LAW INSTITUTE VICTORIA

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY INQUIRY

Contact:
Leanne O'Donnell, Policy Lawyer
T 03 9607 9380 **F** 03 9602 5270
LODonnell@liv.asn.au
www.liv.asn.au

TABLE OF CONTENTS

Executive Summary 1
Unanswered Questions 3
What data will be retained? 3
Is the retention of all this data “strictly necessary” for a legitimate purpose? 3
How will the data be retained? 4
Who will have access to the data? 4
What controls or limits will be on the access? 4
What are the safeguards to protect privacy and data security? 4
What are the costs to the community from this scheme? 5
Context: Legal and Technical 6
Recommendations 9
What data is to be retained? 9
Who can access the data? 11
What controls or limits are there on access to the data? 12
How long should the data be retained? 15
Conclusion 17

EXECUTIVE SUMMARY

The Law Institute of Victoria (LIV) is the peak body for the Victorian legal profession, representing over 17,000 members. Established in 1859, the LIV has a strong and proud history. We advocate on behalf of our profession and the wider community, lead the debate on law reform and policy, lobby and engage with government and provide informed and expert commentary.

There are 31 serious, unanswered questions about the mandatory data retention scheme proposed in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 ('the Bill'). Given the uncertainty about fundamental aspects of the scheme, the LIV agrees with the Law Council of Australia's ('LCA') policy position of opposing the currently proposed mandatory data retention scheme in the Bill. As the then LCA President, Mr Michael Colbran QC, has stated, there must be a proper analysis of the proposed provisions and:

> any mandatory data retention scheme must be shown by the Government to be reasonable, necessary and proportionate to a legitimate purpose.[1]

Preventing and enforcing serious crime is a legitimate purpose, however that does not of itself justify mass data retention. Even if the need for mass data retention could be demonstrated to be in the public interest, this Bill is profoundly flawed, as outlined in this submission.

This Bill is not limited to the stated objectives connected with making Australians safer from serious crime and threats to national security. Data retained under this Bill can be accessed for purposes far beyond serious crime.

The LIV is very concerned about the impact of the Bill on the fundamental human rights of all Australians, such as the rights to privacy, freedom of expression and freedom of association. Preserving these rights is essential to the functioning of a democratic society. The Bill fails to address these concerns.

In October 2014, a United Nations human rights expert concluded in a Report that mandatory data retention "amounts to a systematic interference with the right to respect for the privacy of communications", and therefore "it is incompatible with existing concepts of privacy for states to collect all communications or metadata all the time indiscriminately."[2]

In this context, it is submitted that the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') should recommend that:

- **The Bill not be passed**;
- There be a new Parliamentary Inquiry established to consider and consult on:
    - whether there is a need for mandatory data retention and if so, how this need can be translated into clear legislation that is reasonable, proportionate in not unduly restricting rights and freedoms and would be effective in meeting a legitimate purpose; and

[1] Law Council of Australia does not support mandatory data retention proposal, Law Council of Australia, 3 December 2014, available at: http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/mediaReleases/1429_--_Law_Council_of_Australia_does_not_support_mandatory_data_retention_proposal.pdf

[2] Online Mass Surveillance – protect the right to privacy even when countering terrorism – UN expert, Office for the High Commission of Human Rights, available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200&LangID=E

- a review of the *Telecommunication (Interception and Access) Act 1979* (Cth) ('TIA Act') and *Telecommunications Act 1997* (Cth) ('Telecommunications Act') as they relate to the law enforcement obligations of the communications industry and the related powers of law enforcement agencies.

In the event that the Committee does not agree with our primary position that the Bill not be passed, the LIV has made a number of recommendations concerning the Bill which may mitigate the Bill's infringements of fundamental human rights and freedoms.

RECOMMENDATIONS

Primary Recommendations:

- **The Bill not be passed**
- That there be a new parliamentary inquiry on the need for mandatory data retention and a review of the TIA Act and Telecommunications Act (as outlined above).

Secondary Recommendations:

1. **The data set must be defined in the primary legislation**
2. **Communications providers must not be required to create data**
3. **The agencies which can access telecommunications data must be exhaustively set out in the legislation**
4. **Access to telecommunications data must be restricted to criminal law enforcement agencies for preventing, detecting or prosecuting serious crimes**
5. **Access to telecommunications data must require judicial oversight**
6. **Specific protections for privileged and confidential information are needed**
7. **Data retention periods must be reduced to what is strictly necessary and proportionate**

UNANSWERED QUESTIONS

Below is a list of some of the questions and concerns that must be addressed before the PJCIS provides its report to Parliament. The PJCIS in its 2013 Inquiry into potential reforms of National Security Legislation stated that:

> A mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed.

It is concerning that this Bill has progressed to this Committee stage when so many fundamental legal, operational and technical questions and concerns remain unanswered. Substantially more time should be provided to enable the PJCIS to address these questions and concerns, fully consider the Bill and to undertake a holistic review of the TIA Act and related provisions in the Telecommunications Act.

What data will be retained?

- *What is the scope of the data set to be retained*?
- *What controls will there be over the scope of the data set as new technology emerges and other technology becomes less important?*

Is the retention of all this data "strictly necessary" for a legitimate purpose?

- *What is the legitimate purpose of the data retention scheme and how is the scheme limited to ensure the retained data is not used for purposes beyond this?*
- *Do the relevant agencies have the technical ability to both understand and keep secure the complex and voluminous internet-related data that would be retained under this scheme?*[3]
- *What evidence is there that the scheme is necessary and that the existing set of techniques and powers are not effective, including: intercepts, data preservation notices*[4] *and access to telecommunications data*?
- *What internet-related data is included in the draft data set but is not commonly requested by agencies now? What is the relevance of this data to enforce serious crimes or protect national security?*

[3] In Denmark, Online Tracking of Citizens is an Unwieldy Failure", 22 May 2013, available at: http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy
In 2013, a report produced by the Danish Ministry of Justice, highlighted that five years of extensive Internet surveillance have proven to be of almost no use to the police. The report mentions only two cases in which session logging proved useful to the police — and both were cases of financial crimes. Torben Olander reported: *"… the police and security services are drowning in a tsunami of user data that they cannot sort and therefore cannot use."*

[4] For information on data preservation notices see iiNet's Response to questions on notice, 11 August 2014, available at: http://www.iinet.net.au/about/mediacentre/papers-and-presentations/iinets-response-to-questions-on-notice.pdf

- *Why has two years been chosen as the retention period for subscriber data, telephony and internet-related data?*

How will the data be retained?

- *How will the so-called content and non-content of communications be separated or filtered by service providers in the course of meeting their data retention obligations? Or, in practical terms, will service providers simply retain the whole email, for example?*

- *How will the data be stored? Will the retained data be stored in de-centralised systems and databases across a service provider's operations?*

- *What systems will the service providers need to build in order to capture and then retrieve the data as it is requested?*

Who will have access to the data?

- *Will the data be available to the broad range of agencies that currently access telecommunicatons data including the breadth of security and police agencies, together with the likes of Centrelink, Department of Immigration, ATO, ASIC, RSPCA and local councils?*

- *Will the retained data be available to private individuals and other litigants through court processes such as subpoenas and discovery?*

What controls or limits will be on the access?

- *How will a service provider be able to determine whether a request for data might relate to a communication of a confidential nature, such as attracting legal professional privilege or a journalist's source?*

- *Are there any limits or constraints on how the agencies can use the retained data?*

What purposes could the data be used for other than the prevention or enforcement of serious criminal offences?

- *Will individuals be able to request a copy of all the data retained about them under the access provisions in the Privacy Act 1988 (Cth) or will some components of the data set not be considered "personal information"?*

- *Will service providers be permitted to use all of the elements of the retained data set for their own purposes?*

What are the safeguards to protect privacy and data security?

- *Has a privacy impact assessment been undertaken by the government in relation to this Bill?*

- *What will the privacy impact be on individuals if retained data can be accessed through compulsive court processes such as discovery and subpoenas?*

- *What requirements will be put in place to ensure the safe and timely destruction of retained data by service providers (after the end of the retention period) and by agencies after the purpose for which the data was requested has been satisfied?*

- *Will a service provider be restrained from outsourcing and/or offshoring the performance of its retention obligations?*

- *If service providers can store the data off-shore, how will the data be protected from being accessed by foreign governments, bad actors and others not authorised to access the data?*

- *How does the Bill address data security concerns and heightened risks such as identity theft?*

- *What disclosure regimes will be in place to report data breaches to affected consumers*?

- *How will this scheme and any data security breach impact on public confidence in law enforcement and security agencies?*

- *Will the public's attitude toward law enforcement and security agencies change given their data will be retained and be able to be accessed by these agencies?*

What are the costs to the community from this scheme?

- *How much will the scheme cost service providers? Who will pay these costs and in what proportions: service providers, the government (and therefore taxpayers), consumers*?

- *Could this scheme challenge the efficacy of critical and long-standing legal protections such as legal professional privilege?*

- *Is the scheme the least intrusive option from a privacy perspective?*

- *What assurances can the government provide that the scheme will be effective in meeting a legitimate purpose?*

- *When will the government be publishing its regulatory impact statement as required by its "Guide To Regulation"?*[5]

- *When will the government publish the information on which they based their decision to implement a data retention scheme?*

[5] Guide to Regulation, available at: http://www.cuttingredtape.gov.au/handbook/australian-government-guide-regulation

CONTEXT: LEGAL AND TECHNICAL

The way Australians use their phones, tablets, computers and other communications devices provides important and necessary context for understanding the data retention regime and its intrusion on rights and freedoms such as the right to privacy, freedom of association and freedom of expression.

The data retention scheme, as set out in this Bill, is inappropriate for our data hungry world. The data generated as a result of using the Internet and mobile telephone networks is very different in nature and volume than traditional fixed-line phone records. Internet-related data is far more complex, more voluminous and can be very revealing of an individual's personal information. From a privacy perspective, mobile telephony and mobile broadband will also provide detailed location information.

We know that Australians hunger for data is rapidly increasing. The Australian Communications and Media Authority's recent "Communications Report" revealed that Australians downloaded 1,034,959 terabytes of data in the June quarter 2014, a 53 per cent increase on the previous year.[6] The Communications Report also found that:[7]

- Australians are using more devices to connect to the internet, with nearly seven in ten of us (68 per cent) using three or more different devices.
- The number of fixed-line telephone connections continued to decline (by more than two per cent) to 9.19 million services, while more than half of 25 to 34-year-olds are now mobile only.
- 14.72 million Australians had access to the internet in their home at June 2014.
- At June 2014, there were 31.01 million mobile services in operation in Australia
- The number of VoIP users increased by six per cent to reach 4.87 million people.

The Bill would require telecommunications and internet service providers (service providers) to retain 'information of a kind prescribed by the regulations' and sets out very broad categories of the types of information that can be prescribed[8]. These categories of data are 'based closely' on the EU Data Retention Directive. This Directive was found to constitute an interference with fundamental human rights in a landmark judgment of the European Court of Justice in April last year[9] (this means there is currently no EU law mandating the mass retention of communications data). Digital Rights Ireland, who was one of the parties to this case, noted in July 2014:

> It is unprecedented in Europe for a law to be struck down so widely. Data retention has been rejected unanimously by every supreme court or constitutional court to consider it – at last count being held unconstitutional in Austria, Bulgaria, Cyprus, the Czech Republic, Germany, Romania, and Slovenia as well as by the European Court of Justice.[10]

---

[6] Australians hungry for everything the Internet has to offer, ACMA, 3 December 2014, available at http://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/australians-hungry-for-everything-the-internet-has-to-offer

[7] Australians hungry for everything the Internet has to offer, ACMA, 3 December 2014, available at http://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/australians-hungry-for-everything-the-internet-has-to-offer

[8] Proposed clause 187A

[9] Proposed data set, October 2014, available at: http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/ProposeddatasetOctober2014.pdf Decision of the Court of Justice of the European Union in Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärntner Landesregierung), 8 April 2014, available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[10] "Data retention held unconstitutional in Slovenia", 12 July 2014, available at http://www.digitalrights.ie/data-retention-slovenia-unconstitutional/ . See also The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy Available at: http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf

We must not lose sight of the impact of this Bill on all Australians. The European Court of Justice was especially concerned that mass data retention effectively introduced blanket surveillance and treated everyone's data the same*:*

> 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.[11]

The Bill is an inappropriate vehicle for such a serious change to our law. It is a mere framework or shell for a scheme with substantive and critical obligations and provisions left to regulations or declarations by the Minister. This approach has led to a scheme that is inconsistent with the rule of law. The Bill is far too uncertain for the service providers who are required to comply with the regime and the public in understanding the state of the law.

The data retention scheme also compounds significant problems with the current TIA Act in relation to access and disclosure of telecommunications data. A complete overhaul of the TIA Act is well overdue. The Bill must not be considered in isolation from the significant issues that plague the Act it is amending.[12]

It is also not the case that the work to be done in considering this Bill can be avoided by references to this Committee's 2013 report on national security legislation[13]. The previous consideration of data retention was done in a context where no draft legislation or clearly defined definition of the data to be retained was provided and some 40+ other proposals were being considered.

This Committee must engage in the necessary work of fully considering and hearing evidence on critical questions such as:

- who can access telecommunications data;
- for which offences or contraventions should agencies be able to access telecommunications data; and
- whether a warrant should be required to access telecommunications data.

The government must make the case that the data retention scheme set out in the Bill is necessary, proportionate, reasonable and likely to be effective in meeting legitimate objectives. The Office of the Victorian Privacy Commissioner has previously submitted that where the state seeks to encroach into privacy and other civil liberties through the exercise of intrusive powers, such powers should be:

- exercised for *legitimate* purposes and not for improper reasons;
- used only when *necessary* and not arbitrarily or without reasonable cause;
- carried out in a way *proportionate* to their need and not in a manner that is excessively intrusive or to an extent that is overly broad; and
- shown to be *effective* in achieving their legitimate aims, with appropriate transparency in reporting outcomes and periodic review to ensure ineffective practices are modified or ceased.[14]

The regularly cited claim that telecommunications data is used in almost every criminal investigation means that such data may be useful but it does not establish that a mandatory data retention scheme is necessary, proportionate, reasonable or likely to be effective[15].

---

[11] Decision of the Court of Justice of the European Union in Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärntner Landesregierung), 8 April 2014, available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[12] The LIV notes that there is a separate parliamentary committee reviewing the TIA Act. The detail of that report due to be tabled on 12 February 2015 should be fully considered as part of this Committee's deliberations.

[13] Report of the Inquiry into the Potential Reforms of Australia's National Security Legislation, PJCIS, 24 June 2013, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm

[14] Submissions received to the Inquiry into potential reforms of National Security Legislation Reforms, no 109, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

[15] Seem, for example, Attorney General Department's "data retention" webpages: http://www.ag.gov.au/dataretention

In Germany, (which has had no mandatory data retention laws after its scheme was found to be unconstitutional) a 2011 study found data retention had no impact on either the effectiveness of criminal investigations or the crime rate. Further, the study found:

> There is no evidence that countries using targeted investigation techniques clear less crime or suffer from more criminal acts than countries operating a blanket communications data retention scheme[16].

Similarly, in 2013, the Privacy and Civil Liberties Oversight Board found that there is little evidence that the metadata program has made the US safer.[17] In the UK, Open Rights Group has reported that a 2012 case used to justify data retention was not a communication data problem as alleged but a failure to properly investigate the murder. [18] In fact, it was suggested that the case showed that diligent and proactive use of targeted data preservation could both prevent and detect crime.

In the Australian context, the Office of the Victorian Privacy Commissioner has previously submitted that:

> Collecting the data of all Australians does not appear proportionate to the risk of terrorism, nor is it likely to be effective in stopping terrorist acts … Like any information system, would-be criminals and terrorists will either find a way around the technological limits (such as using a Virtual Private Network, encryption services, or an anonymity network such as Tor), or move communications to other non-electronic channels.[19]

Furthermore, individuals wanting to evade detection could use encrypted or secure messaging services, VPNs or off-shore communications providers. Or more simply, given how this Bill is drafted, such individuals could use over the top services such as Gmail, Facebook or Skype that are not covered by the scheme. They could also access the Internet via those providers that might not be covered by the retention obligations in the Bill such as a WiFi provider in an airport lounge, café, library or university.

[16] Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics, 19 February 2011, available at: http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

[17] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Privacy and Civil Liberties Oversight Board, 23 January 2014, available at: http://www.pclob.gov/ SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf

[18] Tales of the unexpected: The Communications Data Bill, Open Rights Group, 3 December 2012, available at: https://www.openrightsgroup.org/blog/2012/evidence-for-the-cdb

[19] Submissions received to the Inquiry into potential reforms of National Security Legislation Reforms, no 109, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

RECOMMENDATIONS

In the event that this Committee does not accept the LIV's recommendation that the Bill not be passed, we make the further recommendations as set out below.

What data is to be retained?

1. ***The data set must be defined in the primary legislation***

Mandatory data retention is not targeted surveillance. The data retention scheme set out in this Bill covers all individuals without any exception or differentiation. It will impact on all Australians; including people under no suspicion whatsoever. The Office of the Victorian Privacy Commissioner has previously asserted that mandatory data retention:

> …is characteristic of a police state. It is premised on the assumption that all citizens should be monitored. Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life.[20]

The government has released only a draft of the data set.

The joint submission from Communications Alliance and AMTA[21] to this Inquiry outlines a history of discussions with industry players on this contentious topic stretching back to March 2008. Given this long history, it is an indictment on the policy-making process that the public and this Committee is again being asked to consider a data retention scheme without the data set being finalised and other operational requirements being unclear. Such uncertainty has a flow-on effect on the effectiveness and ultimate value of this current committee process. It is inappropriate that the Committee and the public are being asked to consider this Bill without the scope of the data set being known.

Moreover, leaving such a critical component of the data retention scheme to be prescribed by regulations is an inappropriate delegation of power to the Executive, as was recognised by the Senate Standing Committee for the Scrutiny of Bills.[22]

How can the public understand the law's potential consequences when the reach of the law is unknown? This approach is inconsistent with the rule of law. Given the privacy-instrusive nature of this Bill, it is critical that the government is transparent about the type and nature of the data that would be retained by service providers.

Another difficulty of the data set being only defined in regulations, which are not yet finalised, is that the communications industry cannot be expected to reliably provide an estimate of the costs.

[20] Submissions received to the Inquiry into potential reforms of National Security Legislation Reforms, no 109, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

[21] Submissions received by the Committee, Submission no. 6, APH, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions

[22] Senate Standing Committee for the Scrutiny of Bills, Alert Digest No. 16 of 2014 26 November 2014, available at http://www.aph.gov.au/~/media/Committees/Senate/committee/scrutiny/alerts/2014/pdf/d16.pdf.

The relevance of the uncertainity as to the data is to be retained directly relates to what might be the eventual cost of this scheme on both industry and ultimately consumers and tax payers. . Ultimately, the government has advanced no information on which the Parliament may make a reasonable assessment of the likely costs.

In 2010, Digital Rights Ireland reported:
Several network operators said the need to invest in retention infrastructure had caused them to delay or abandon improvements to national networks.

Deutsche Telekom claimed it had spent €5.2 million on implementation of retention infrastructure and €3.7 million a year to facilitate about 13,000 call data requests and 6,500 internet data requests. Other operators said they had spent in excess of €4 million setting up systems for providing access to stored data.[23]

Understanding the exact scope of the data set to be retained is also central to the crucial analysis of whether the data retention scheme is reasonable, proportionate and strictly necessary to achieve a legitimate purpose.

Why is it necessary, for example, for service providers to retain the features and service descriptions of their account holders products and services? [24] This data would seem to include information like a customer changing their monthly broadband quota, whether they have call waiting activated, whether their phone plan allows free international calls or free texts to numbers from the same provider.

Beyond name, address and other contact details, how is all the very detailed subscriber information set out in category 1 of the draft data set relevant to law enforcement? Data such as billing information, status of the service and metrics of the service appears to have marginal relevance to the enforcement of serious crimes and protecting national security.

The Internet is not a telephone. The failure to distinguish between telephony and internet-related data exacerbates the problems with the data set. An IP address does not identify a person. The LIV is concerned about the preservation of the presumption of innocence in the context of use of source IP addresses.

The unclear and open-ended language used in the proposed data set means that the obligations which service providers are required to comply with are far too vaguely defined. Communications Alliance's submission sets out the practical consequence of such unclear language:

> The issue is that although AGD is willing to provide verbal reassurance at this stage about the reasonable intent of the language, there is a risk that, down the track and once the Bill is passed, open-ended language can be used by agencies to demand much more of CSPs in order to demonstrate compliance.[25]

The question of what data is to be retained must be fully considered and transparently debated. It is insufficient from the perspective of protecting fundamental rights and freedoms to add some form of oversight measures after the data has been captured, retained and accessed. As academic Paul Bernal has emphasised:

> it is the gathering of data that creates the chilling effect – impacting upon our freedom of speech, of assembly and association and so forth. This isn't just about privacy. [26]

---

[24] Draft data set category 5(c)
[25] Submissions received by the Committee, Submission no. 6, APH, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions
[26] DRIP: a shabby process for a shady law, Paul Bernal, 12 July 2014, available at: http://paulbernal.wordpress.com/2014/07/12/drip-a-shabby-process-for-a-shady-law/

The ongoing task of deciding where the balance between law enforcement purposes and rights of citizens must remain within Parliament; the scope of data to be included in any data retention scheme must not be capable of revision by the Executive without parliamentary scrutiny.

2. Providers must not be required to create data

On 12 January 2015, the Attorney-General stated that the data retention bill "requires telecommunications companies to retain information they have routinely kept but which they might not keep in future." [27]

This statement does not encapsulate the full scope and scale of the scheme. The Bill requires service providers to **create** and then retain data that falls within the data set, even if they have no business need to do so. This data creation obligation does not appear in the EU Data Retention Directive.

The requirement to create data also displaces the protection afforded by Australian Privacy Principle 3.2 which states that an entity must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities.[28]

In October 2014, iiNet submitted that the requirement to retain information necessary to identify the source of a communication would require a material extension of existing retention periods and in some instances the creation of data such as:

- Email and webmail access logs – including identifiers associated with emails sent and received (3.5 million non-spam emails per day)
- Connection history and bandwidth traffic consumption.[29]

The more data that is created, the more the scheme will cost and the greater intrusion on privacy and risk of data breach.

Who can access the data?

3. The agencies which can access telecommunications data must be exhaustively set out in the legislation

The Bill creates a new definition of 'criminal law enforcement agencies', which is defined with a list of agencies. The Bill also allows the Attorney General to declare by legislative instrument that an agency is a criminal law enforcement agency for the purposes of the TIA Act.[30]

The government can therefore expand the list of criminal law enforcement agencies that can access the retained data without parliamentary scrutiny. This is yet another example of an inappropriate delegation of power in this Bill.

[27] One more anti-terror tool, George Brandis, The Australian, 12 January 2015
[28] Australian Privacy Principles, OAIC, available at: http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles
[29] iiNet's response to Industry Consultation Paper – Telecommunications data retention – statement of requirements September 2014, 8 October 2014, available at: http://www.iinet.net.au/about/mediacentre/papers-and-presentations/industry-consultation-paper-data-retention.pdf
[30] See proposed clause 110A

Even more concerning is that the Bill leaves wide open the critical question of what authorities or bodies will be listed as an "enforcement agency" and therefore be able to access the retained data.[31]

This clause gives the Attorney-General the power to list by legislative instrument any authority or body with functions to enforce criminal law or administer a law imposing a pecuniary penalty or relating to the protection of the public revenue. These functions are incredibly broad and reflect the existing and problematic situation where an unknown number of diverse federal, state and even local government entities currently access telecommunications data.

In this context, it seems unlikely that the Bill will significantly limit the range of agencies permitted to access telecommunications data. ASIC has already publicly stated that it wants to be added to the list of agencies that can access retained data.[32] Other entities such as ATO, Centrelink and even local councils who are accustomed to having access to telecommunications data upon request will likely seek to have such access continue.

Again the Bill fails to adhere to the rule of law. How can the public foresee when and by which agency they might be subjected to surveillance?

It is Parliament who must determine which agencies will be able to gain access to telecommunications data. The service providers and the public should be able to easily determine which agencies can obtain access to telecommunications.

What controls or limits are there on access to the data?

4. Access to telecommunications data must be restricted to criminal law enforcement agencies for preventing, detecting or prosecuting serious crimes

The CJEU in its press release, discussing its ruling that the EU Data Retention Directive was not proportionate and constituted a wide-ranging and particularly serious interference with the fundamental rights at issue, relevantly highlighted that:

> the directive fails to lay down any objective criterion which would ensure that the competent national authorities have access to the data and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body. [33]

This Bill does not refer to 'serious crime'. There are no criteria which would ensure that data is only accessed or used for purposes of prevention, detecting or prosecuting serious crime or even matters that constitute criminal offences. The Bill goes beyond a legitimate purpose. The agencies that can be classified

[31] See proposed clause 176A
[32] ASIC to lobby govt for metadata access, IT News, 28 November 2014, available at: http://www.itnews.com.au/News/398334,asic-to-lobby-govt-for-metadata-access.aspx
[33] The Court of Justice declares the Data Retention Directive to be invalid, Press Release of the Court of Justice of the European Union, 8 April 2014, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

as “enforcement agencies” can access data related to their function of enforcing offences that impose pecuniary penalties and/or protect public revenue.

The legislative hurdles authorities or bodies need to overcome to be listed as an “enforcement agency” under the scheme and, if so listed, to gain access to the data, are minimal. There are simply a number of matters that the Minister must “have regard to” such as whether the authority or body is required to comply with the Australian Privacy Principles or comparable binding scheme.[34]

The Bill does not provide any substantive or procedural conditions to the access and use of the retained data by law enforcement agencies.

Furthermore, the Bill does not provide any constraints on access to the retained data by litigants using court processes such as discovery and subpoenas. The impact of this scheme on civil litigation processes, litigants and the cost to providers of responding to such requests has not been fully considered.

Access to telecommunications data under the TIA Act must be:

- limited to the more narrowly defined and listed criminal law enforcement agencies, rather than “enforcement agencies” more broadly; and
- only permitted where it is strictly necessary for the prevention, detection, investigation or prosecution of serious crimes.

5. Access to telecommunications data must require judicial oversight

The justification provided for why a warrant is not needed to access telecommunications data is that access to this data is less intrusive than other powers[35]. This reasoning is no longer valid.

The Internet generates very different data than a traditional fixed line telephone. Telecommunications data is not like the information written on an envelope. Such analogies, especially when used in relation to internet-related or mobile telephony data, can be very misleading. The impact on privacy from mass retention, access and analysis “metadata” can be seen from the examples below:

- Frank La Rue, UN Special Rapporteur: “When accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone”.[36]
- NSA General Counsel Stewart Baker has said, “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content”.[37]
- The EU Advocate General, Pedro Cruz Villalón argued the retention of such data: “may make it possible to create both a faithful and exhaustive map of a large portion of a person’s conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity”.[38]

---

[34] See proposed clause 110A

[35] See http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Frequentlyaskedquestions.aspx and the question “Why are warrants not required for access to metadata”.

[36] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations general Assembly, 17 April 2013, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[37] We kill people based on metadata, David Cole, New York Review of Books, 10 May 2014, available at: http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/

[38] Advocate General’s Opinion in Joined Cases C-293/12 Digital Rights Ireland and C0594/12 Seitlinger and Others, 12 December 2013, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/ cp130157en.pdf

In July 2014, the UN High Commissioner for Human Rights released her report on the right to privacy in the digital age. The report concluded that **mandatory third-party data retention is neither necessary nor proportionate:**

- It has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.[39]
- It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy.[40]
- Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of governments on private sector actors to retain data 'just in case' it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many states, where governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.[41]

The Parliamentary Joint Committee on Human Rights recommended that the Bill be amended to provide that access to retained data be granted only on the basis of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime on defined objective grounds.[42]

European experience shows that judicial oversight of access to telecommunications data is feasible, with a 2011 report identifying eleven countries with various levels of judicial oversight.[43]

The LIV recommends that there should be judicial oversight of access to telecommunications data. This requirement is not a disproportionate burden on law enforcement agencies given the intrusive nature of the power.

6. Specific protections for privileged and confidential information are needed

The Bill contains no safeguards to protect confidential and privileged information, such as communications subject to client legal privilege, health records and journalists' sources. The lack of such safeguards was one of the flaws highlighted by the CJEU in assessing the EU Data Retention Directive:

> … it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy. [44]

[39] UNHRC: Joint statement on privacy in the digital age, 12 September 2014, IFEX, available at: https://www.ifex.org/international/2014/09/12/privacy_digital_age/ Paragraph 19
[40] Paragraph 20
[41] Paragraph 26
[42] Parliamentary Joint Committee on Human Rights, Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011, Bills introduced 20 – 30 October 2014 (the PJCHR report), at [1.59]. See http://www.aph.gov.au/~/media/Committees/Senate/committee/humanrights_ctte/reports/2014/15_44/15th%20Report.pdf
[43] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 (the 2011 EU report) available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.

As illustrated above, telecommunications data is capable of revealing substantial information, and this could include information about communications between a lawyer and their client. For example, information exchanged by email or calls about potential witnesses between the lawyer and associates of the client, experts or other relevant parties, could disclose a defence case. A litigation strategy or case theory could be identified based on witnesses or experts contacted by the lawyer.

The Bill should contain specific safeguards to prevent disclosure of potentially privileged and confidential information. This issue could be taken into account as part of the warrant process and may in appropriate circumstances give an individual an opportunity to challenge access on the basis of privilege.

How long should the data be retained?

7. Data retention periods must be reduced to what is strictly necessary and proportionate

The Bill establishes a blanket two year retention period that applies to all categories of data.

Further information needs to be provided as to how this two year retention period is strictly necessary, reasonable and proportionate.

In the UK, a 2011 report revealed that, over a 4 year period, 74%+ of disclosures to law enforcement agencies, where the age of data being sought was known, related to data that was less than 3 months old. [45] In Australia, Communications Alliance revealed that "CSPs report that the vast majority of warrantless requests they receive from Australian agencies relate to data that is 6 months old or younger". [46]

The EU Data Retention Directive imposed a retention period of between 6 and 24 months. Only Poland chose the same two-year retention period as the government in this Bill.

The categories of data to be retained are closely based on the EU Data Retention Directive. However, the Bill fails to address the numerous flaws identified by the Court of Justice of the European Union when it invalidated the Directive as a fundamental interference of human rights. As the EU Parliament recently confirmed, this judgment means that any legislation requiring retention of communications data by a Member State of the EU should now comply with the principles set out in the judgment, which include:

- restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and/or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences;
- distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned;
- ensure retention periods are limited to that which is 'strictly necessary';
- restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes.[47]

---

[44] Decision of the Court of Justice of the European Union in Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärntner Landesregierung), 8 April 2014, available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[45] Evaluation report on the Data Retention Directive (Directive 2006/24/EC), European Commission, 18 April 2011, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

[46] Submissions received by the Committee, Submission no. 6, APH, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions

[47] Decision of the Court of Justice of the European Union in Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärntner Landesregierung), 8 April 2014, available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

Reducing the time the data is retained would also reduce the risk of data breaches and the extent to which privacy is compromised. This is critical as there are currently no meaningful safeguards in the Bill to protect the security of the data. The Office of the Victorian Privacy Commissioner in its 2012 submission emphasised that:

> Retaining the data would create a massive security risk if an ISP suffers a breach of security, including a significant risk of identity theft. The immense amount of data would also create an incentive for hackers to view ISPs as a target. Unlawful access of this data could cause extensive privacy concerns, given the data is likely to contain a wealth of personal information, including potential online financial transactions.[48]

Similarly, the Office of the Australian Information Commissioner (OAIC) suggested that consideration should be given to what steps could be taken to protect these large volumes of data given the risk of creating "a 'honey pot' of personal information that would be an attractive target for individuals with criminal or malicious intent".[49]

These risks are exacerbated by the lack of mandatory data breach notification laws.

The LIV recommends that the data retention period be reduced according to demonstrated need of each particular element of the data set for legitimate purposes. It is likely that more appropriate retention periods would be in the order of, for example, one year for telephony data and 6-months for internet-related data.

[48] Submissions received to the Inquiry into potential reforms of National Security Legislation Reforms, no 109, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm
[49] Submissions received to the Inquiry into potential reforms of National Security Legislation Reforms, no 183, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm

CONCLUSION

There are few, if any, meaningful safeguards in the Bill to uphold human rights and to protect against unlawful access and disclosure. The interference with human rights is arguably intensified in Australia, as we lack the strong human rights and data protection framework that exists in the EU.

The government has not demonstrated any urgency for passing this Bill, nor for the very short amount of time given for the public to make submissions to this Committee or for the Committee to provide their final report.

It is unclear why the passage of this data retention scheme is so urgent. A data retention scheme has been a matter for consideration by the Attorney-General's Department since at least 2008 and the proposal in this Bill itself will take at least 18 months to be implemented. This implementation period counters any suggestions that the recent devastating events in Sydney and Paris warrant urgent passage of the Bill.

In Australia, there are also significant existing powers under telecommunications legislation, together with a huge body of anti-terrorism law enacted since 2001, that empower our agencies to engage in a targeted approach to serious crime and counter-terrorism. As Paul Bernal has written:

> The fundamental problem is that terrorism, by its very nature, is hard to deal with. That's something we have to face up to – and not try to look for silver bullets. No amount of technology, no level of surveillance, will solve that fundamental problem. We shouldn't pretend that it can.[50]

The data retention scheme proposed in this Bill is invasive, likely to be very costly and threatens the right to privacy, freedoms of expression and speech and a free press. Moreover, the effectiveness of such schemes remains unproven.

[50] Paris damages the case for mass surveillance, Paul Bernal, 9 January 2015, available at: https://paulbernal.wordpress.com/2015/01/09/paris-damages-the-case-for-mass-surveillance/