of agencies having access to telecommunications data must be drastically reduced and the apparent agreement that the data will only be accessed for the investigation of serious criminal activity, there is some question as to whether there should be a second category of 'enforcement agencies' at all.

RECOMMENDATION 8

The CCLS recommend that a clearer and tighter definition of types of organisations which can be declared as enforcement agencies be specified in the bill and that these be limited to those whose functions include:

- **i enforcement of the criminal law; or administering a law imposing a pecuniary penalty; or administering a law relating to the protection of the public revenue;[52] and**
- **ii some additional clear criteria which would ensure that only agencies dealing with serious crimes or serious unlawful actions are included.**

7. DEFINITION OF TELECOMMUNICATIONS DATA

Much of the controversy surrounding the early proposals from 2012 for a mass data retention scheme have centred on the issue of exactly what data would be captured, and exactly what did the Government have in mind when it flagged its intention to only capture 'meta-data".

No definition of the categories of data to be collected and retained in the bill, but to be set out in later regulation. Justification is that want to provide sufficient technical detail to telecommunications providers while retaining flexibility to adapt to rapid and significant future changes in technology.

[51] Eg Malcolm Turnbull's rejection that data retention would be used to pursue copyright infringements Bernard Keane in Crikey 11/12/14
[52] Sch 2, 176A, 4 (a), (i) (ii) (iii)

The flexibility argument is a weak and unacceptable excuse for the failure to define precisely what data will be collected and retained.

RECOMMENDATION 9

The CCLS strongly recommend that the bill be withdrawn from parliament and be redrafted to include the precise detail of the telecommunication meta-data which is required to be collected and retained. A further adequate consultation period be allowed for parliament and community to assess and respond to the defined data set.

The explicit exclusion of 'content' from the categories of prescribed data is a welcome concept. However, as experts point out, the presumed clear distinction between 'content' data and 'meta' data is mistaken. Much 'content' information about a person's life can be extracted from so called 'meta' data. Without a precise definition of what is meant by 'content' and by 'meta data' there can be no common understanding of what can lawfully be captured by the legislation.

RECOMMENDATION 10

The CCLS strongly recommend that the bill be withdrawn from parliament and be redrafted to include a clear definition of 'content' telecommunications data and 'meta' telecommunications data.

8. DATA RETENTION PERIOD

The bill proposes that the prescribed data for collection be retained for a period of two years. This is at the high end of the spectrum across jurisdictions with mass data retention regimes. Such information as is publicly available as to the use of meta data in Australia indicates that such data is accessed most frequently within 6 months. It is said that the less frequent (%?) use of the data post 6 months is necessary for investigations into terrorism and complex criminal offences.[53] The CCLs share the view of the PJCHR that the government has not provided a convincing justification for the lengthy two year retention period. The community is entitled to regard the specification of a poorly justified 2 year period as a concession to an ambit claim from the intelligence and law enforcement agencies.

RECOMMENDATION 11

The CCLS strongly recommend that the item 1 cl 187C be redrafted to reduce the period of mandatory data retention from two years to 6 months to align with the available evidence as to utility of the objective and therefore proportionality in the restriction of privacy rights.

Recommendation 12

The CCLS recommend that all persons whose telecommunications data has been accessed by criminal law enforcement agencies, enforcement agencies or ASIO should be informed of this access within a specified period of no more than two years.

[53] EM 19

CONCLUDING COMMENTS

The CCLs from NSW, Victoria, Queensland and South Australia and the Australian Council for Civil Liberties have collaborated on this submission because of the obvious national importance of the proposed data retention scheme and its major implications for privacy and other fundamental liberties long cherished in liberal democracies.

We hope our submission is of assistance to the PJCIS and the Government. We are pleased to take up the invitation to elaborate on this submission and respond to any questions at the public hearing on 30th January.

This submission was written by Dr Lesley Lynch, Secretary NSWCCL, Hugo De Kock, Barrister, LibertyVictoria and Michael Cope, President Queensland CCL on behalf of the combined CCLS.

Yours sincerely

Dr Lesley Lynch
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission
Dr Lesley Lynch
Secretary NSW Council for Civil Liberties