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

Jaan Murphy and Monica Biddington
Law and Bills Digest Section

Note: this Bills Digest replaces an earlier version dated 24 March 2015.

Contents

The Bills Digest at a glance ...................................................... 7
Purpose of the Bill ................................................................. 8
Structure of the Bill ............................................................... 8
Background ............................................................................. 8
Definition of metadata .............................................................. 8
Debate about applicability of the definition to modern telecommunications ......................................................... 9
Rationale for affording metadata less privacy protection than content ............................................................... 11
Privacy implications ................................................................. 13
Risk to personal privacy presented by retained metadata .................................................................................. 13
Is retention of metadata necessary and proportionate? .... 15
  1) Mandatory metadata retention is not a necessary or proportionate response to terrorism and serious crime ................................................................. 16
  2) Mandatory metadata retention is a necessary or proportionate response to terrorism and serious crime 17
Appropriate retention period .................................................... 17
Table 1: Parliamentary committee views on appropriateness of a two-year retention period .......... 17
Oversight and scrutiny ............................................................. 19
Table 2: Parliamentary committee views on appropriateness of a metadata warrant regime ............. 19

Date introduced: 30 October 2014
House: House of Representatives
Portfolio: Attorney-General
Commencement: Sections 1 to 3, Schedule 1, items 8 to 11 on Royal Assent; Schedule 1, items 1 to 7, Schedules 2 and 3 — six months after Royal Assent.

Links: The links to the Bill, its Explanatory Memorandum and second reading speech can be found on the Bill’s home page, or through the Australian Parliament website.

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the ComLaw website.
Committee consideration ........................................... 20

Senate Standing Committee for the Scrutiny of Bills .......... 20
  Using regulations to specify the definition of the scope of data ................................................................. 20
  Using regulations to expand the category of services that will be subject to the data retention obligations .... 20
  Using regulations to expand the meaning of ‘criminal law enforcement’ and ‘enforcement’ agency .......... 21
  Other concerns ................................................................................................................................. 21

Parliamentary Joint Committee on Intelligence and Security ................................................................. 21
  Using regulations to define the scope of data that must be retained .......................................................... 21
  Using regulations to expand the category of services subject to data retention obligations ........................... 22
  Using regulations to expand the meaning of ‘criminal law enforcement’ and ‘enforcement’ agency .......... 22
  The length of time data is to be retained .................................................. 23
  The cost of the Scheme .................................................................................................................. 23

Access to retained metadata by civil litigants ................. 24

The application of the Privacy Act 1988 to all service providers covered by the Scheme ......................... 24

The application of the Scheme to ‘offshore’ and ‘over the top’ providers ............................................... 26

Evaluating the effectiveness of the Scheme .................... 27

Using retained metadata to identify journalists’ sources ... 27

Parliamentary Joint Committee on Human Rights ........... 28

The right to privacy ................................................................. 29
  The data set .............................................................................................................................. 29
  Retention period and use of retained metadata to investigate minor offences ........................................... 29
  Subsequent use of disclosed metadata for unrelated purposes ......................................................... 30

Warrants, oversight and accountability .................................. 31

Table 3: PJCHR recommendations in relation to pre-access oversight of metadata applications ................. 32

Table 4: PJCHR recommendations in relation to pre-access oversight of metadata applications ................. 34

Policy position of non-government parties/independents ... 35

Labor .................................................................................................................. 35

Greens ............................................................................................................. 35

Other Senators .......................................................................................... 35

Family First ............................................................................................... 35

Palmer United Party ................................................................................. 36
Senator Leyonhjelm ....................................................... 36
Senator Xenophon.......................................................... 36
Other Independent Senators........................................... 36

Position of major interest groups ................................. 37
Intelligence and law enforcement agencies...................... 37
ASIO ............................................................................... 37
Table 5:  Historical communications data –
comparative range of retention ........................................ 37
Table 6:  Ranges of retention by service providers of
historical communication data........................................... 38
Australian Federal Police................................................. 38
State and territory police forces ........................................ 39
Other government agencies............................................. 39
Attorney-General’s Department ........................................ 39
Issues related to accessing metadata associated with
sensitive or privileged communications.......................... 40
Application of the metadata retention obligations to
Wi-Fi service providers..................................................... 41
Application of the metadata retention obligations to
‘offshore’ service providers.............................................. 41
The retention period .......................................................... 41
Security of the retained metadata ..................................... 42
AHRC ............................................................................. 42
The data set ...................................................................... 42
The definition of ‘content’ .................................................. 42
Retention period ................................................................. 43
Access to retained metadata .............................................. 43
Office of the Australian Information Commissioner .......... 43
The proposed data set .......................................................... 43
Privacy impact of the Scheme ............................................ 44
Inadvertent collection of content ....................................... 44
Retention period ................................................................. 44
Services to be covered ......................................................... 45
Warrant regime options....................................................... 46
Limiting the use of metadata to serious criminal
offences ........................................................................... 46
Definition of enforcement agency ..................................... 47
Security of retained metadata .......................................... 47
Mandatory data breach notification ................................... 48
Providing individuals with access to their metadata .......... 48
Inspector-General of Intelligence and Security .................. 49
Data which will be accessible to ASIO ............................... 49
The length of time ASIO may retain data ......................... 49
Industry - Optus ................................................................. 49
Financial implications .................................................. 50

PJ CIS Report .................................................................. 50
Estimated cost as noted by the PJCIS ............................... 51
PJ CIS Recommendation .................................................. 52
Unresolved issue: on-going cost ..................................... 52

Does the Cybercrime Convention prevent metadata being used only in relation to serious offences? .................. 52

Data preservation versus data retention .......................... 53

Australia’s obligations under the Cybercrime Convention .................................................................................. 54

Limits on Australia’s obligations under the Cybercrime convention .................................................................... 54

Conclusion: restricting the disclosure or use of metadata to serious offences is permitted ................................. 54

Statement of Compatibility with Human Rights ............ 55

Key issues and provisions .............................................. 55

Schedule 1, Part 1: Data Retention ................................. 55

Obligation to retain metadata ....................................... 55
Definition of metadata to be retained ........................... 56

Subscriber, account, service and device information relating to the relevant service ....................................... 56

The source of a communication .................................. 56

The destination of a communication ............................ 57

The date, time and duration of a communication, or of its connection to a relevant service .............................. 57

The type of a communication or of a relevant service used in connection with a communication .................. 57

The location of equipment, or a line, used in connection with a communication ........................................... 57

Metadata definition declaration power ........................ 58

Service declaration power ............................................. 59

Application of the proposed scheme to ‘over the top’ services ......................................................................... 60

No requirement to retain content .................................. 60

Certain services exempted from metadata retention obligations ............................................................................ 60

Confidentiality of retained metadata ............................. 61

Application of the Privacy Act 1988 to retained metadata .................................................................................. 61

Proposed two-year retention period ............................... 62
Certain subscriber and account related information or documents........................................................................ 62
Other types of metadata........................................................................................................................................ 63
Data retention implementation plans..................................................................................................................... 63
Effect of data implementation plans.................................................................................................................... 63
Applying for data implementation plan approval................................................................................................ 63
Pre-approval consultation requirements................................................................................................................ 64
Considerations relevant to data implementation plan approval ................................................................................ 64
Duration of data implementation plans ................................................................................................................ 65
Penalties for failing to comply with a data implementation plan ........................................................................... 65
Effect of exemptions or variations to metadata retention and confidentiality obligations........................................ 65
Applying for exemptions or variations to metadata retention and confidentiality obligations.................................. 66
Considerations relevant to approving exemptions or variations............................................................................ 66
Approval and review ............................................................................................................................................... 66
Financial assistance to service providers ............................................................................................................... 67
Schedule 1, Part 2: other amendments .................................................................................................................... 67
ASIO Reporting requirements .................................................................................................................................. 67
Expanded role of the PJCIS ...................................................................................................................................... 68
New threshold for access to retained metadata ....................................................................................................... 68
Access to retained data in connection with civil litigation ..................................................................................... 68
Access to journalists’ metadata .............................................................................................................................. 68
PJCIS Report and position on accessing journalists metadata ............................................................................... 69
Current position in the United Kingdom .................................................................................................................. 69
Why are journalists special? ..................................................................................................................................... 69
Proposed journalist information warrant regime .................................................................................................... 70
Prohibition on accessing journalists metadata ...................................................................................................... 70
Lack of definition of a journalist............................................................................................................................. 70
ASIO JIWs................................................................................................................................................................. 70
Enforcement agency JIWs ......................................................................................................................................... 71
Role of the Public Interest Advocate ..................................................................................................................... 71
New offences related to JIWs ..................................................................................................................................... 72
Additional oversight and reporting of JIWs ................................................................................................................ 72
Schedule 2: Restricting access to stored communications and telecommunications data ................................................... 72
Definition of criminal-law-enforcement agency ..................................................................................................... 72
Ministerial power to declare criminal law-enforcement agencies ........................................................................ 73
Definition of law-enforcement agency ................................................................................................................... 74
Summary of criminal law enforcement and law enforcement agency declaration powers .................. 75

Schedule 3 - Oversight by the Commonwealth Ombudsman .......................................................... 75

Appendix : A .................................................................................................................................. 77

Table 7: PJCIS recommendations and amendments made to the Bill ................................................. 77
The Bills Digest at a glance

- The Bill creates new obligations on telecommunications and internet service providers (service providers) to retain prescribed information or documents (metadata) for a period of two years for the purposes of access by national security authorities, criminal law-enforcement agencies and enforcement agencies.
- The Bill also requires service providers to encrypt the retained metadata (subject to certain exemptions).
- The Bill outlines which enforcement agencies will have access to the information and documents available under the proposed Scheme.
- Schedule 3 outlines oversight of the scheme by the Commonwealth Ombudsman, a measure that has been criticised as inappropriate scrutiny post facto.
- A key concern at the time of consideration in detail is the lack of full costings and clarity surrounding the burden of the proposed Scheme on individuals, businesses and Government. Many submissions to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the Bill claim that it could be considered unconscionable for non-Government Parliamentarians to vote in favour of the Bill without understanding the financial impacts on the community.
- At the time of publication of the Digest, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) had provided its recommendations. Whilst the Government has indicated that it accepted all of the recommendations made by the PJCIS, the amended Bill as passed by the House of Representatives arguably does not give effect to all of them, as detailed in Table 7: PJCIS recommendations and amendments made to the Bill.
Purpose of the Bill
The purpose of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) is to amend the Telecommunications (Interception and Access) Act 1979 (the TIA Act) and the Telecommunications Act 1997 to, primarily, introduce a statutory obligation for telecommunications and internet service providers (service providers) to retain for two years types of metadata prescribed in the Bill (the proposed Scheme).

Structure of the Bill
The Bill is presented in three Schedules. Schedule 1 outlines the data collection, retention and confidentiality obligations for service providers. Schedule 2 outlines amendments relating to access by criminal law enforcement agencies to stored communications and metadata. Schedule 3 inserts new provisions into the TIA Act to facilitate the oversight of law enforcement agencies' records by the Commonwealth Ombudsman.

Background
The Bill follows the National Security Legislation Amendment Bill (No. 1) and Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 as the Government's third tranche of legislation in response to the current national security threat. While it is presented by the Government as a national security measure, data retention has broader reaching and immediate implications for all Australians who use the Internet and other modern telecommunications technologies.

The proposal to introduce a mandatory data retention scheme was previously explored in depth in the Parliamentary Joint Committee on Intelligence and Security (PJCIS) 2013 Report of the Inquiry into the Potential Reforms of Australia’s National Security Legislation (2013 PJCIS Report).

Definition of metadata
As the Bill deals with the collection, retention and confidentiality of telecommunications data (referred to as metadata throughout this Digest), its definition must be considered. This is because the definition of metadata provides the contextual background against which the existing metadata access provisions in the TIA Act and the new collection, retention and confidentiality obligations proposed by the Bill must be considered.

Assertions that the TIA Act does not contain a definition of metadata are incorrect. Whilst the TIA Act does not provide a specific, positive definition of metadata, it is negatively defined in sections 171 and 172. Section 171 makes it clear that metadata consists of information or document(s). Section 172 operates negatively, defining metadata as:

- information other than the ‘contents or substance of a communication’ or
- a document ‘to the extent’ that it ‘does not contain the contents or substance of a communication’.

1. See for example: Australian Government, Equipping Australia against emerging and evolving threats, AGD, Canberra, July 2012, accessed 26 August 2014, p. 25; Australian Government, Telecommunications (Interception and Access) Act 1979, Report for the year ending 30 June 2012, Canberra, July 2012, accessed 26 August 2014, p. 3: ‘Telecommunications data is not defined but can include information such as subscriber details and the date, time, and location of a communication. Telecommunications data does not include the content or substance of the communication’ and p. 10: ‘Telecommunications data is not defined in the TIA Act. It is also referred to as ‘metadata’, ‘communications data’ and ‘communications associated data’, and is generally understood as comprising information that allows a communication to occur, and information about the parties to the communication.’; C Ricci, ‘Metadata law equal mega change and confusion’, The Sydney Morning Herald, 18 August 2014, accessed 26 August 2014: ‘...because there is no definition for the term in Australian law, there is confusion about how metadata might be defined under the proposed legislation and what personal information it might encompass.’; B Grubb and J Massola, “What is ‘metadata’ and should you worry if yours is stored by law?”, The Sydney Morning Herald, 6 August 2014, accessed 26 August 2014: ‘Currently there is no definition of metadata under Australian telecommunications law.’

2. Section 171 provides (in part) that ‘Divisions 3, 4 and 4A set out some circumstances when sections 276, 277 and 278 of the Telecommunications Act 1997 do not prohibit a disclosure of information or a document’ (emphasis added) and also notes ‘Those Divisions do not permit the disclosure of the contents or substance of a communication’.

3. Telecommunications (Interception and Access) Act 1979 (Cth), section 172. This definition of metadata was summarised by the LCA as being: ‘...information about a telecommunication that does not include the content or substance of the communication.’ However, the LCA also noted that ‘This definition is workable only insofar as there is a clear distinction between the contents or substance of a communication and all other information about the communication’: Law Council of Australia (LCA), Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re: Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007 (provisions), July 2007, p. 15, accessed 24 March 2015.
Importantly ‘communication’ is defined in the TIA Act as including conversations and messages (or any part of a conversation or message), whether in the form of speech, data, text, or visual images (animated or otherwise). 4

In the context of web browsing, metadata is what remains of the communication or document (that is the text of a webpage or video) after its ‘contents’ or ‘substance’ is excluded. As a result, the legal definition of metadata is ambiguous (perhaps deliberately so). Nonetheless, commentators, including the Law Council of Australia (LCA) have suggested that the failure to include a positive definition of metadata in the TIA Act is a surprising omission:

It is assumed that one of the key aims of the exercise is to ensure that both the privacy rights of individuals and the powers of enforcement agencies are clearly understood. It seems unfortunate, and possibly counterproductive, in those circumstances not to properly define “telecommunications data”. 5 (emphasis added).

In part, the ambiguity surrounding the legal definition of metadata arises from conflicting views on what, from both technical and legal perspectives, constitutes ‘the content’ of a communication (discussed below under the heading ‘Debate about applicability of the definition to modern telecommunications’). 6 The Parliamentary Joint Committee on Human Rights (PJCHR) made a direct reference to this issue when it noted:

…without a clear definition of ‘content’ there is the potential that what constitutes ‘content’ could be interpreted restrictively so that the scope of data to be retained is broader than what is required to achieve the stated objective (that is, that the scope of the dataset may be disproportionate). 7

The PJCHR recommended that ‘the Bill be amended to include a non-exclusive definition of what type of data would constitute ‘content’ for the purposes of the scheme’. 8

In summary, the current legal definition of metadata is what is left in respect of information or a document, after the ‘contents and substance’ of the communication are removed. As noted below however, there are diverging views as to precisely what information does (or can) amount to the ‘content’ or ‘substance’ of a communication, and the PJCHR recommended that what type of data would constitute ‘content’ should be defined, at least for the purposes of the proposed Scheme.

However, whilst not providing a definition of metadata, by prescribing types of data that must be retained the Bill effectively provides a (non-exhaustive) list of types of data that meet the negative definition of metadata contained in the TIA Act.

Debate about applicability of the definition to modern telecommunications

Traditionally, metadata (legally and technically) is viewed as all the non-content information associated with a communication, including that which allows the communication to occur. 9 Put another way, metadata has been

5. LCA, Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007 [provisions], op. cit., p. 15. See also: S Rodrick, ‘Accessing Telecommunications Data for National Security and Law Enforcement Purposes’, Federal Law Review, 37(3), 2009, accessed 24 March 2015, p. 388: ‘One of the most controversial aspects of the scheme is definitional, namely, what constitutes ‘telecommunications data’. The problem is that, although the Chapter is headed ‘Access to telecommunications data’, that phrase is not otherwise used in the Chapter, nor is it defined. The omission is surprising, given that the entire Chapter is devoted to the circumstances in which such data can be lawfully disclosed or used for national security and law enforcement purposes.’
6. See: B Grubb and J Massola, ‘What is ‘metadata’ and should you worry if yours is stored by law?’, op. cit.; Australian Communications Consumer Action Network (ACCAN), ‘Hacking the grapevine’, ACCAN website, 15 July 2014, accessed 24 March 2015, which notes at p. 17 that defining metadata by reference to content and non-content information is a ‘…distinction which is becoming increasingly difficult to sustain.’ The report contains a useful discussion about the conflicting views about what constitutes metadata on pp. 17-20. See also: LCA, Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007 [provisions], op. cit. p. 15: ‘This definition is workable only insofar as there is a clear distinction between the contents or substance of a communication and all other information about the communication. The Law Council believes that such a distinction can not necessarily be drawn. For example, submissions on the Exposure Draft of the Bill revealed that there remains room for debate about whether the address of a webpage, which may reveal a great deal about the contents of the page, falls into the “substance and contents” or the residual “telecommunication data” category.’ (emphasis added).
8. Ibid., p. 50, para [1.183].
9. See for example section 172 of the Telecommunications (Interception and Access) Act 1979, which prohibits the disclosure of information that is ‘the contents or substance’ of a communication or documents that contain ‘the contents or substance’ of a communication; World Wide
viewed as all the information about (or which facilitates) a communication, other than the content of the communication itself.

This content/non-content distinction dates back to a time when telephone calls were the communications of interest to agencies. The content of a telephone call is the actual conversation. The non-content information, or metadata, includes the telephone numbers of the two people involved in the conversation, the time and duration of the call.\(^\text{10}\)

The content/non-content distinction was justified on the (now) questionable basis that the content of a communication is more personal than non-content, so access to it ought to be harder to get.\(^\text{11}\) Under the Australian legal regime, access to content usually requires a warrant, but there are fewer requirements for access to metadata.

The content/non-content distinction has survived its application to some communications methods that have since emerged, but it is not well adapted to others. A reason for this is that, for some kinds of communication, data is generated which does not appear to have the characteristics of content but which does, in fact, reveal much about the content of, or at the very least, the ‘substance of’ the communication it is associated with. For these, many advocate that either the content/non-content distinction is inapt, or that if it is to be maintained, such information should be considered content, and so subject to higher levels of protection.\(^\text{12}\) This issue is discussed below under the heading ‘Rationale for affording metadata less privacy protection than content’.

Taking email as an example, the content of the communication is the text of the email message itself and any attachments. The non-content information of the communication includes the email addresses of the sender and recipients of the email.\(^\text{13}\) But the transmission of an email generates other data too, like headers, which convey information about the communication, the status of which under the content/non-content taxonomy, is not clear (although it tends to be treated as content).

There is even more uncertainty about the status of information generated by web use. In both legal and technical circles, in relation to web use—including browsing and searching—there is debate about the types of data that are content and those that are not.\(^\text{14}\) It is generally agreed that the actual content that is displayed when a person visits a particular page on a website is the content of the communication. However, there is debate about the status of other data associated with web use because, as with email, some information associated with web use, whilst not obviously content, is capable of conveying a great deal about the nature of the web use. Many website addresses, for instance, convey clearly the nature of the content found there.\(^\text{15}\)

---

10. Replacement Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007, p. 6: ‘For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration.’

11. As noted by the OPCC: ‘...the distinction between a “communication” or “content” on one hand, and information generated by or about that communication or content, on the other, is not that clear’ and ‘...Depending on the context, it is sometimes difficult to set out a precise line dividing a communication from metadata.’; OPCC: ‘Metadata and Privacy, A Technical and Legal Overview’, op. cit., pp. 1 and 3 respectively.

12. LCA, Submission to the Senate Standing Committee on Legal and Constitutional Affairs Re Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007 [provisions], op. cit. p. 15: ‘This definition is workable only insofar as there is a clear distinction between the contents or substance of a communication and all other information about the communication. The Law Council believes that such a distinction cannot necessarily be drawn. For example, submissions on the Exposure Draft of the Bill revealed that there remains room for debate about whether the address of a webpage, which may reveal a great deal about the contents of the page, falls into the “substance and contents” category or the residual “telecommunication data” category.’ (emphasis added) and ACCAN, ‘Hacking the grapevine’, op. cit., which notes at p. 17 that defining metadata by reference to content and non-content information is a ‘...distinction which is becoming increasingly difficult to sustain.’ The report contains a useful discussion about the conflicting views about what constitutes metadata on pp. 17-20.

13. Replacement Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2007, p. 8: ‘For Internet based telecommunications, such as email... data includes the sender’s and recipient/s’ Internet Protocol (IP) addresses, the devices from which they were sent from or to, and the time and date at which it was sent. The information does not include content such as the subject line of an email, the message sent by email...’

14. iiNet, Submission to Senate Standing Committees on Legal and Constitutional Affairs, Inquiry into the Comprehensive review of Telecommunications (Interception and Access) Act 1979, n.d., accessed 24 March 2015, p. 4: ‘URL is both metadata (a delivery instruction) and is also content’.

15. For example, it has been noted that ‘some website addresses may have logins and passwords in the URL’: A Bendall & J Forté, ‘The privacy impacts of the proposed changes to Australia’s national security regime’, Privacy Law Bulletin, 9(2), November 2012, p. 15.
However, it should be noted that the Bill excludes web browsing histories from the metadata that must be collected, but does not prohibit them from being collected. The PJCIS noted that some major service providers are ‘currently developing and implementing the capability to collect and retain at least some web-browsing history for commercial purposes, unrelated to the proposed data retention scheme’. As a result, as long as what constitutes the ‘content’ or ‘substance’ of a communication remains undefined, a degree of ambiguity surrounding precisely what retained information and documents can be accessed without a warrant by national security, criminal law enforcement and enforcement agencies will remain.

**Rationale for affording metadata less privacy protection than content**

As noted earlier, warrantless access to metadata has traditionally been justified on the basis that because this data does not consist of ‘content’, it deserves less privacy protection. However, the notions that metadata:

- does not consist of (or can amount to) the content or substance of a communication or
- reveals less about a person’s life or activities than content

has come under serious scrutiny. The Office of the Privacy Commissioner of Canada (OPCC) concluded:

> ... the revelatory nature of metadata is increasingly bringing into question the view that such information is less worthy of privacy protection because it is to be distinguished from content information, and that such information is less sensitive as a result. It also brings into question the view that metadata is less worthy of privacy protection because it may already be publicly available to others in some form or another.

In addition, one US academic (in relation to mobile phone location information) noted:

> ... today, aggregated noncontent information about a user’s mobile phone account reveals information about actual habits and associations in ways that the content of any specific individual communication cannot.

These views have empirical support. Research demonstrates that when analysed, metadata can allow the creation of a revealing profile of a person’s life including medical conditions, political and religious views, friends and associations, to the point that some have argued ‘metadata absolutely tells you everything about somebody’s life’. Clearly, it is for this reason that national security and law enforcement agencies want to be able to access it and use it in their investigations.

The PJCHR and PJCIS both noted evidence suggests that metadata can allow ‘very precise conclusions’ about the private lives of persons whose data has been retained. A widely reported example provided by Electronic Frontiers Foundation of how telephone metadata can be used is reproduced below:

---

16. See the notes to proposed paragraphs 187A(4)(a) and (b).
19. See for example: See for example: Stilgherrian, *Think your data is anonymous? Ha*, Crikey, 27 October 2014, accessed 24 March 2015: ‘According to research by Yves-Alexandre de Montjoye and others, more than 50% of mobile phone users can be identified from just two randomly chosen location data points. With four points, the figure rises to 95%. Most people reveal vastly more than that through social media — either by stating their location directly, or giving it away indirectly by posting photos of what they see’; PJCIS, *Report: Inquiry into potential reforms of National Security Legislation*, op. cit., paras 5.71-5.9.
- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don’t know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don’t know what was discussed.
- They know you received a call from the local NRA office while it was having a campaign against gun legislation, and then called your senators and congressional representatives immediately after. But the content of those calls remains safe from government intrusion.
- They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood’s number later that day. But nobody knows what you spoke about.

Whilst the above example may appear alarming, it is worth noting that the Australian Security Intelligence Organisation (ASIO) and government agencies are only likely to link these calls together if you are the subject of an investigation. Despite this, it is clear that due to the:

- proliferation of different types of metadata
- changes in how people use telecommunications and Internet technology
- increased prevalence of GPS-enabled devices and
- application of sophisticated data analysis techniques to metadata

the traditional justification for affording metadata less privacy protection (in the form of warrantless access) than the contents of communications is questionable. Therefore the rationale for affording the mandatorily collected and retained metadata less privacy protection than ‘content’ is an issue that has, and that is likely to continue to be, discussed in any debate surrounding the proposed Scheme.

25. K Lachmayer & N Witzleb, ‘The challenge to privacy from ever increasing state surveillance: a comparative perspective’, University of New South Wales Law Journal, 37(2), 2014, pp. 748-783, accessed 24 March 2015, see 749-750, 774-775: ‘...the spectre of total surveillance no longer appears impossible because technology provides ever-expanding potential for data sharing, data matching and data meshing. Data processors can be public or private, and the state increasingly coopts private business into its surveillance agenda. Anyone with whom we communicate, or whose infrastructure we use, can be turned into a potential contributor to state surveillance. Information resulting from internet surveillance can be combined with personal information held by private enterprises, such as bank accounts, travel itineraries, social networks, or with data held in government repositories of tax, social security and other state-held information... Big data applications raise the prospect of mining information to predict future behaviour or psychological preferences of which a target person might not even be aware... The data collected by these networks is subject to exponential growth, as more information is gained, analytical tools are improving and the storage capacities are expanding. (emphasis added); B Arnold (Associate Professor, Law School, University of Canberra), Evidence to Senate Legal and Constitutional Affairs References Committee, Inquiry into the Comprehensive revision of the Telecommunications (Interception and Access) Act 1979, 21 July 2014, accessed 24 March 2015: ‘Look at what is now the very large literature about the joys, the importance, the wonders of big data—the sorts of things that government has been really enthusiastic about and that academics and businesses have been really enthusiastic about. Give me enough data, give me enough envelopes about you, and I have a pretty good idea of what you are up to or what you might be up to, and, by extension, the people around you. This is privacy-invasive. I question whether it is appropriate.’ (emphasis added); Stilgherrian, ‘Think your data is anonymous? Ha’, op. cit., generally.

26. See for example: Andrew Nikolic MP and Jason Clare MP (Members, PJCIS), Question during Parliamentary Joint Committee on Intelligence and Security, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2013, 17 December 2014, accessed 24 March 2015, p. 17 (Nikolic MP): ‘I will move on to my next question, which is about some of the criticisms around non-warranted access to metadata. Some see it as exceptional and troubling. Indeed, some of the public commentary in the submissions I have seen almost tries to invest in the metadata the same sort of privacy sensitivity as you would find in the content of some of the data that is produced. So I am wondering to what extent you consider non-warranted access to metadata exceptional. Where else in law enforcement do we already find non-warranted access to records and information which would reasonably attract similar sorts of privacy concerns?’; p. 18-19 (Clare MP): ‘We would obviously need to explore this area in a bit more detail. We have got submissions from the Law Council that recommend a warrant based process. We have got the recommendation of the Joint Parliamentary Committee on Human Rights that recommends a warrant based process. We have got a submission from the University of New South Wales that is recommending a ministerial warrant based process similar to the way processes work for the Attorney-General and ASIO at the moment. And then we have got the former head of ASIO suggesting there may be a generic warrant based process and that has been endorsed by the former National Security Legislation Monitor, Brett Walker. So I think this is deserved of some serious investigation and consideration and advice back to the committee about how this might work and how it may be different from the existing authorisation process, particularly given that in many of the other jurisdictions overseas where we have mandatory data retention there is some additional level of judicial approval or extra approval processes before the data is
Privacy implications

As noted above, the view that metadata should be afforded less privacy protection than ‘content’ because it does not consist of ‘content’ has attracted substantial criticism, much of it related to the privacy implications posed by the proposed Scheme. First, there is substantial debate about the nature of the metadata that is required to be retained by service providers and whether or not it amounts to ‘personal information’ and, if it does, the risks that unauthorised access to the retained metadata poses to individual’s privacy. Second, there is debate about whether retention of metadata is a necessary and proportionate response to the threats posed by terrorism and other serious crimes, as well as the appropriateness of warrantless access to metadata. These issues are examined below.

Risk to personal privacy presented by retained metadata

Whether metadata is ‘personal information’ as defined in the Privacy Act 1998 (information about an identified individual, or an individual who is reasonably identifiable) is a topic of on-going debate.27 However, in the context of the proposed Scheme, it would appear that the collected metadata would amount to personal information. This is the view adopted by the Australian Privacy Commissioner (Privacy Commissioner) who noted:

The Privacy Act defines personal information broadly, to include any information about an identified individual or an individual who is reasonably identifiable. Whether an individual is reasonably identifiable from particular information will depend on, among other things, what other information is held about the individual. This means that the types of information that will also be personal information for the purposes of the Privacy Act will not be limited to just subscriber information (such as an individual’s name, date of birth and address), but will include information that can be linked to the subscriber information.28 (emphasis added)

27. For example, in submissions filed as part of proceedings before the Office of the Australian Information Commissioner (OAIC) related to metadata Telstra stated that: ‘Telstra’s position is fundamentally that the so-called “metadata” that may be generated and stored on Telstra’s network… is not personal information for the purpose of the Privacy Act 1988 (Cth) because it is not information about an individual whose identity can be reasonably ascertained from that information.’ (emphasis added); Telstra, Letter to Office of the Australian Information Commissioner (OAIC), 15 August 2014, accessed 24 March 2015, p. 1. In contrast, the OPCC, in the context of the Canadian regime (which uses a similar definition of personal information), noted that: ‘Our Office has also considered that seemingly innocuous information, when viewed along with other available information, can be personal information and can sometimes provide a fairly accurate picture of one’s personal activities, views, opinions, and lifestyle. For example, an Internet Protocol (IP) address can be personal information if it can be associated with an identifiable individual, and can be quite revealing about an individual’s Internet-based activities. Indeed, as the OPCC’s report entitled What an IP Address Can Reveal About You highlights, an IP address linked with basic information about a subscriber of telecommunication services can reveal a person’s interests, their leanings, with whom they associate, and where they travel, among other things.’ (emphasis added); OPCC, ‘Metadata and Privacy, A Technical and Legal Overview’, op. cit., p. 7. See also: Stilgherrian, ‘Think your data is anonymous? Ha…’, op. cit.: ‘But as the research is demonstrating, individuals’ identity can be “reasonably ascertained” from all manner of data with ever-decreasing effort — perhaps not from one dataset, but certainly by cross-referencing it with others.’

The Privacy Commissioner concluded that the proposed Scheme ‘requires service providers to collect and retain a large volume of personal information’ which ‘has the potential to significantly impact on the privacy of individuals’. The issue about whether or not metadata is personal information for the purposes of the Privacy Act 1988 was resolved through amending the Bill to include proposed section 187LA, which provides that metadata retained for the purposes of the Scheme is personal information.

However, given that metadata can establish a detailed profile of a person’s life, the security of the metadata retained by services providers and the risks to individuals’ privacy posed by potential unauthorised access to it has attracted attention and debate. For example, Senator Zed Seselja in the Senate Legal and Constitutional Affairs Reference Committee inquiry into the Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979, noted that some submissions indicated that the mandatorily retained metadata ‘would create a honey pot’ of useful personal information for hackers to target. The same point was made by Telstra during the PJCIS Inquiry into the Bill:

If I were that way inclined as a hacker, you would go for that system, because it would give you the pot of gold as opposed to working your way through our multitude of systems today to try to extract some data. But your fundamental point is that, yes, we face this risk today—absolutely... And I know that because if I were in a foreign intelligence service wanting to hack Telstra’s network, this new proposed system would be where I would go. You would tell the computer; you compromise the account of the user that has access to the system to provide the answer to law enforcement and you type in the subscriber information and, presto, there is your answer. The alternative is you probably have to be on the network for months, if not years, studying how it is set up, because that is not available to people from outside Telstra, and figuring out how to do that to then answer the question, should that be your question. As you know, there would be some hackers out there who would like to know who has been calling who and where a phone has been in a certain period of time.

Likewise, the Victorian Commissioner for Privacy and Data Protection (VCPDP) noted that:

The most sophisticated businesses are not immune to cyber vandalism. A recent US-based study found that the organisations they canvassed were on average victims of 1.6 successful cyber attacks every week. Given the ‘honey-pot’ of data to be retained by service providers under the scheme it is not unreasonable to assume they will be the targets of more than their share of attacks.

The Australian Privacy Foundation also noted that:

... the attraction to hackers, or to insider miscreants, is increased by the aggregation of the personal data involved. In effect, the Bill has the potential to create ‘honeypots’ of personal data where little previously existed, or which would not otherwise be created, thereby facilitating computer crime.

The Office of the Australian Information Commissioner also expressed a similar sentiment:

... telecommunications data retained under the scheme is likely to be a target for people with malicious or criminal intent. In the event of a security breach resulting in unauthorised access to or disclosure of telecommunications data, affected individuals would face increased risks of identity theft, fraud, harassment or embarrassment. I
note that 46% of breaches in Australia during 2013 were attributable to malicious or criminal attacks, which were the most prevalent cause of data breaches. Further, I note that Australian service providers have experienced significant issues in handling and keeping personal information secure. Major telecommunications services providers that will be covered by the scheme are amongst the 20 entities most complained about to our office. This (emphasis added).

It is clear from the above that the risks to personal privacy posed by the retention of large amounts of metadata include identity theft, fraud, harassment and use of sensitive information to embarrass or even potentially blackmail individuals whose metadata is inappropriately accessed, obtained or released.

Therefore it is clear that security of the retained metadata (which will be classified as ‘personal information’ if the Bill is passed) will be an issue of ongoing concern. This has concern has been addressed in part by proposed sections 187BA (which deals with the encryption and confidentiality of retained metadata) and proposed section 187LA (which extends the operation of the Privacy Act 1988 to service providers).

However, in addition to the risks to individuals’ privacy posed by unauthorised access to (or use of) large amounts of retained metadata, the Bill also raises issues related to the level of intrusion into individuals’ personal affairs by the government, and in particular, the appropriateness of warrantless access to retained metadata, as discussed below.

Is retention of metadata necessary and proportionate?

Australia is a signatory to the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR). Article 17 of the ICCPR and Article 12 of the UDHR both provide that no-one shall be subjected to arbitrary or unlawful interference with their privacy or correspondence. This means that any interference with privacy must:

- be in accord with the provisions and objectives of the ICCPR and
- should be reasonable in the particular circumstances.

Reasonable in this context means that any limitation on the right to privacy must be both proportionate and necessary to achieve a legitimate objective, which in this case, is:

The protection of national security, public safety, addressing crime, and protecting the rights and freedoms of others by requiring the retention of a basic set of communications data required to support relevant investigations.

The Office of the United Nations High Commissioner for Human Rights recently summarised the proportionate and necessary requirements in the following terms:

[A] limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right ... must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary. (emphasis added).

34. Ibid., p. 10.
35. A Bendall & J Forté, ‘The privacy impacts of the proposed changes to Australia’s national security regime’, op. cit., p. 15; ‘The importance of the resulting data collected by such a scheme cannot be understated. 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 could cause extensive privacy concerns, given the data is likely to contain a wealth of personal information, including potential online financial transactions.’ (emphasis added).
The differing arguments as to whether mandatory metadata retention is a necessary and proportionate response to terrorism and serious crime are discussed below.

1) **Mandatory metadata retention is not a necessary or proportionate response to terrorism and serious crime**

In relation to metadata retention schemes the UN Human Rights Committee (UNHRC) noted:

> 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.39 (emphasis added).

As well as the UNHRC, the European Court of Justice of the European Union (ECJ) has also ruled that mandatory metadata retention is neither a necessary nor proportionate response to the threats of terrorism and other serious crimes. This has direct relevance to the proposed Scheme in Australia as the proposed data set states that the categories of metadata now included in the Bill are ‘based closely’ on the European Union Data Retention Directive (EU-DRD).40

The EU-DRD was declared invalid by ECJ in the **Digital Rights Ireland** case in April 2014 on the basis that it interfered in a ‘particularly serious’ manner with the rights to respect for private life provided by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter).41 Those rights resemble those provided by Article 17 of the ICCPR.42

The ECJ noted retention of metadata (what is being proposed by the Bill) and access to metadata (which is currently regulated by the **TIA Act**) both constituted an interference with the right to privacy. As noted by two legal academics:

> This is important as proponents of data retention have long argued that the mere retention of data should be regarded as a lesser type of interference and should therefore not enjoy the full protection provided for by Article 7.43


The ECJ case revolved around the proportionality of the interference with the EU Charter rights by the EU-DRD. The ECJ was of the view that because the EU-DRD:

- facilitated broad-brush and generalised measures that impacted on all citizens (rather than targeted and tailored measures that impacted on citizens who could contribute to the prevention, detection or prosecution of serious offences) and
- was a disproportionate response to fighting serious crime and terrorism
- it therefore breached certain EU Charter rights (which are partially replicated in the ICCPR).44

As the Australian Law Reform Commission (ALRC) noted in its recent report *Serious Invasions of Privacy in the Digital Era*, there was a view put by some submissions that legislation authorising the collection of metadata

39. ibid., [26].
41. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General (C-293/12 & C-594/12) [2014] [ECJ], (Digital Rights Ireland) at [37]: ‘It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is... wide-ranging, and it must be considered to be particularly serious.’
42. International Covenant on Civil and Political Rights (ICCPR), opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976)Article 17: ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. . . . Everyone has the right to the protection of the law against such interference or attacks’ compared to EU Charter Article 7: ‘Everyone has the right to respect for his or her private and family life, home and communications’.
44. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, op. cit., at [37], [39] and [64].
breaches Australia’s human rights obligations. Similar concerns were expressed by the PJCHR (explicitly referencing the ECJ’s reasoning).

Because Australia is a signatory to the ICCPR and UDHR, both of which provide similar rights to privacy, the issues dealt with by the ECJ above are relevant to future attempts to provide a legislative definition of metadata (absent from the 2014 Bill), as well as determining the appropriateness of the proposed Scheme itself, and hence is compatibility the right to privacy.

2) Mandatory metadata retention is a necessary or proportionate response to terrorism and serious crime

Importantly however, the view that Digital Rights Ireland should be interpreted as standing for the proposition that mandatory metadata automatically breaches the right to privacy provided by the ICCPR and UDHR is not universal.

For example, the Attorney-General’s Department has stated that in its view ‘the Court’s judgment was based on the lack of appropriate safeguards and limits within the Directive itself’ rather than finding data retention per se was inherently incompatible with the right to privacy. The Attorney-General’s Department noted that on its reading of the case, the EU-DRD was declared invalid because it:

- ‘cover[ed], in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception’
- ‘fail[ed] to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions’
- ‘require[d] that those data be retained for a period of at least six months, without any distinction being made between the categories of data... on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned’
- ‘[did] not provide for sufficient safeguards... to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data’, and
- ‘[did] not require the data in question to be retained within the European Union’.

The Attorney-General’s Department then notes that in its view the ‘Bill has been drafted to ensure that it addresses each of the bases for the Court of Justice’s decision.’ This view is shared by the Government.

Appropriate retention period

One of the main issues raised by the proposed Scheme is the appropriate length of time metadata should be retained. This was an issue that the Senate Scrutiny of Bills Committee, PJCHR and PJCIS all examined closely. The issue is explored in detail below. However, the following table outlines their positions on the appropriateness of a two-year retention period.

Table 1: Parliamentary committee views on appropriateness of a two-year retention period

<table>
<thead>
<tr>
<th>Committee</th>
<th>Position on retention period</th>
</tr>
</thead>
</table>

47. Article 17 of the ICCPR, as noted by the PJCHR: ‘...prohibits arbitrary or unlawful interferences with an individual’s privacy, family, correspondence or home. However, this right may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, they must seek to achieve a legitimate objective and be reasonable, necessary and proportionate to achieving that objective’: PJCHR, Fifteenth Report of the 44th Parliament, op. cit., p. 11. This right is similar to that provided by the EU Charter (albeit using different terminology). Unlike the EU Charter, the ICCPR does not provide rights in relation to personal data: ICCPR, op. cit., Article 17.
49. Ibid.
50. Ibid., p. 40.
<table>
<thead>
<tr>
<th>Committee</th>
<th>Position on retention period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senate Scrutiny of Bills Committee</td>
<td>The committee noted the comments the PJCHR made about the Bill. In particular the committee noted the following comments by the PJCHR: ‘The PJCHR has sought advice from the Attorney-General as to whether the two year retention period is necessary and proportionate in pursuit of a legitimate objective.’</td>
</tr>
<tr>
<td>Parliamentary Joint Committee on Human Rights</td>
<td>The two year data retention period appears broader than is strictly required to achieve its stated objectives. That is, the scheme is not a proportionate way to achieve its ends, as is required under international law to justify a limitation of human rights.</td>
</tr>
<tr>
<td>Parliamentary Joint Committee on Intelligence and Security</td>
<td>The proposed two-year retention period is appropriate and should be maintained.</td>
</tr>
</tbody>
</table>

Sources: as per footnotes.

It is clear from the above that there are differing views as to the appropriateness of the proposed two-year retention period and what changes, if any, are required to ensure that it does not impose a more disproportionate limitation on the right to privacy than is required to achieve its objective. It is worth noting that the PJCHR stated that:

> ... the two year data retention period may be necessary for investigations of complex or serious crimes. However, the committee considers that the case has not been made as to the proportionality of the two year mandatory data retention period in relation to less serious crimes.

As a way of avoiding the disproportionate limitation on the right to privacy that would result from a two year retention period and allowing metadata to be used in the investigation of any offence, the PJCHR therefore recommended the Bill be amended to limit disclosure authorisation for existing metadata to instances where:

- it is reasonably necessary
- for the investigation of specified serious crimes, categories of serious crimes or the investigation of certain serious matters by key non-traditional criminal law enforcement agencies.

The PJCIS made a similar, albeit less direct recommendation when it recommended that the Bill be amended to require that an officer authorising access to metadata must be ‘satisfied on reasonable grounds’ that any interference with the privacy of any person or persons that may result from the disclosure or use of the metadata is justifiable and proportionate. Further, in reaching such a decision the authorised officer ‘should be required to have regard to... the gravity of the conduct being investigated, including whether the investigation relates to a serious criminal offence’.

Importantly however, unlike the PJCHR, the PJCIS did not specifically link that recommendation to the appropriateness of the two-year retention period.

On balance, it would appear that the PJCIS is correct when it notes that ‘a two-year retention period would place Australia at the upper end of retention periods adopted in other jurisdictions’. As a result, the PJCHR’s
recommendation that the Bill be amended to restrict access to metadata to instances where it is reasonably necessary for the investigation of categories of serious crimes and serious matters to ensure the proportionality of the two-year retention period, despite concerns about the impact of such a restriction on Australia’s obligations under the Council of Europe Cybercrime Convention (discussed below) is both a reasonable and practicable solution to the issue of the proportionality of the proposed the two-year retention period.60

Oversight and scrutiny
Another major issue raised by the Bill is the appropriateness of the existing post-access oversight mechanisms in the TIA Act and the appropriateness (and practicality) of introducing independent pre-access oversight or accountability mechanisms (such as a warrant regime). This was an issue that the Senate Scrutiny of Bills Committee, PJCHR and PJCIS all examined closely. The issue is explored in detail below. However, the following table outlines their positions on the appropriateness of oversight mechanisms.

Table 2: Parliamentary committee views on appropriateness of a metadata warrant regime

<table>
<thead>
<tr>
<th>Committee</th>
<th>Position on retention period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senate Scrutiny of Bills Committee</td>
<td>The committee noted the comments the PJCHR made about the Bill. In particular the committee noted the following comments by the PJCHR: ‘the PJCHR noted that the proposed oversight mechanisms in the bill are directed at reviewing access powers after they have been exercised... [t]he PJCHR therefore 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.’61</td>
</tr>
<tr>
<td>Parliamentary Joint Committee on Human Rights</td>
<td>The Committee stated that ‘requirements for prior review would more effectively ensure that the grant of access to metadata under the scheme would be consistent with the right to privacy... so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior review, the bill [should] 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 and defined objective grounds’ 62</td>
</tr>
<tr>
<td>Parliamentary Joint Committee on Intelligence and Security</td>
<td>The Committee acknowledged ‘that in some circumstances access to telecommunications data can represent a significant privacy intrusion.’ However, it noted that ‘the evidence provided that telecommunications data and telecommunications content are not used in the same way by law enforcement and security agencies, and does not consider that the same authorisation processes must necessarily apply’ and therefore concluded that ‘the existing internal authorisation regime contained in the TIA Act is appropriate, noting the other safeguards and oversight mechanisms that apply.’63</td>
</tr>
</tbody>
</table>

Sources: as per footnotes.

As with the appropriateness of the two-year retention period for metadata, it is clear that there are differing views as to whether a warrant should be required to access metadata and if the current post-access oversight and accountability mechanisms are adequate.

60. PJCHR, Twentieth Report of the 44th Parliament, op. cit., p. 54, para [1.190].
Committee consideration

Senate Standing Committee for the Scrutiny of Bills

In its Alert Digest of 26 November 2014 and First Report of 2015, the Senate Standing Committee for the Scrutiny of Bills (Scrutiny Committee) made extensive comments on the Bill. One of its key concerns was the inappropriate delegation of legislative power through the use of regulations to:

- specify the definition of the scope of data
- expand the category of services that will be subject to the data retention obligations
- expand the meaning of ‘criminal law enforcement agency’ and ‘enforcement agency’.

These concerns are examined in detail under the heading ‘Key issues and provisions’ below. However, they have since been addressed by amendments made to the Bill.

Using regulations to specify the definition of the scope of data

The Scrutiny Committee, after examining the arguments for and against placing the specific types of metadata to be retained into regulations, and considering the level of privacy intrusion involved, concluded that it was not ‘an appropriate delegation of legislative power’. Further, after considering the Attorney-General’s Response to its concerns raised in its Alert Digest of 26 November 2014, the Scrutiny Committee stated:

… the committee considers that this ‘data set’ is a core element of the proposed scheme and therefore reiterates its conclusion that the types of data to be retained should be set out in the primary legislation to allow full Parliamentary scrutiny.

The committee therefore considered that the Bill, as originally drafted, inappropriately delegated legislative power to the Executive Branch of the government in respect of the types of data that services will be required to collect and retain. As the Bill has since been amended (see discussion below under the heading ‘Metadata definition declaration power’), it would appear that this concern has been ameliorated.

Using regulations to expand the category of services that will be subject to the data retention obligations

The Scrutiny Committee noted that the Bill as drafted allowed the expansion of types of services that will be required to collect and retain metadata under the proposed Scheme via regulations. Although the Scrutiny Committee noted that regulation-making powers are, in some cases, properly justified by allowing a level of flexibility in response to changing circumstances it noted:

… how this scheme—which is highly intrusive of individual privacy—should be applied in a new technological context is a matter which will raise significant questions of policy that are not appropriately delegated by the Parliament to the executive government.

After considering the Attorney-General’s Response to its concerns raised in its Alert Digest of 26 November 2014, the Scrutiny Committee noted that, in its view, the range of services required to collect and retain metadata ‘is a core element of the proposed scheme’. It concluded that:

… the types of service providers subject to the data retention obligations should be set out in the primary legislation to allow full Parliamentary scrutiny.

64. Senate Scrutiny of Bills Committee, Alert Digest No. 16 of 2014, op. cit., p. 3.
65. Ibid., p. 4.
66. Ibid., p. 5.
67. Ibid., p. 3.
69. Ibid., p. 118, Senate Scrutiny of Bills Committee, Alert Digest No. 16 of 2014, op. cit., p. 3.
70. Senate Scrutiny of Bills Committee, Alert Digest No. 16 of 2014, op. cit., p. 4.
71. Ibid.
72. Senate Scrutiny of Bills Committee, First Report of 2015, op. cit., p. 120.
For the above reasons, the committee considered that the Bill, as originally drafted, inappropriately delegated legislative power in respect of the types of services that will be required to collect and retain metadata. As the Bill has since been amended (see discussion below under the heading ‘Service declaration power’), it would appear that this concern has been ameliorated.

Using regulations to expand the meaning of ‘criminal law enforcement’ and ‘enforcement’ agency
The Scrutiny Committee noted that the Bill, as drafted, allowed the use of regulations to expand the number of agencies that will be able to access retained metadata by allowing the Minister to declare, by legislative instrument, agencies not listed in the Bill as ‘criminal enforcement’ or ‘enforcement’ agencies. The Scrutiny Committee noted that ‘given the highly intrusive nature of the scheme’, in its view, any expansion of the number of agencies that can access metadata ‘should be determined by Parliament’ and not by the Executive branch of the government through the a legislative instrument.

As the Bill has since been amended (see discussion below under the heading ‘Ministerial power to declare criminal law-enforcement agencies’), it would appear that this concern has been, at least in part, ameliorated.

Other concerns
In addition to the above concerns, the Scrutiny Committee also noted its concerns in relation to the lack of a definition of ‘content’ in the Bill, the extent of interference with personal rights and liberties posed by the proposed Scheme, as well as the proposed accountability and oversight mechanisms. These concerns are examined in detail under the heading ‘Key issues and provisions’ below.

Parliamentary Joint Committee on Intelligence and Security
The Bill was referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry. The PJCIS handed down its report on 27 February 2015. Details of the inquiry and the report are here.

At over 300 pages, the PJCIS report provides extensive analysis of, and commentary on, the Bill and the proposed Scheme generally. Some of the key concerns raised by the PJCIS about the Bill (reflected in its recommendations) include:

• the appropriateness of using regulations to:
  – specify the definition of the scope of data that must be retained
  – expand the category of services that will be subject to the data retention obligations and
  – expand the number of ‘criminal law enforcement’ and ‘enforcement’ agencies that can access the retained metadata
• the length of time metadata is to be retained
• the cost of the Scheme
• access to (and use of) retained metadata by civil litigants
• the application of the Privacy Act 1988 to all service providers covered by the Scheme
• the application of the Scheme to ‘offshore’ and ‘over the top’ providers
• ensuring the effectiveness of the Scheme is evaluated and
• using retained metadata to identify journalist’s sources.

A brief summary of the PJCIS’s concerns in relation to the above is provided below.

Using regulations to define the scope of data that must be retained
The PJCIS noted that it had received ‘a number’ of submissions and heard evidence ‘recommending that the data set be set out in the Bill, rather than in regulations’ and that the Scrutiny Committee had likewise recommended that the types of data to be retained should be set out in the primary legislation.
In relation to the argument that it is desirable or necessary to keep key definitions related to the data-set technology-neutral as a way of preventing obsolescence, the Committee stated it did not ‘see a situation where emergency changes to the data set may be required.’

Hence, after weighing the arguments for and against placing the specific types of metadata to be retained into regulations, the PJCIS concluded that as the data set is ‘central to the operation of the proposed data retention regime’ that the proposed data set ‘should be set out in primary legislation’ (reflected in recommendation 2).

However, the PJCIS did note that ‘given the dynamic environment of developing technologies’ it had considered the merits of including an emergency data set declaration power (reflected in recommendation 3).

As the Bill has since been amended (see discussion below under the heading ‘Metadata definition declaration power’), it would appear that this concern has been ameliorated.

**Using regulations to expand the category of services subject to data retention obligations**

The PJCIS noted that the Bill would create a regulation-making power that would allow additional kinds of service providers to be prescribed (and hence required to collect and retain metadata under the proposed Scheme). The PJCIS noted the concerns expressed by the Scrutiny Committee and concluded that expanding the application of the proposed data retention scheme to ‘new classes of service providers’ via regulations raised ‘significant questions of policy that would be more appropriately considered by the Parliament’. However, the PJCIS acknowledged that:

> … rapid changes in technology may require data retention obligations to be applied to a different range of service providers, potentially in response to emergency circumstances.

For the above reasons, the PJCIS recommended that the Bill be amended so that whilst the Attorney-General can still declare additional classes of services providers (thus providing a degree of flexibility to deal with rapidly changing technology or emergency situations), the following conditions would apply:

- the declaration would cease to have effect after 40 sitting days of either House of Parliament
- an amendment to include the class of service provider in legislation should be brought before the Parliament before the expiry of the 40 sitting days and
- any such amendment should be referred to the PJCIS with a minimum of 15 sitting days for review and report.

As the Bill has since been amended (see discussion below under the heading ‘Service declaration power’), it would appear that this concern has been ameliorated.

**Using regulations to expand the meaning of ‘criminal law enforcement’ and ‘enforcement’ agency**

The PJCIS noted that a number of submissions had raised concerns about the ‘Attorney-General’s broad discretion to declare an agency as a criminal law enforcement agency, including agencies which may not have functions in respect of serious contraventions.’ The PJCIS noted that:

- whilst it is appropriate for criminal law-enforcement agencies to be listed in the primary legislation
- there may be ‘emergency circumstances’ where a rapid response is required, and
- hence there is ‘merit in the Attorney-General being able to declare an agency as a criminal law-enforcement agency in such circumstances’.

---

76. Ibid., p. 79, para [3.30].
77. Ibid., p. 79, paras [3.28-3.29].
78. Ibid., p. 79, para [3.30] and p. 80, recommendation 3.
79. Ibid., p. 162 para [5.38].
80. Ibid., pp. 162-162, para [5.40].
81. Ibid., p. 163, para [5.42].
82. Ibid.
83. Ibid., recommendation 14.
84. Ibid., p. 192, para [6.27].
However, the PJCIS stated that such emergency declarations ‘should only be made in regard to agencies whose functions include investigating serious contraventions’, and hence should be limited to agencies investigating serious contraventions as defined in section 5E of the TIA Act. Further, the PJCIS recommended that:

- criminal law-enforcement agencies (those that can obtain stored communications warrants) be specifically listed in the TIA Act but
- the Bill be amended to provide an emergency declaration power subject to appropriate constraints.

The PJCIS noted that any such emergency declaration ‘should only be in effect for 40 sittings days of either House of the Parliament’ as this would provide enough time to enable any proposed legislative amendment listing an agency as a criminal law enforcement agency to brought before the Parliament and the PJCIS for review. As the Bill has since been amended (see discussion below under the heading ‘Ministerial power to declare criminal law-enforcement agencies’), it would appear that this concern has been ameliorated.

The length of time data is to be retained

One of the most controversial aspects of the proposed Scheme is the length of time metadata is to be retained. The PJCIS examined the issue in detail, noting that the ‘length of time for which telecommunications data is retained has direct implications for both the necessity and the proportionality of the scheme’.

In particular the PJCIS noted that:

... longer retention periods may aid particular investigations. However, the effective conduct of serious national security and criminal investigations must be balanced against the degree to which a two-year retention period could interfere with the privacy, freedom of expression and other rights of ordinary Australians.

In relation to the appropriateness of a two-year retention period, the PJCIS made the following key points:

- intelligence and law enforcement agencies consider a two year retention period the minimum amount of time that is acceptable from a national security and law enforcement perspective
- evidence demonstrates that between 10 and 15 per cent of authorisations for access to metadata made by Australian agencies are for metadata more than a year old. However, such requests disproportionately relate to investigations into serious and complex criminal activity and matters of national security
- a two-year retention is at the upper end of metadata retention periods adopted in other jurisdictions.

As a result of the above, the PJCIS recommended that the proposed two-year retention period be maintained.

The cost of the Scheme

The PJCIS noted that a number of submissions and witnesses had raised the potential cost of relevant service providers complying with the proposed Scheme as an issue of concern. In particular the PJCIS noted that it:

... has heard significant concerns about the potential cost-impact of mandatory data retention, particularly in relation to small and medium-sized ISPs, which may not have the financial wherewithal to fund any significant capital expenditure.
This issue is discussed in detail under the heading ‘Financial implications’ below.

**Access to retained metadata by civil litigants**

The PJCIS noted that during the Inquiry into the Bill, a number of submissions raised concerns that mandatorily retained metadata will be able to be accessed for civil litigation or other purposes not related to law enforcement, such as enforcing copyright, divorce proceedings, commercial disputes and defamation proceedings. The PJCIS also noted the concern (and support for) the prospect of agencies excluded from the TIA metadata access regime resorting to using other statutory powers to access mandatorily retained metadata in civil regulatory investigations and proceedings.

Whilst such concerns may appear alarmist, they have a legitimate basis. The current metadata access Scheme created by the TIA Act and the *Telecommunications Act 1997* does not restrict access to metadata solely to ASIO and enforcement agencies. Rather, metadata may be lawfully disclosed by relevant carriers and service providers in a number of specific circumstances set out in the *Telecommunications Act 1997*. Importantly, this includes disclosure where ‘required or authorised by or under law’ and by witnesses summoned to give evidence or produce documents. As a result, currently it is possible for both civil litigants and government agencies with coercive investigatory powers to access metadata.

After considering the arguments for and against allowing mandatorily retained metadata to be used in civil proceedings, the PJCIS noted it ‘holds concerns’ about the prospect of the increasing use of metadata in civil litigation arising from the implementation of the proposed Scheme and ‘has paid careful heed to suggestions that such access be restricted’. The PJCIS also noted that as the proposed Scheme is being specifically established for law enforcement and national security purposes, ‘as a general principle it would be inappropriate for the data retained’ to be used ‘as a new source of evidence in civil disputes’. Therefore it recommended that:

- the Bill should be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime, and
- the amendment should include a regulation making power to enable provision for appropriate exclusions, such as family law proceedings relating to violence or international child abduction cases, but
- the prohibition should not apply to other forms of metadata retained by relevant service providers for purposes other than complying with the proposed Scheme.

As the Bill has since been amended (see discussion below under the heading ‘Access to retained data in connection with civil litigation’), it would appear that this concern has been, at least in part, ameliorated.

**The application of the Privacy Act 1988 to all service providers covered by the Scheme**

The PJCIS expressed the view that appropriate privacy protections and mechanisms to ensure the security of mandatorily retained metadata are ‘essential to the integrity’ of the proposed Scheme. As noted earlier, whilst subject to an on-going debate, it would appear that, notwithstanding proposed section 187LA, the mandatorily retained metadata would amount to personal information, and thus the potential application of the *Privacy Act 1988* in relation to the retained metadata must be considered.

The PJCIS noted that the Australian Privacy Principles (APPs), which dictate the standards, rights and obligations for the handling, holding, accessing and correction of personal information, generally apply to Australian government agencies, private sector organisations with:

- an annual turnover of $3 million or more, and

---

101. Ibid., para [6.115].
103. Ibid., p. 282, para [7.74].
• some private sector organisations, such as health providers, with an annual turnover of less than $3 million.  

The PJCIS noted the Australian Government Solicitor’s advice that, as a result of the above, ‘a threshold consideration is whether the service providers to which the new regime will apply are entities which are required to comply with the Privacy Act’ and that therefore:

... there are a small number of service providers that may be a small business operator within the meaning of s 6D of the Privacy Act, and for that reason may not be required to comply with the Privacy Act.

The PJCIS concluded that it was ‘important to recognise, however, that not all providers are APP entities’ and therefore it is ‘appropriate to require all providers to be subject to either the Australian Privacy Principles or binding rules of the Australian Privacy Commissioner’, especially given that there are precedents for requiring small businesses to comply with the APPs. Proposed section 187LA addresses this issue, as discussed under the heading ‘Application of the Privacy Act 1988 to retained metadata’.

The PJCIS also noted a number of other privacy-related concerns about the Bill and proposed Scheme. First, it noted that the mandatorily retained metadata would become a ‘honey pot’ or target ‘both for those with criminal or malicious intent and civil litigants.

Second, it noted that the Bill does not contain any provisions that prevent offshore storage of the mandatorily retained metadata in cloud services under the control of foreign corporations or governments. In the context of that concern, it is worth noting that offshore transfer and storage of personal information is not automatically or inherently incompatible with the Privacy Act 1988 and the APPs or privacy protection or security in generally. This is because the Privacy Act 1988 does not prohibit offshore storage or transfer of personal information. APPs 8 and 11 are applicable to offshore storage of personal information, such as that proposed to be collected and retained under the proposed Scheme.

APP 8 (cross-border disclosure of personal information) regulates the disclosure and transfer of personal information by an Australian entity to a different entity overseas (importantly, this includes a parent company). APP 8 does not prohibit such disclosure, but instead requires the relevant Australian entity, prior to the disclosure or transfer of personal information, to ‘take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information’. An example of such ‘reasonable steps’ would be through the use of appropriate contractual provisions between the two entities. However, the Australian entity remains accountable for an act or practice of the overseas recipient that would breach the APPs (subject to limited exceptions).

Likewise, APP 11 (security of personal information) requires that an entity must:

• take active measures to ensure the security of personal information it holds and
• actively consider whether it is permitted to retain personal information.

APP 11 also requires entities to take ‘reasonable steps to protect the personal information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure’. It could be argued that transferring personal information to offshore data storage providers in overseas jurisdictions that either lack laws that provide equivalent protection to that provided by the Privacy Act 1988 or are known to have frequent data breaches would breach APP 11.

104. Ibid., p. 283, para [7.76].
105. Ibid., p. 284, para [7.78].
106. Ibid., p. 290, para [7.99].
108. Ibid., p. 287, para [7.89].
109. Ibid., pp. 287 and 289, paras [7.89] and [7.94].
113. OAIC APP 11, ibid., p. 2.
Importantly however, the key point here is that currently, it is not illegal for Australian companies to store or transfer personal information offshore, or to transfer it to other entities offshore for storage.

The PJCIS also noted that the Bill does not explicitly require metadata to be destroyed at the end of the retention period and that the commercial entities that will store the mandatorily collected metadata are not required to adhere to the same level of data security standards as government agencies. As a result of the above, the PJCIS recommended that:

- the Bill be amended to require all service providers to be compliant, in respect of retained data, with either the Australian Privacy Principles or binding rules developed by the Australian Privacy Commissioner;

- the Bill be amended to require service providers to encrypt telecommunications data that has been retained for the purposes of the mandatory data retention regime (as a way of enhancing the security of retained data) and

- a mandatory data breach notification scheme be introduced by the end of 2015 (which would, in the view of the PJCIS, provide a strong incentive for service providers to implement robust security measures to protect data retained under the data retention regime).

The Bill has been amended to reflect those recommendations, with the exception of the introduction of a mandatory data breach notification scheme.

The application of the Scheme to ‘offshore’ and ‘over the top’ providers

So-called ‘offshore’ service providers are entities that provide communications services but ‘do not have infrastructure in this country’. The PJCIS noted that there are a number of offshore telecommunication service providers that ‘have a significant presence in the Australian market’. In contrast ‘over the top’ service providers are services ‘such as web-based email, VoIP or [a] cloud service’.

Hence the PJCIS noted that there was some confusion as to the precise obligations of ‘offshore’ and ‘over the top’ service providers under the Bill, as well as concerns about the impact of the proposed Scheme on Australian service providers’ competitiveness and the potential impact of ‘this ‘gap’ on agencies’ investigative capabilities’.

After evaluating those issues the PJCIS noted:

- it is appropriate that data retention obligations apply in respect of services provided to Australian customers, even where infrastructure used by the service provider to deliver that service is not located in Australia, but

- limiting the application of data retention obligations to companies that are within Australia’s territorial jurisdiction is an appropriate measure, as it avoids subjecting multinational companies to competing and potentially irreconcilable legal obligations.

However, it concluded that the ‘primary effect of this limitation is that data retention obligations will apply to ‘over-the-top’ services provided by service providers with infrastructure in Australia, but will not apply to ‘over-the-top’ services provided by wholly-offshore companies’. It also acknowledged that the exclusion of over-the-top services provided by wholly-offshore entities (that is, without any physical presence in Australia) ‘may have capability implications’. However the PJCIS concluded that ‘Australian agencies are able to obtain

---

114. Ibid., p. 288, para [7.89].
115. Ibid., p. 289, para [7.94].
116. Ibid., pp. 296-297, para [7.122] and recommendation 35.
117. Ibid., pp. 297-298, para [7.127] and recommendation 37.
118. Ibid., pp. 298-299, para [7.128] and recommendation 38.
119. See proposed sections 187LA and 187BA.
120. Ibid., p. 152, para [5.7].
121. Ibid.
122. Ibid., p. 154, para [5.13].
123. Ibid., p. 152, para [5.7].
124. Ibid., p. 155, paras [5.16-5.17].
125. Ibid., p. 155, para [5.17].
126. Ibid, pp. 158-159, para [5.18].
relatively rapid assistance from law enforcement counterparts’ in a number of Western countries where such over-the-top service providers are based when seeking access to metadata potentially held by them.\textsuperscript{127}

As result, the PJCIS recommended that the Bill be amended to define the term ‘infrastructure’ in greater detail, and thus that ensure overseas providers of over-the-top services are excluded from the proposed Scheme, as intended.\textsuperscript{128} The Bill was amended to give effect to that recommendation as discussed below.\textsuperscript{129}

**Evaluating the effectiveness of the Scheme**

After examining the views of witnesses and submitters on the issue of the review of the proposed Scheme provided by \textbf{proposed section 187N} of the Bill, the PJCIS noted the ‘importance of having a sound evidence base that draws on practical experience’ to inform any future review of the operation of the proposed Scheme.\textsuperscript{130} As a result, the PJCIS noted that the terms of reference for such a review should (amongst other items) include:

- the effectiveness of the scheme
- the appropriateness of the dataset and retention period and
- the number of data breaches.\textsuperscript{131}

The PJCIS also noted that statistical data related to the issues above will be required (for example, the age of data requested). The PJCIS also, rather pointedly, noted that:

\ldots during the course of this inquiry, the Committee was informed on numerous occasions that the data it sought was not collected. The Committee considers that, to facilitate an effective future review, it is essential that appropriate statistical data be retained by agencies.\textsuperscript{132} (emphasis added).

As a result, the PJCIS recommended that ‘agencies be required to retain records for the period from commencement of the regime until the Committee’s review is concluded’ in order to provide an evidentiary base for any future review of the effectiveness of the Scheme.\textsuperscript{133} The Bill was amended to give effect to these recommendations.\textsuperscript{134}

**Using retained metadata to identify journalists’ sources**

The PJCIS noted that a number of submitters to the Inquiry ‘expressed significant concerns’ in regard to agencies accessing ‘privileged or otherwise sensitive’ metadata, including the capacity of metadata to identify journalists’ sources.\textsuperscript{135}

After examining the views of witnesses and submitters on issues related to the potential use of mandatorily retained metadata to identify the confidential sources of journalists, the PJCIS noted:

- metadata ‘has the potential to possess an additional level of sensitivity because of the nature of the relationship of those communicating, including… journalist relationships with confidential sources’\textsuperscript{136}
- metadata has ‘the capacity for telecommunications data to be used to identify confidential sources’ and whilst this may have a ‘chilling impact’ there may be circumstances ‘such as the investigation of serious crimes’ in which it may be ‘appropriate and proper for journalists to be investigated by law enforcement agencies’.\textsuperscript{137}

\textsuperscript{127} Ibid.
\textsuperscript{128} Ibid., p. 156, para [5.20] and recommendation 11.
\textsuperscript{129} See: \textit{item 5} in Part 2 of the Schedule 1 of the Bill.
\textsuperscript{130} Ibid., p. 276, para [7.56].
\textsuperscript{131} Ibid., pp. 276-277, para [7.58].
\textsuperscript{132} Ibid., p. 277, para [7.59].
\textsuperscript{133} Ibid., p. 277, para [7.60].
\textsuperscript{134} See \textit{proposed subsections 187N(3)-(5)}.
\textsuperscript{135} Ibid., p. 251, para [6.193] and p. 257, para [6.210].
\textsuperscript{136} Ibid., p. 257, para [6.210].
\textsuperscript{137} Ibid., pp. 257-258, para [6.214].
The PJCIS, after noting the importance of freedom of the press and the protection of journalists’ sources concluded that ‘this matter requires further consideration before a final recommendation can be made’. However, the PJCIS proposed (as an interim measure in the absence of pre-access oversight of by an independent body) that:

... it is reasonable to require the Ombudsman or Inspector-General of Intelligence and Security (IGIS), as appropriate, to be notified of the making of an authorisation which is for the purpose of determining the identity of a journalist’s sources.

As a result, the PJCIS recommended that:

- the question of how to deal with the authorisation of a disclosure or use of telecommunications data for the purpose of determining the identity of a journalist’s source be the subject of a review by the PJCIS (which would report back to Parliament within three months)

- any such review should ‘consider international best practice, including data retention regulation in the United Kingdom’

- the TiA Act be amended to ‘require agencies to provide a copy’ to the Commonwealth Ombudsman, (or IGIS in the case of ASIO) of each authorisation that ‘authorises disclosure of information or documents’ under Chapter 4 of the TiA Act for the purpose of determining the identity of a journalist’s sources and

- the IGIS or Commonwealth Ombudsman ‘be required to notify’ the PJCIS on each such instance, as it relates to authorisations made by the AFP or ASIO ‘as soon as practicable after receiving advice of the authorisation and be required to brief the Committee accordingly’.

In response to the above, the Government established the recommended Inquiry and has also since amended the Bill to create a warrant regime governing access to journalists’ metadata for the purposes of determining a source, as discussed below under the heading ‘Proposed journalist information warrant regime’.

Parliamentary Joint Committee on Human Rights

The Parliamentary Joint Committee on Human Rights (PJCHR) reported on the Bill in November 2014 (the 2014 Report), and indicated that it will ‘report on a response recently received from the Attorney-General in relation to matters raised by the Committee’. It subsequently reported on the response received from the Attorney-General on 18 March 2015 (the 2015 Report). The PJCHR noted that:

Having accepted the important and legitimate objective of the bill, the committee raised a number of issues going to the proportionality of the scheme in support of that legitimate objective. The Attorney-General’s response provided further information in response to the committee’s initial scrutiny analysis. Some committee members considered the Attorney-General’s advice addressed many of their concerns, while some other members remained concerned about the proportionality of the scheme as proposed. The difference of views within the committee reflects the inherent difficulty of assessing proportionality. Nevertheless, the report provides a useful assessment for members of the bill’s compatibility with Australia’s international human rights obligations.

The PJCHR noted in both the 2014 and 2015 Report that the proposed Scheme engages the rights to:

---

138. Ibid., p. 258, para [6.125].
139. Ibid., p. 258, para [6.126].
140. Ibid., p. 258, recommendation 26.
141. Ibid.
142. Ibid., p. 259, recommendation 27.
143. Ibid.
• privacy\textsuperscript{147}
• freedom of opinion and expression\textsuperscript{148} and
• an effective remedy.\textsuperscript{149}

The PJCHR’s views on each of these rights is outlined below.

The right to privacy
In its 2014 Report the PJCHR noted that ‘the proposed scheme clearly limits the right to privacy’ and that whilst the right to privacy may be subject to limitations provided by law which are not arbitrary, any such limitations ‘must seek to achieve a legitimate objective and be reasonable, necessary and proportionate to achieving that objective’.\textsuperscript{150}

The data set
The PJCHR stated in its 2014 Report that as ‘the proposed scheme would require private service providers to collect and retain data on each and every customer... just in case that data is needed for law enforcement purposes’ the proposed Scheme is ‘very intrusive of privacy’ and therefore ‘raises an issue of proportionality’.\textsuperscript{151}

In both its 2014 and 2015 Report, the PJCHR expressed the view that the Bill created an arbitrary interference with the right to privacy and therefore should be amended to:

• define the types of data that are to be retained (instead of using regulations to do so) or alternatively, release an exposure draft of the regulation specifying the types of data to be retained\textsuperscript{152} and

• include an ‘exclusive definition of ‘content’ for the purpose of the scheme’.\textsuperscript{153}

Whilst the Bill has been amended to place the definition of metadata into the Bill, it has not been amended to provide a definition of ‘content’ as recommended by the PJCHR.

Retention period and use of retained metadata to investigate minor offences
The PJCHR also noted in the 2014 Report that the proposed retention period of two years ‘raises the question of whether the period is disproportionate, and may go beyond the period necessary to achieve the scheme’s legitimate objective’ (that being the ‘pressing social need’ for enforcement agencies to be able to effectively investigate and prosecute crimes).\textsuperscript{154} It then noted that whether the retention period is proportionate and necessary can be ‘resolved by reference to the purposes for which the data is accessed’.\textsuperscript{155} As noted in the Replacement Explanatory Memorandum and Second Reading Speech, those purposes include:

• counter-terrorism, organised crime, counter-espionage and cyber-security investigations and serious criminal investigations (such as serious sexual assaults, drug trafficking, murder and kidnapping)\textsuperscript{156}

• the protection of national security, public safety and addressing crime\textsuperscript{157}

• advancing criminal and security investigations and ensuring they are effectively investigated and prosecuted.\textsuperscript{158}


\textsuperscript{150} PJCHR, *Fifteenth Report of the 44th Parliament*, ibid., pp. 11 and 13, paras [1.25] and [1.31].

\textsuperscript{151} ibid., p. 13, para [1.31].


\textsuperscript{154} ibid., p. 12, para [1.29] and p. 15, para [1.41].

\textsuperscript{155} ibid., p. 15, para [1.41].


\textsuperscript{157} Explanatory Memorandum, op. cit., p. 10, para [33].

\textsuperscript{158} ibid., p. 11, paras [34-35].
The PJCHR noted that ‘the scheme does not limit access to data which is older than six months to the investigation of national security and complex criminal offences’ and hence requested further advice from the Attorney-General as to ‘whether the two year retention period is necessary and proportionate in pursuit of a legitimate objective.’\(^{159}\) In addition the PJCHR also noted in its 2014 Report that there were not any ‘significant limits’ on the type of investigations to ‘which a valid disclosure authorisation for existing data may apply’.\(^{160}\)

The PJCHR expressed particular concern at the lack of a requirement that disclosure of metadata be related only to serious crimes and that as currently drafted, the Bill and TIA Act would allow the disclosure of mandatorily retained metadata ‘where it is ‘reasonably necessary’ for the enforcement of minor offences’.\(^{161}\) As a result it concluded that:

> The lack of a threshold, relating to the nature and seriousness of the offence, for access to retained data appears to be a disproportionate limitation on the right to privacy. The committee considers that to ensure a proportionate limitation on the right to privacy, an appropriate threshold should be established to restrict access to retained data to investigations of specified threatened or actual crimes that are serious, or to categories of serious crimes such as major indictable offences (as is the current threshold for requiring the option of trial by jury). The committee is additionally concerned that the threshold of ‘reasonably necessary’ for the enforcement of offences may lack the requisite degree of precision.\(^{162}\) (emphasis added).

In response to the above concerns and suggestion to limit access to retained metadata to investigations of serious crimes, the Attorney-General stated (amongst other things) that:

> Australia is required to make metadata available for all criminal investigations by virtue of being a party to the Convention on Cybercrime. Article 14 of that Convention requires that Australia and other States parties establish powers and procedures, including access to historical telecommunications data, to enable the collection of evidence in electronic form of a criminal offence.

> Telecommunications data is valuable to combatting all crimes, is less intrusive than other investigative techniques, and should not be arbitrarily limited to a narrow selection of crimes.\(^{163}\)

This issue is explored in detail under the heading ‘Error! Reference source not found.’ in the ‘Key issues and provisions’ section of this Digest. However, it is worth noting that the above contention appears to reflect an overly narrow reading of the obligations imposed by the Cybercrime Convention on Australia.

**Subsequent use of disclosed metadata for unrelated purposes**

In its 2014 Report the PJCHR recommended that the Bill be amended to limit disclosure authorisations for existing metadata to situations where it is ‘necessary’ for the investigation of specified serious crimes, or categories of serious crimes.\(^{164}\) Likewise, it also recommended that the Bill be amended to ensure that metadata disclosed for one authorised purpose is not then used for unrelated purposes by restricting such subsequent access or disclosure to situations where:

- it is ‘necessary’ for investigations of specific serious crimes such as major indictable offences or specific serious threats and
- used only by the requesting agency for the purpose for which the request was made and for a defined period of time.\(^{165}\)

After considering the Attorney-General’s response to its concerns and recommendations outlined above, the PJCHR noted in its 2015 Report that it agreed with the Attorney-General’s view ‘that there is no general


\(^{160}\) Ibid., p. 16, para [1.48].

\(^{161}\) Ibid., p. 16, para [1.48].

\(^{162}\) Ibid., p. 16, para [1.48].

\(^{163}\) Ibid., p. 17, para [1.51].
proposition in international law that information gathered by a law enforcement or security agency may be used only for the purpose for which it was obtained. However, it reiterated its previous view that:

... measures which permit access to personal information or information sharing between agencies will be a permissible limitation on human rights where they pursue a legitimate objective, are rationally connected to that objective and are a proportionate means of achieving that objective.  

It therefore restated that in its view, the proposed Scheme still ‘raises questions regarding the proportionality’ even though it ‘pursues a legitimate objective’. However, it stated that after considering the Attorney-General’s response:

... law enforcement agencies may have legitimate reasons for utilising metadata obtained for one purpose for the purpose of investigating another crime or for sharing data across agencies. The committee therefore considers that, based on the information provided regarding the conduct of investigations, it may not be necessary in this case to restrict use of metadata once accessed solely to the purpose for which the request for access was made... [but] there still needs to be sufficient limitations on the use of retained metadata, once accessed, to ensure that the interference with the right to privacy is proportionate, in the sense of being the alternative that is the least restrictive of rights. In this respect, the committee considers that, where agencies are working together, a less restrictive alternative from the perspective of the right to privacy may be to have a system which expressly authorises the access of each agency to the retained telecommunications data.  

The PJCHR therefore recommended that to avoid the disproportionate limitation on the right to privacy that could result from metadata that is disclosed for an authorised purpose subsequently being used for an unrelated purpose, the Bill be amended to restrict access to retained data on defined objective grounds such as:

- where it is reasonably necessary for investigations of specific serious crimes such as major indictable offences, specific serious threats or the investigation of serious matters by the ASIC, the ATO and ACCC and
- where it used by the authorised agency within a defined period of time.

Those recommendations are not fully implemented by the amendments to the Bill provided by items 6J and 6K.

Warrants, oversight and accountability

The PJCHR noted in its 2014 Report that the proposed oversight mechanisms provided by the Bill are ‘directed at reviewing access powers after they have been exercised’. It noted that the Explanatory Memorandum:

... does not address the question of why access to metadata under the scheme should not be subject to prior review through a warrant system, as is the case for access to other forms of information under the TIA Act.

The PJCHR noted that in its view a requirement ‘for prior review would more effectively ensure that the grant of access to metadata under the scheme would be consistent with the right to privacy’ and therefore 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 and defined objective grounds.

Further, it also recommended that, in relation to the proposed oversight of the scheme by the Commonwealth Ombudsman and the PJCIS, a mechanism to provide ‘close prior oversight of the recommended warrant process
for access to retained metadata under the scheme’ be established to complement the proposed ‘important subsequent review mechanisms’.\(^\text{174}\)

In its 2015 Report, the PJCHR noted that in his response to the issues and recommendations outlined above, that the Attorney-General had rejected its 2014 Report recommendation that agencies should be required to obtain a warrant to access metadata under the proposed data retention scheme.\(^\text{175}\) It noted that:

... technological developments have meant that metadata now allows very precise conclusions to be drawn about an individual’s life, habits, interests, relationships and views even without access to the content of a communication being available. Given this, a prior review mechanism would assist to ensure that a person’s metadata is accessed only in circumstances where such access would be proportionate. That is, prior review could assist to prevent unjustifiable interference with a person’s privacy before it occurs.\(^\text{176}\)

Further, it noted that whilst it considered the proposed post-access oversight mechanisms ‘extremely important’, they were somewhat limited as they ‘are directed at reviewing the exercise of powers only after a potentially unjustifiable interference with a person’s privacy has occurred.’\(^\text{177}\) It also expressed the view that the existing internal agency approval processes imposed by the TIA Act, whilst being ‘important controls’ nonetheless ‘provide a lower level of protection than could be provided by external independent review processes.’\(^\text{178}\)

It also noted that one of the relevant factors in the Digital Rights Ireland case that led to the ECJ declaring the EU-DRD invalid was:

... the absence of a requirement that access to retained data be subject to prior review by a court or independent administrative body (such as is provided by a warrant scheme).\(^\text{179}\) (emphasis added).

After considering the above issues and the response provided by the Attorney-General to its 2014 Report in relation to them, the PJCHR did not arrive at a unanimous conclusion, nor did it make recommendations with unanimous support. The differing recommendations are noted in the table below. As noted in the tabling statement that accompanied the 2015 Report: ‘[t]he difference of views within the committee reflects the inherent difficulty of assessing proportionality.’\(^\text{180}\)

**Table 3: PJCHR recommendations in relation to pre-access oversight of metadata applications**

<table>
<thead>
<tr>
<th>Recommendation / view</th>
<th>Level of support</th>
</tr>
</thead>
<tbody>
<tr>
<td>• the existing requirements in the TIA Act for internal agency authorisation for disclosure of telecommunications data provide a sufficient safeguard to address privacy concerns.(^\text{181})</td>
<td>‘the majority of the committee’</td>
</tr>
<tr>
<td>• a prior independent authorisation system should be instituted, and that such a mechanism could assist to ensure impartial assessment of the content and sufficiency of application. This would be an important safeguard where applications occurred ex parte,(^\text{182}) and so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior review, the Bill be amended to provide that access to retained data be granted only on the basis of prior independent</td>
<td>‘some committee members’</td>
</tr>
</tbody>
</table>

\(^{174}\) Ibid., pp. 18-19, para [1.60].
\(^{176}\) Ibid., p. 68, para [1.227].
\(^{177}\) Ibid., p. 69, para [1.228].
\(^{178}\) Ibid., p. 69, para [1.229].
\(^{179}\) Ibid., p. 69, para [1.230].
\(^{181}\) Ibid., p. 70, para [1.237].
\(^{182}\) Ibid., p. 70, para [1.238].
Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Warning: All viewers of this digest are advised to visit the disclaimer appearing at the end of this document. The disclaimer sets out the status and purpose of the digest.

<table>
<thead>
<tr>
<th>Recommendation / view</th>
<th>Level of support</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorisation, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds.</td>
<td>‘another committee member’ (i.e. one member)</td>
</tr>
</tbody>
</table>

- in order to provide a sufficient safeguard, and to avoid the unnecessary limitation on the right to privacy, any prior independent review should take the form 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 and defined objective grounds.
- warrant processes are able to be sufficiently flexible to respond to investigative timeframes, including emergency situations. They may be expedited where necessary, including by, for example, having magistrates available to issue warrants out of hours or over the phone, and it is usual for warrant systems to have expedited processes to allow for time critical situations, and
- so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior, independent judicial review, 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 and defined objective grounds.

Sources: as per footnotes in the table above.

The right to freedom of opinion and expression and the right to an effective remedy

The PJCHR noted in its 2014 Report that the proposed Scheme may impact on both the right to freedom of expression and the right to an effective remedy. In relation to the right to freedom of expression it noted that:

... the proposed scheme may have an inhibiting or ‘chilling’ effect on people’s freedom and willingness to communicate via telecommunications services. The committee notes that the proposed provisions may have a particular inhibiting or ‘chilling’ effect on journalists who may be concerned about the protection of their sources.

It concluded that as the proposed Scheme would allow retained metadata to accessed and used ‘without the user or individual ever being informed’ that there was the potential that the proposed Scheme would ‘lead people to ’self-censor’ the views expressed via telecommunications services, or to restrict their own use of such services.’ The PJCHR then recommended that the Bill be amended to introduce a delayed notification requirement whereby:

- individuals would be notified when their metadata is subject to an application for authorisation for access or
- once it has been accessed (noting that there may be circumstances where delayed notification would be appropriate, such as in the context of investigating a serious crime).

Further, in relation to the right to an effective remedy, the PJCHR noted that the Explanatory Memorandum did not address the limitation on the right to an effective remedy. It recommended that the Bill be amended to provide ‘a process to allow individuals to challenge’ access to their metadata (subject to certain exemptions to, for example, facilitate continuing investigations of serious crimes). It also noted that the right to an effective remedy would be supported by the inclusion of a delayed notification requirement into the proposed Scheme.

---

183. Ibid., p. 70, para [1.236].
184. Ibid., p. 70, para [1.239].
185. Ibid., p. 70, para [1.240].
186. Ibid., p. 71, para [1.241].
188. Ibid., p. 20, para [1.70].
189. Ibid., p. 20, para [1.71].
190. Ibid., p. 21, para [1.74].
191. Ibid., p. 21, paras [1.74-1.76].
because ‘it would be impossible for an individual to seek redress for breach of their right to privacy if they did not know that data pertaining to them had been subject to an access authorisation’. 192

The Bill has not been amended to reflect those recommendations.

After considering the above issues and the response provided by the Attorney-General to its 2014 Report in relation to them, the PJCHR restated its view that ‘the scheme limits the right to freedom of expression.’ 193 In relation to the response received by the Attorney-General, the PJCHR noted:

... the Attorney-General’s view that a notification requirement that telecommunications data had been accessed would hamper investigations... However, the committee notes that its suggestion clearly acknowledged the potential for such a requirement to impact on investigations, in stating that delayed notification arrangements would be appropriate in a range of circumstances including where ongoing investigations may be hampered. The committee notes that the Attorney-General’s response therefore does not significantly address the issues raised by the committee in relation to the right to freedom of opinion and expression, and ensuring the proportionality of the scheme in this regard. 194 (emphasis added)

After considering the above issues and the response provided by the Attorney-General to its 2014 Report in relation to them, the PJCHR did not arrive at a unanimous conclusion, nor did it make recommendations with unanimous support. The differing recommendations are noted in the table below.

Table 4: PJCHR recommendations in relation to pre-access oversight of metadata applications

<table>
<thead>
<tr>
<th>Recommendation / view</th>
<th>Level of support</th>
</tr>
</thead>
<tbody>
<tr>
<td>• requests advice from the Attorney-General as to what measures there are to ensure that there are effective remedies available to individuals for any breaches that may occur of the right to privacy or the right to freedom of association as a result of the mandatory data retention regime 195</td>
<td>‘the committee’</td>
</tr>
<tr>
<td>• to ensure a proportional limitation on the right to freedom of opinion and expression, consideration be given to amending the proposed scheme to provide a mechanism to guarantee that access to data is sufficiently circumscribed, so that individuals are notified when their metadata has been accessed (noting that there may be circumstances where such notification would need to be delayed to avoid jeopardising any ongoing investigation) 196</td>
<td>‘some committee members’</td>
</tr>
<tr>
<td>• the following requirements would better ensure the proportionality of the scheme in relation to the right to freedom of expression:</td>
<td></td>
</tr>
<tr>
<td>‒ a requirement for individuals to be notified when their metadata is subject to an application for authorisation for access (noting that there may be circumstances where delayed notification would be appropriate, such as in the context of investigating a serious crime), and</td>
<td></td>
</tr>
<tr>
<td>‒ a process to allow individuals to challenge such access (noting that exemptions may need to be available for continuing investigations of, for example, a serious crime). 197</td>
<td>‘another committee member’ (i.e. one member)</td>
</tr>
</tbody>
</table>

Sources: as per footnotes in the table above.

192. Ibid., p. 21, para [1.76].
194. Ibid., pp. 72-73, paras [1.250-1.251].
195. Ibid., p. 74, para [1.257].
196. Ibid., p. 73, para [1.253].
197. Ibid., p. 73, para [1.254].
Policy position of non-government parties/independents

**Labor**

The Labor party has indicated that, subject to the Government accepting all 39 recommendations made by the PJCIS (and moving amendments to the Bill to give effect to them), it will support the Bill.\(^{198}\) The Government has since formally indicated that it ‘will support all’ of the PJCIS’s recommendations made ‘in its unanimous bipartisan report’.\(^{199}\)

As such, the Labor party will support the Bill, subject to further consideration of the issues related to accessing journalists’ metadata, greater oversight of the Scheme by the PJCIS and where the metadata will be stored (in Australia or offshore).\(^{200}\)

However, as Table 7: PJCIS recommendations and amendments made to the Bill demonstrates, not all of the PJCIS’s recommendations have been dealt with by the amendments made to the Bill in the House of Representatives.

**Greens**

The Greens have indicated that they will ‘fight to amend [the] metadata surveillance bill’.\(^{201}\) Further, Senator Scott Ludlam, the Greens spokesperson for Communications has indicated and that even if the Bill is amended in accordance with the PJCIS’s recommendations the:

> ... bill should be rejected. It’s a two-year mandatory data retention regime. It’s pretty much exactly what has been cooking away in the background since 2008 that’s been condemned by all sides of politics when it’s suited them at different times and that’s what it looks like the government is going to proceed with.’\(^{202}\)

As a result, it would appear unlikely that the Greens will support the passage of the Bill.

**Other Senators**

**Family First**

The position of Family First Senator Bob Day on the Bill as drafted or as amended to reflect the PJCIS’s recommendations is not clear. However, Senator Day voted in favour of an Order for the Production of

---

200. B Shorten (Leader of the Opposition), *Doorstop interview*, Canberra, transcript, 4 March 2015, accessed 24 March 2015, p. 6: ‘There are a couple of issues which do require more work and I think any fair minded person would recognise it. One, and not the least of which would be interest to you is press freedom... Also we’re keen to make sure that Senator John Faulkner lately of this place proposed having some greater power for the Parliamentary Committee like happens in other jurisdictions around the world on national security for oversight. We think that’s very important. There’s also been some issues raised about where the data is stored in the cloud. Is it stored onshore, is it stored offshore? None of these issues are issue which are too hard to work out, but they’re not issues which can be sorted out by, you know, a statement or a press release in a matter of minutes.’; B Shorten (Leader of the Opposition), *Doorstop interview*, Sydney, transcript, 10 March 2015, accessed 24 March 2015, p. 9: ‘... Labor will make improvements on that legislation. There has been a parliamentary joint committee on intelligence matters and security matters working carefully through it - over 200 submissions. Labor will get the balance right because what we understand is it’s important to think for the long term as well as the immediate problems. But we will work with the government in national security, but yes, I can say to you, Ian that we’ll also make sure that we keep press freedoms uppermost in our mind. We will get this balance right, this country is smart enough to do both.’; S Jones (Shadow Assistant Minister for Health), *Doorstop interview*, Canberra, transcript, 2 March 2015, accessed 24 March 2015, p. 1: ‘We have also put a big red circle around the issue of journalists and the important issue of data retention for journalist information - this is going to be subject to a further inquiry. So far from just waving things through, you will see much tougher requirements when it comes to privacy arrangements and much closer scrutiny when it comes to parliamentary oversight’; J Clare (Shadow Minister for Communications), *Doorstop interview*, Canberra, transcript, 4 March 2015, accessed 24 March 2015, pp. 2-3: ‘Labor’s strong view is that there should be a warrant that law enforcement agencies should get before they can access journalist’s metadata, because we do think journalists are different. If you can access their sources it undermines press freedom... [keep this in mind too, sometimes journalists are investigating law enforcement and that’s why I think they need to be treated separately. We couldn’t get agreement on that point. We have agreed to a further investigation of that and that Committee hopefully will begin those inquiries shortly.’; S Martin, ‘Labor to fall in line on data laws’, op. cit.
201. S Ludlam (Greens spokesperson for Communications), *Greens will fight to amend metadata surveillance bill as Labor looks to have caved*, media release, 27 February 2015, accessed 12 March 2015.
Document in relation to the PricewaterhouseCoopers (PWC) report that modelled the cost of the proposed Scheme. 203

**Palmer United Party**

The position of the Palmer United Party on the Bill as drafted or as amended to reflect the PJCIS’s recommendations is not clear. However, Palmer United Party (PUP) leader Clive Palmer has been reported as dismissing the data retention laws as a ‘diversion from the main economic issues’. 204 Senator Zhenya Wang voted in favour of an Order for the Production of Document in relation to the PWC report that modelled the cost of the proposed Scheme moved by Greens Senator Scott Ludlam. 205

**Senator Leyonhjelm**

Whilst Liberal Democrat Senator David Leyonhjelm has not formally indicated his position on the Bill as drafted, from media comment it appears likely that he will oppose the Bill, even if amended to reflect all of the PJCIS’s recommendations. 206

**Senator Xenophon**

The position of Independent Senator Nick Xenophon on the Bill as drafted or as amended to reflect the PJCIS’s recommendations is not clear. However, Senator Xenophon has previously stated ‘we should oppose any move by the government that treats innocent Australians like potential suspects’ and that the proposed Scheme will ‘treat every single Australian, man, woman or child like a potential criminal.’ 207 He also argues that the proposed Scheme would amount to ‘the biggest mass surveillance program in our nation’s history’. 208 Since the amended Bill was passed by the House of Representatives, Senator Xenophon has indicated that he plans to move amendments to ‘mend’ the Bill. In relation to the proposed journalist metadata warrant regime, Senator Xenophon has indicated that he ‘wants Australia to adopt the US system where media groups are told of warrant requests and can challenge them.’ 209

Further, Senator Xenophon voted in favour of an Order for the Production of Document in relation to the PWC report that modelled the cost of the proposed Scheme. 210 That, combined with his previous comments appears to suggest a level of scepticism towards the Bill as drafted by Senator Xenophon.

**Other Independent Senators**

The position of Independent Senators John Madigan, Jacqui Lambie and Glenn Lazarus on the Bill as drafted or as amended to reflect the PJCIS’s recommendations is not clear. However, all voted in favour of an Order for the Production of Document in relation to the PWC report that modelled the cost of the proposed Scheme (although Senator Lazarus did so whilst a member of the PUP). 211
Position of major interest groups

The PJCIS Inquiry into the Bill received 204 submissions, many from private citizens expressing concern at the proposed Scheme. Due to time and resource constraints, only a selection of responses from interest groups and stakeholders are examined in this Digest.

Intelligence and law enforcement agencies

ASIO

In its supplementary submissions ASIO notes that in its view the proposed two year retention period is ‘very much a compromise’ and it would ‘prefer a longer retention period to enable us to perform our statutory functions – but we recognise the policy balance to be struck between national security needs, privacy of the community and industry regulation’. 212

Further, ASIO also noted that as, in its view, ‘in the near term’ all metadata ‘will be IP-based due to the uptake of IP-based technologies’ it is important that ‘the legislation remain technology neutral’.213 ASIO also noted that in its view ensuring the application of the Bill to Wi-Fi networks ‘will be critical’ and hence it argued ‘against wide-scale exemption of Wi-Fi network access providers from data retention obligations’.214 In relation to Wi-Fi networks, it noted that, therefore at ‘a minimum, identifying details of the device, the Wi-Fi point of connection and the date-time stamp of the connections should be retained’.215

In relation to a number of concerns raised by various interest groups during the PJCIS Inquiry into the Bill and recommendations made by the PJCHR, ASIO noted that:

- preventing non-government entities (for example, civil litigants) from accessing metadata would not result in any ‘adverse effect on ASIO’s ability to perform its statutory functions’216
- placing further restrictions on the use of metadata disclosed for one purpose for another unrelated purpose would ‘impede ASIO’s effective pursuit of its functions’ as it is ‘likely that there will be instances’ where metadata disclosed in relation to one national security matter ‘then becomes relevant to another national security matter, as presently occurs’217
- the introduction of a warrant regime to govern access to metadata ‘would significantly impede ASIO’s operations’ resulting in ‘a significant impact on operational agility’ and ‘is just not practical’.218

ASIO also argued that the Bill should introduce consistent retention periods for all type of metadata, be it IP or telephony based metadata.219 ASIO noted that in its experience the retention period for metadata is ‘variable across service providers’220 as the tables below (produced by ASIO) demonstrate.221

Table 5: Historical communications data – comparative range of retention

<table>
<thead>
<tr>
<th>Matters to which information must relate</th>
<th>Telephony</th>
<th>Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service</td>
<td>Up to 7 years (and longer)</td>
<td>90 days to 5 years</td>
</tr>
<tr>
<td>2. The source of a communication</td>
<td>6 weeks to 7 years</td>
<td>0 days to 5</td>
</tr>
</tbody>
</table>


214. Ibid., p. 7.

215. Ibid.

216. Ibid., p. 4.

217. Ibid., p. 3.

218. Ibid., p. 4.

219. Ibid., p. 4.

220. Ibid., pp. 4-5.

221. Ibid., p. 5.
3. The destination of a communication

4. The date, time and duration of a communication, or of its connection to a relevant service

5. The type of communication or relevant service used in connection with a communication

<table>
<thead>
<tr>
<th>Historical communications data</th>
<th>Range of retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber information - name and address</td>
<td>7 years or longer</td>
</tr>
<tr>
<td>Telephone numbers called/received</td>
<td>6 weeks to 7 years</td>
</tr>
<tr>
<td>Telephone numbers associated with SMS</td>
<td>60 days to 7 years</td>
</tr>
<tr>
<td>Mobile Handset and SIM data</td>
<td>Up to 7 years</td>
</tr>
<tr>
<td>IP account, device and address information</td>
<td>90 days to 3 years</td>
</tr>
<tr>
<td>Addresses associated with email and other IP communications</td>
<td>45 days to 3 years</td>
</tr>
</tbody>
</table>

Source: as per footnote 221.

Table 6: Ranges of retention by service providers of historical communication data

ASIO noted that it would support any revision of the TIA Act and related legislation conducted on the basis of three guiding principles (1) the legislation remains technology neutral, (2) that carriers retain the metadata for access by ASIO and law enforcement agencies (rather than a central government-controlled repository), and (3) any amendments reduce ‘unnecessary bureaucratic overlay’.

ASIO noted that as the Bill was consistent with those principles, it is broadly supportive of the Bill.

Australian Federal Police

The Australian Federal Police (AFP) supports the Bill. In a supplementary submission the AFP expressed the view that ‘there is no clear correlation between the age of the information’ and its investigatory value as its value depends on the type of investigation, not its age. However, it expressed the view that ‘the two year retention period proposed in the Bill is a reasonable and appropriate timeframe’. The AFP also noted that in its view:

• given the increasing use of encryption, there is a ‘diminishment of law enforcement’s ability to access content’ and therefore the value of metadata itself increases

• the Bill address ‘critical capability requirements’ ensuring that increasingly-valuable metadata is consistently available to law enforcement agencies

• if the Bill does not pass it ‘will be increasingly relying on chance that perpetrators of crime’ are using specific service providers that retain metadata, a situation that is ‘clearly unsatisfactory when dealing with investigations into criminal matters such as child exploitation, counter-terrorism or serious and organised crime’ and

---

222. ASIO, *Supplementary submission 1 to PJCIS*, op. cit., p. 20.
223. Ibid., p. 10.
224. Ibid., pp. 7, 10; ASIO, *Supplementary submission 2 to PJCIS*, op. cit., accessed 24 March 2015, p. 1: ‘ASIO supports the Government’s data retention Bill...’.
226. Ibid., p. 5.
227. Ibid., p. 5.
228. Ibid., p. 6.
229. Ibid., p. 2.
230. Ibid., p. 2.
• the Bill will resolve ‘the existing incongruity’ whereby law enforcement can legitimately seek metadata from service providers ‘but there is no corresponding requirement’ for them to retain the metadata sought.\(^{231}\)

The AFP opposes the introduction of a warrant regime for metadata, noting that ‘such a scheme would generate unnecessary administrative burden and costs’.\(^{232}\) Further, it argued that the introduction of a warrant regime would ‘reduce operational responsiveness in time sensitive cases’.\(^{233}\) The AFP concluded that:

Without this reform the AFP will face growing uncertainty that telecommunication carriers will retain this data and a vital investigative tool will be lost. This state of affairs is manifestly unsatisfactory when dealing with criminal matters and national security.\(^{234}\)

State and territory police forces

The state and territory police forces all support the proposed Scheme.\(^{235}\) In their combined submission to the PJCIS, the state and territory police forces noted that whilst they supported the ‘retention of metadata for a period of two years for the majority of data sets’ they also supported ‘an extended data retention period of seven years for access to particular data sets’.\(^{236}\) The rationale given for an extended retention period for certain types of metadata (for example, subscriber related metadata) by the state and territory police forces was:

The New South Wales Police Force has tabled evidence to the PJCIS on 30th January 2015 which outlined the need to access telecommunications data for periods in excess five years. These crimes involved unsolved homicides, historical sexual assault and child abuse matters, armed robbery and kidnapping investigations to name but a few... it is submitted that these crimes are relevant to all police jurisdictions and are complex and significant crimes to investigate necessitating access to relevant telecommunications data. Further, the data sets sought are currently available to law enforcement for periods up to 7 years with certain carriers and this is of great assistance to law enforcement. Any period of less than 7 years for those data sets would potentially be a retrograde step for law enforcement and impact on the success of criminal investigations.\(^{237}\) (emphasis added).

In addition to supporting an extended retention period for certain types of metadata, the state and territory police forces also noted that they support the proposition that Wi-Fi providers should not be exempted from retaining metadata, on the basis that:

The increased availability of free network access poses obvious risks in terms of being able to solve crimes that are facilitated or committed using telecommunications devices roaming and operating on these Wi-Fi networks.\(^{238}\)

Finally, the state and territory police forces noted that whilst they support the current oversight and compliance frameworks, in their view a ‘more pragmatic and consistent approach would be to have a single oversight authority perform the compliance role in each jurisdiction.’\(^{239}\)

Other government agencies

Attorney-General’s Department

The Attorney-General’s Department (the AGD) provided a detailed submission to the PJCIS Inquiry.\(^{240}\) Key points made by the AGD in its submission include that (in its view):

\(^{231}\) Ibid., p. 6.

\(^{232}\) Ibid., p. 13.

\(^{233}\) Ibid.

\(^{234}\) Ibid., p. 14.

\(^{235}\) State and Territory police forces (Victoria Police, South Australia Police, Western Australia Police, Northern Territory Police, Queensland Police, Tasmanian Police and New South Wales Police), Submission to PJCIS, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 16 February 2015, accessed 16 March 2015, p. 2.

\(^{236}\) Ibid.

\(^{237}\) Ibid.

\(^{238}\) Ibid., p. 2.

\(^{239}\) Ibid., p. 3.

\(^{240}\) Attorney-General’s Department (AGD), Submission to PJCIS, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 12: ‘Considering the investigative and technological environment in which our agencies now operate, the ability to access communications and telecommunications data is, therefore, not just useful for Australia’s law enforcement and anti-corruption agencies. These powers are essential to allow agencies to investigate a wide range of criminal acts and security threats in this
the proposed data set is based on current best practice retention practices within the telecommunications industry and does not require the retention of metadata that is not currently retained by at least one provider\textsuperscript{241}

preservation orders are not a practical alternative to mandatory metadata retention as ‘service providers cannot preserve information that no longer exists’\textsuperscript{242}

the introduction of a mandatory data retention scheme is consistent with international approaches to these challenges\textsuperscript{243}

any benefits arising from the introduction of a metadata warrant regime ‘would be outweighed by the impact on agencies’ ability to combat serious crime and protect public safety’\textsuperscript{244} and

in any case post-access independent oversight (which is what is currently in place) ‘has a very similar psychological effect to a warrant process’ and hence is ‘a strong deterrent against non-compliance or misconduct’.\textsuperscript{245}

In addition to the above points, the AGD also discussed a number of other issues related to accessing metadata associated with sensitive or privileged communications, the application of the metadata retention obligations to both Wi-Fi service and ‘offshore’ service providers, the retention period and the security of the retained metadata, as discussed below.

**Issues related to accessing metadata associated with sensitive or privileged communications**

In regards to concerns raised about the disclosure of lawyers’ and journalists’ metadata, the AGD noted that the common law does not attach legal professional privilege to the fact of the existence of a communication between a client and their lawyer, only to the content of privileged communications.\textsuperscript{246} As a result, it concluded that the proposed Scheme ‘do[es] not affect or authorise the disclosure of the content of any communication, including any privileged communication’.\textsuperscript{247}

In relation to concerns about using metadata to identify journalists’ sources and the suggestions that ‘a special status should be afforded’ to the metadata of journalists (at least in regards to their interactions with public sector whistleblowers) the AGD noted that:

- it is not appropriate to afford a special status to particular types of communications (as powers of this type should, by their nature, be applied generally) and
- legitimate whistleblowers are ‘immune from all criminal, civil and administrative liability’ under the Public Interest Disclosures Act 2013 and hence, metadata access powers ‘will generally not be available to law enforcement agencies in relation to genuine whistleblowers by reason of those disclosures alone’\textsuperscript{248}

The AGD did however, note that in relation to the UK metadata retention scheme, the UK Government had proposed:

> ... that authorising officers should give special consideration to necessity and proportionality when considering authorising the disclosure of data relating to the particular professions noted above [the draft code specifies doctors, lawyers, journalists, MPs and ministers of religion as such professions].\textsuperscript{249}

\textsuperscript{241}. Ibid., covering letter.
\textsuperscript{242}. Ibid., pp. 6 and 17.
\textsuperscript{243}. Ibid., p. 6.
\textsuperscript{244}. Ibid., p. 18.
\textsuperscript{245}. Ibid., p. 20.
\textsuperscript{247}. Ibid.
\textsuperscript{248}. Ibid., pp. 21-22.
\textsuperscript{249}. Ibid., p. 22.
As such, it would appear that as a matter of policy, the AGD does not support journalists’ metadata being afforded a ‘special status’ (given the Australian framework in regards to whistleblowing) and that, should restrictions on accessing the metadata of journalists be considered, it should be considered in the broader context of professions with similarly sensitive communications, such as doctors and lawyers.

**Application of the metadata retention obligations to Wi-Fi service providers**

The AGD noted that metadata retention obligations will not apply to services that are provided only to a single place, or to places in the same area ‘such as free Wi-Fi access provided in restaurants, libraries or a campus’. The AGD stated that:

> This exception reflects an assessment that the law enforcement and national security benefit of imposing data retention obligations on these services would be outweighed by the privacy and compliance burden.

However, it also noted that some key non-content data relating to the communications made from internet cafes will be retained by the internet service providers, supplying those services to the internet cafes. Further, the AGD also noted that the Bill will provide the Communications Access Co-ordinator (CAC) the power to declare that the metadata retention obligations apply to particular services that would otherwise be exempt (for example, a particular internet café) and thus:

> ... provides the flexibility to apply data retention obligations to services or networks operated by particular companies... or in particular buildings or places, where this is consistent with the requirements of law enforcement or national security.250

**Application of the metadata retention obligations to ‘offshore’ service providers**

The AGD noted that the metadata retention obligations created by the Bill are intended to apply to service providers that have infrastructure such as servers, routers and/or cables within Australia, and that this obligation is designed to ‘ensure that service providers cannot avoid their data retention obligations by off-shoring part of their infrastructure or outsourcing the provision of some services to overseas entities’.251 However, the AGD noted that:

> ... there are a number of service providers that have a significant presence in the Australian telecommunications market that do not own or operate such infrastructure in Australia, and that therefore will not be covered by data retention obligations, including the major social media providers.252

However, the AGD expressed the view that ‘many companies based in foreign jurisdictions are subject to data retention laws in those jurisdictions’ and thus this reduced the need for Australian extra-territorial legislation, which invariably ‘would give rise to significant jurisdictional and conflict-of-laws issues’.253 Finally, the AGD also noted that as a party to the Council of Europe Cybercrime Convention, Australian law enforcement agencies ‘are able to obtain expedited assistance from 43 countries to obtain metadata held in those countries where it is relevant to their investigations’.254 Thus it appears that the AGD is satisfied that, on balance, the proposed Scheme, when combined with the international mechanisms discussed above, will capture enough service providers to allow for the effective investigation of crimes using metadata within Australia, even if some service providers are located offshore.

**The retention period**

The AGD appeared to be supportive of the proposed two-year retention period, and noted that law enforcement and national security agencies ‘advise that a two year retention period is appropriate to maintain their ability to investigate serious crime and threats to national security’ and that this advice ‘is consistent with the international experience’.255 They also noted that certain types of investigations (for example, drug trafficking, counter-terrorism and organised crime investigations) frequently involve longer investigatory periods and

---

250. Ibid., p. 23.
251. Ibid., p. 24.
252. Ibid.
253. Ibid.
254. Ibid.
255. Ibid., 30.
therefore require a disproportionate level of access to older metadata. \footnote{256} \footnote{257} Put simply, ‘where agencies require access to telecommunications data, its value does not decrease with age’. \footnote{258}

However, in relation to the possibility of having different retention periods for the different types of metadata (for example, internet protocol records versus location related metadata) the AGD noted that in its view ‘there is no rational basis for such a distinction in relation to the proposed data set’. \footnote{259}

The AGD therefore concluded that the proposed two year retention period ‘strikes a balance between the law enforcement and national security interests, cost to industry, and the privacy intrusion associated with retaining metadata’. \footnote{260}

**Security of the retained metadata**

In relation to the security of the retained metadata, the AGD noted that the ‘proposed dataset includes information that is privacy-sensitive’ and hence it was of the view that ‘it is important that this information is stored in an appropriate and secure manner’. \footnote{261} The AGD expressed the view that:

> Existing information security frameworks provide strong protections for the privacy of information held by the telecommunications industry, and will continue to apply to information held in accordance with data retention obligations. The Government has also announced new measures to further strengthen security across the telecommunications sector. The Department’s view is that it is preferable to implement a holistic security framework for the telecommunications sector, rather than imposing specific, stand-alone and potentially duplicative security obligations that apply only to a relatively narrow subsection of the information held by industry.

The AGD outlined the existing information security framework, focusing on the role played by the *Privacy Act 1988* but did not directly address the issue of offshore storage of metadata. Finally, the AGD noted that the Government had ‘announced that it will implement the Telecommunications Sector Security Reforms’ recommended by the PJCIS before metadata retention is fully implemented. \footnote{262}

**AHRC**

In its submission to the PJCIS Inquiry into the Bill, the Australian Human Rights Commission (AHRC), whilst acknowledging the ‘critical importance of ensuring that our police and security agencies have appropriate tools to investigate criminal activity as well as to protect our national security’ expressed the view that ‘that the Bill goes beyond what can be reasonably justified’. \footnote{263} The AHRC then made a number of recommendations related to its concerns about the Bill, as discussed below.

**The data set**

The AHRC, whilst acknowledging the ‘rationale for using regulations’ to define the types of metadata to be retained recommended that definition should be included in the legislation itself, given that the definition ‘is a critical feature of the Bill’. \footnote{264} This has since occurred.

**The definition of ‘content’**

The AHRC expressed its support for the provisions contained in the Bill that ‘explicitly exclude web browsing history and ‘content’ from metadata that must be retained’. \footnote{265} However, it recommended that ‘the Bill be amended to include a definition of ‘content’ for the purposes of the scheme’ \footnote{266} in light of ‘the question of

---

\footnote{256}{Ibid.}
\footnote{257}{Ibid., p. 31.}
\footnote{258}{Ibid., p. 32.}
\footnote{259}{Ibid., p. 33.}
\footnote{260}{Ibid., p. 38.}
\footnote{261}{Ibid., p. 39.}
\footnote{262}{Australian Human Rights Commission (AHRC), *Submission to PJCIS, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, January 2015, accessed 17 March 2015, p. 3.}
\footnote{263}{Ibid., p. 7.}
\footnote{264}{Ibid., p. 8.}
whether the distinction between content and communications data for the purposes of the right to privacy can be legitimately maintained.\footnote{267} This concern remains unaddressed.

**Retention period**

The AHRC noted that in Digital Rights Ireland, the ECJ considered that retention periods should be limited to that which is ‘strictly necessary’ and should differentiate between the usefulness of different types of metadata ‘and tailor retention periods to the objective pursued or the persons concerned.’\footnote{268} After reviewing evidence of the EU regarding the average age of metadata accessed for criminal investigations, it concluded that a retention period of one year ‘would be a more proportionate interference with the right to privacy’, and hence recommended that ‘initial retention period of 1 year be trialled for the first 3 years of the scheme’s operation.’\footnote{269} This recommendation has been rejected and the two year retention period retained.

**Access to retained metadata**

The AHRC noted that in Digital Rights Ireland, one of the reasons why the ECJ considered that the EU-DRD was not a proportionate interference with the right to privacy was because it did not ‘expressly provide that… access and the subsequent use of the data… must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto.’\footnote{270} The AHRC expressed the view that access to metadata ‘should be restricted to sufficiently serious crimes to warrant the intrusion on the right to privacy.’\footnote{271} It also noted that whilst it ‘supports the Bill’s proposal to confine the number of agencies that can access metadata, in its view access to historical metadata ‘should only be allowed where it is reasonably necessary for the prevention, detection or prosecution of defined, sufficiently serious crimes.’\footnote{272} It therefore recommended that PJCIS:

\[
\text{... review the circumstances in which communications data can be accessed and restrict it to circumstances where it is reasonably necessary for the prevention, detection or prosecution of defined, sufficiently serious crimes.}\footnote{273}
\]

As noted previously, items 6J and 6K arguably gives partial effect to this recommendation.

**Office of the Australian Information Commissioner**

The Office of the Australian Information Commissioner (OAIC) provided an extensive and detailed submission to the PJCIS Inquiry into the Bill, and made 18 recommendations. The key issues raised by the OAIC are examined below.

**The proposed data set**

The OAIC expressed a number of concerns about the proposed data set. First, it noted that that the description of the types of metadata in the draft data ‘set may create a risk that types of data that are not intended to be collected and retained under the data retention scheme may be captured’ because the type of metadata ‘are not clearly and narrowly defined.’\footnote{274} Second, the OAIC noted that ‘it is important that clear, specific, consistent and unambiguous language’ is used to define the kinds of information that service providers may be required to collect, and also to describe and define each specific type of metadata in the data set.\footnote{275}

\begin{footnotes}
\item 267. Ibid., p. 11.
\item 268. Ibid., p. 8.
\item 269. Ibid., p. 9.
\item 270. Ibid., p. 9; Digital Rights Ireland at [60].
\item 271. AHRC, Submission to PJCIS, op. cit., p. 9.
\item 272. Ibid., p. 10.
\item 273. Ibid.
\item 274. OAIC, Submission to PJCIS, op. cit., p. 13.
\item 275. Ibid.
\end{footnotes}
Third, the OAIC noted that without further clarification ‘these ambiguities could create... difficulties in compliance for service providers and enforcement for regulators’. As a result, the OAIC recommended that:

[t]he types of telecommunications data that service providers would be required to collect and retain under the proposed data retention scheme should be sufficiently clear and narrowly described to effectively implement the intentions of the scheme.

Privacy impact of the Scheme

In relation to the privacy impact of the proposed Scheme, the OAIC noted:

• the metadata collected would be personal information for the purposes of the Privacy Act 1988

• the collection of metadata is potentially ‘highly privacy intrusive’ because metadata ‘has the potential to create a detailed picture of the individual’s personal life’ and

• the large repository of personal information created by the proposed Scheme would increase ‘the risk and possible consequences of a data breach’ and

• the proposed Scheme would ‘require service providers to handle personal information in a way that may otherwise be inconsistent with those providers’ obligations under the Privacy Act’.

As a result of the above, the OAIC noted that the proposed Scheme ‘has the potential to significantly impact on the privacy of individuals’ and therefore recommended that to mitigate the impact of any data breaches, a mandatory data breach notification requirement be introduced (discussed below).

The Bill has not yet been amended to give effect to this recommendation.

Inadvertent collection of content

The OAIC noted that in its view, it was ‘unclear’ whether the proposed Scheme may ‘in some circumstances’ necessitate the collection of the content of communications ‘in order for service providers to ensure that they comply with their obligations’. It noted that:

... some types of communications are delivered in a way that makes it difficult to distinguish between the content of a communication and information about that communication... [f]or example, in general, internet-based communications are delivered as a single stream of data. I understand that, with respect to unencrypted communications, it is possible to automatically extract telecommunications data from the data stream, making it possible to retain the telecommunications data without also retaining the content. However, it is unclear how service providers will comply with their obligations where the communication has been encrypted. In that scenario, the practical result may be that the service provider retains the entire encrypted communication, including the encrypted content, in order to ensure that they retain the telecommunications data.

As a result, the OAIC again recommended that types of metadata that must be retained ‘should be sufficiently clear and narrowly described to effectively implement the intentions of the scheme’.

Retention period

The OAIC noted that the proposed Scheme will only be necessary and proportionate (and thus not breach Article 17 of the ICCPR) where the metadata is retained for the ‘minimum amount of time necessary’ to meet the needs of Australian national security and law enforcement agencies. The OAIC stated that in its view:
Publicly available evidence, including evidence put forward by Australian enforcement and security agencies, provides some evidence to suggest that a data retention scheme with a retention period of up to one year may be necessary to enable those agencies to investigate serious offences and threats to national security. However, the case for a longer data retention period is less clear. This may be because the Committee has been provided with evidence that supports a longer retention period but which has not been released publicly.  

The OAIC noted that the Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness (SECILE) report *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy* found ‘a lack of quantitative evidence to support the effectiveness of data retention schemes in the European Union’. The OAIC, after examining the evidence provided to the PJCIS Inquiry into the Bill regarding the experience of similar metadata retention schemes in other jurisdictions concluded that:

> ... the experience with similar data retention schemes in international jurisdictions has not produced quantitative evidence that supports the proportionality of a two year retention period.

As a result, the OAIC stated that ‘it is not clear whether a retention period of two years is the minimum amount of time necessary to meet the needs of enforcement and security agencies’ and therefore recommended that:

> Evidence that shows why it is necessary to retain telecommunications data for a minimum of two years should be made available to the public to the extent practicable.

It is worth noting that it appears that the PJCIS heeded the OAIC’s recommendation that it request and consider such evidence, and then ‘communicate to the public that it has considered that evidence, and state the Committee’s conclusions’. It also recommended that the retention period that applies to each type of subscriber related metadata be expressly set out in the Bill.

**Services to be covered**

The OAIC noted that whilst ‘it should be easy to ascertain the types of services to which the scheme applies’ that the broad framing of the regulation-making part of the Bill that deals with prescribing additional services by regulation ‘may result in confusion about what services are intended to be covered’ by the proposed Scheme. The OAIC identified ‘what services that operate ‘over-the-top’ (OTT) of other services that carry communications are covered by the scheme’ as a specific example of such potential confusion. The OAIC, in relation to the prescription of additional services by regulation (discussed below) noted that:

> ... the volume of telecommunications data that is required to be collected and retained under the proposed data retention scheme may depend, to a large extent, on what services are prescribed by the regulations. For example, the inclusion of OTT web-based email services may significantly increase the amount of email telecommunication data that is collected and retained. Further, as technology and communications services evolve, additional services may be prescribed that significantly affect the amount and nature of the telecommunications data collected and retained under the scheme.

As a result, the OAIC recommended that the Bill be amended to clarify when a service provider would ‘be considered to ‘operate infrastructure’ in Australia and what types of communications it is intended will be

---

287. Ibid.
288. Ibid., p. 15.
289. Ibid.
290. Ibid., p. 15.
291. Ibid., pp. 5 and 15.
292. Ibid.
293. Ibid., pp. 6, 16.
294. Ibid., p. 17.
295. Ibid., p. 17.
prescribed by regulations ‘because they are not provided by a carrier, CSP or ISP’. This recommendation has been implemented by item 5 of Part 2 of Schedule 1 of the Bill.

Warrant regime options

The OAIC noted the significant amount of public discussion around whether there is a need for access to metadata to be on the basis of a warrant issued by a court or tribunal. The OAIC stated that whilst it did not ‘advocate for warrant based access in this submission, these concerns require careful consideration.’ As such, in noted that:

The blurring of the distinction between telecommunications data and the content of the communications means that additional oversight is necessary. However, consideration needs to be given to whether a warrant scheme, similar to that which applies to accessing stored communications, is the most appropriate form for this additional oversight to take.

The OAIC suggested that consideration be given to whether a ‘requirement to obtain a warrant on an investigation-by-investigation basis’ would be appropriate, or would impose ‘a disproportionate burden on the ability of enforcement and security agencies to perform their legitimate functions when balanced against the impact on individuals’ privacy.’ In relation to the discussion surrounding so-called ‘generic’ warrants, the OAIC stated that it ‘does not consider that such a generic warrant regime... would provide the necessary level of scrutiny to be effective to increase the current level of oversight of the disclosure of telecommunications data.’ The OAIC concluded that:

... in the absence of a warrant-based access regime, and recognising the changing nature of communications technology and the telecommunications data that it creates, I consider that it is essential that the Bill be amended to limit the purpose for which telecommunications data may be used and disclosed.

The limitations proposed by the OAIC in the absence of a warrant regime for accessing historical metadata are discussed below.

Limiting the use of metadata to serious criminal offences

The OAIC noted that currently an ‘enforcement agency’ may self-authorise access to metadata where it is satisfied that its disclosure is ‘reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue’, and that the Bill would not change this requirement. Further, it noted that ‘there is nothing in’ the TIA Act that prevents an enforcement agency from self-authorising access to metadata ‘where it is satisfied that it is necessary for the investigation of a minor offence’ and that this had been raised as an issue of concern by the PJCHR. The OAIC then recommended that:

Chapter 4 of the TIA Act should be amended to limit the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security. Further, that once an authorisation has been made and information has been disclosed, that the use and further disclosure of that information be limited to the original purpose of the authorisation.

As noted previously, items 6J and 6K arguably gives partial effect to this recommendation.

---

296. Ibid.
297. Ibid., p. 19.
298. Ibid.
299. Ibid., p. 20.
300. Ibid.
301. Ibid.
302. Ibid.
303. Ibid., p. 21.
304. Ibid.
305. Ibid., pp. 7, 21-22.
Definition of enforcement agency

The OAIC supported the amendment proposed by the Bill to the definition of ‘enforcement agency’ to ensure it includes ‘only those bodies with responsibility for investigating or enforcing serious criminal offences’ on the basis that ‘it is appropriate’ that access to metadata ‘should be restricted to bodies with responsibility for investigating serious offences’, given the ‘large volumes of personal information’ that will be stored and public concern about the metadata being used in ‘the investigation of relatively minor offences or civil matters’. 306

Security of retained metadata

The issue of the security of the retained metadata was referred to a number of times in the OAIC’s submission to the PJCIS Inquiry into the Bill. The OAIC noted that:

... the large volume of personal information held by service providers will be an attractive target for people with malicious and/or criminal intent. 307

Whilst the OAIC noted that service providers already have obligations related to their arrangements for the storage and protection of personal information ‘under the Privacy Act or applicable state or territory privacy legislation’ it was important to understand that ‘different service providers may be subject to different levels of oversight in relation to their handling of personal information, including different security standards’. 308

As a result, the OAIC expressed the view that the security measures that protect the retained metadata should be standardised. 309 It welcomed the Government’s indication that the proposed Telecommunications and Other Legislation Amendment Bill will implement reforms relevant to the security of the retained metadata, but noted that it was:

... not aware of that Bill being tabled in Parliament and have not been consulted on a draft version of that Bill. Given the Commissioner’s responsibility for oversight of service providers’ handling of information collected and retained in compliance with the data retention scheme, where those providers are subject to the Privacy Act, I would welcome the opportunity to provide input into the development of any additional security obligations. 310

Further, the OAIC noted that the Bill does not prescribe how the metadata collected ‘is to be stored or any specific security standards that service providers must implement to ensure... [it] is adequately protected’. 311

Additionally, the OAIC noted that the Bill also fails to include ‘any mechanism for prescribing’ such security standards or requirements. 312 As a result the OAIC recommended that the Bill be amended to include:

• a mandatory data breach notification requirement that applies to services providers 313 (this has not yet occurred)

• a requirement that implementation plans include details of the measures that will be taken by the service provider to ensure that metadata collected and retained under the plan is protected from misuse, interference and loss and from unauthorised access, modification and disclosure 314 (provided by proposed section 187BA) and

• require the CAC ‘to assess the steps that the service provider proposes to take’ to protect the metadata from ‘misuse, interference and loss and from unauthorised access, modification and disclosure’ (provided by proposed paragraphs 187E(2)(a) and (b)). 315

Finally, the OAIC noted that in its view:

306. Ibid., p. 22.
307. Ibid., p. 10.
308. Ibid., 35.
309. Ibid., p. 35.
310. Ibid., p. 35.
311. Ibid., pp. 34-35.
312. Ibid., p. 35.
313. Ibid., pp. 10-11, 28-29.
314. Ibid., p. 25.
315. Ibid., p. 25.
... while I support the establishment of a security framework for the telecommunications sector, I consider that this framework should be in place before service providers are required to collect and store any information under the proposed data retention scheme (or an approved data retention implementation plan). If this is not possible, my recommendation that the Bill be amended to require a service provider’s data retention implementation plan to specify, in relation to each service, the steps that the provider will take to protect the information become essential.\textsuperscript{316}

\textit{Mandatory data breach notification}

As noted above, the OAIC recommend that the Bill be amended to impose a mandatory data breach requirement on service providers. The rationale for this recommendation put forward by the OAIC was:

- the proposed data retention scheme would require service providers to collect and retain a large volume of information, including personal information, and that this has the potential to be highly intrusive
- the collection and retention of that information had the potential to reveal a detailed picture of a person’s personal life and therefore metadata retained under the scheme is likely to be a target for people with malicious or criminal intent and
- therefore in event of a security breach resulting in unauthorised access to or disclosure of telecommunications data, affected individuals would face increased risks of identity theft, fraud, harassment or embarrassment.\textsuperscript{317}

The OAIC noted that there ‘has been an upward trend in the voluntary notification of data breaches to our office’ that is ‘consistent with national and global trends that also reflect an increase in the number and severity of data breaches.’\textsuperscript{318} Further the OAIC noted that:

\begin{quote}
... Australian service providers have experienced significant issues in handling and keeping personal information secure. Major telecommunications services providers that will be covered by the scheme are amongst the 20 entities most complained about to our office.\textsuperscript{319}
\end{quote}

As a result of the above, the OAIC stated that in its view, a mandatory notification requirement is an ‘important mitigation strategy’ that can ‘enable individuals to take steps to reduce their exposure to risks, which cannot be taken by other entities’ (for example, cancelling credit cards).\textsuperscript{320} Therefore the OAIC recommended that the Bill should be amended to include, in the event of a serious data breach, an obligation for service providers to notify:

- the Commissioner, and
- affected individuals, where
- other appropriate conditions are met (such as where the data breach could give risk to a real risk of serious harm to affected individuals).\textsuperscript{321}

Further, the OAIC noted that the possibility of a mandatory notification requirement had been previously raised by the Australian Law Reform Commission in 2008, and was introduced in 2012 in relation to the unauthorised collection, use or disclosure of health information included in a consumer’s eHealth record under the \textit{Personally Controlled Electronic Health Records Act 2012}.\textsuperscript{322} Such an amendment has not yet been made.

\textit{Providing individuals with access to their metadata}

The OAIC noted the concerns of some service providers regarding the ‘impact that the proposed data retention scheme may have on their existing obligation under the \textit{Privacy Act 1988} to provide individuals with access to
their personal information. The OAIC noted that currently APP 12 requires organisations bound by the Privacy Act 1988 to ‘give an individual access to any personal information that the provider holds about the individual on request, subject to certain exceptions. The OAIC concluded, that despite the concerns expressed, ‘APP 12 provides a balanced approach to ensuring individuals are able to gain access to their personal information whilst also recognising the operational requirements of organisations. Proposed section 187LA gives effect to this recommendation.

Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) provided a submission to the Inquiry which noted that the IGIS does not have a role in relation to metadata retained by carriers, but does have an interest in the information accessed and retained by ASIO. Where the Bill will require certain carriers and internet service providers to keep prescribed metadata for two years, ASIO will continue to be able to access that metadata under the current arrangements in the TIA Act. The Inspector-General of Intelligence and Security Act 1986 (the IGIS Act) provides sufficient authority for the IGIS to continue oversight of ASIO access to telecommunications data.

Data which will be accessible to ASIO

The IGIS noted that while the proposed amendments set minimum data retention requirements, telecommunications providers may retain data which exceeds this minimum set for business, cost efficiency or other reasons. Any additional data retained will be accessible by ASIO under an authorisation.

The length of time ASIO may retain data

Once ASIO has lawfully obtained telecommunications data from a carrier or carriage service provider there is no statutory requirement for ASIO to either delete the data or to make an active decision as to whether the material is, or continues to be, relevant to security.

Industry - Optus

Optus provided the Inquiry with a detailed submission, as well as two confidential supplementary submissions. The Optus detailed submission contained 18 recommendations chiefly relating to the draft data set, implementation aspects of the proposed scheme and the likely burden on industry. The key issues raised are examined below.

The proposed data set

Optus considered that the proposed data set is basically workable, but that an appropriate level of detail and interpretive guidance should be made available. Optus recommended that a draft of the regulation describing the data set definitions be made available as soon as possible, to assist the Committee and the Parliament’s consideration of the Bill, and further consideration of cost and implementation issues by the industry.

Optus recommends that to ensure that service providers are not required to keep information about a subscriber’s web browsing history, proposed section 187A(4)(b) should be amended to specifically exclude the collection of origin IP packet address details.

Optus also recommended that the data set prescribed in regulations be stable for the initial three year period of operation so that the Committee’s review can be based on a stable and known set of parameters in place and able to be used by law enforcement and national security agencies for this workable period.

Optus recommended that parameter 1 of the draft data set should be clarified to remove potential replication of records and to make it clear that the data retention regime does not require retention of customer passwords.

323. Ibid., p. 36.
324. Ibid., p. 36.
325. Ibid., p. 36.
326. Inspector-General of Intelligence and Security (IGIS), Submission to PJCIS, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 21 January 2015, accessed 18 March 2015, p. 3
Optus noted that service providers may have no visibility of specific device connections or connection activity at the end user level. Optus recommended that the data set obligations be adjusted to only require collection of information relating to events that the access service provider can reasonably control, rather than elements which are more directly related to actions that end users take and which providers have no easy method of determining at all, or only via detailed packet inspection of the content of a communication.

Optus recommended that the data set be adjusted to reflect the fact that some service providers will have no location information available to them and that in these circumstances the obligation at proposed subsection 187A(6) to ‘create’ such data should not apply.

The length of time data should be retained
Optus noted that a small quantity of data set elements, mainly those related to service usage, are likely to create a high volume of data and be major contributors to the overall IT storage costs for data retention. Optus considered that it would be useful for the regulations to be able to prescribe an alternative shorter period (than the two year period specified in proposed paragraph 187C(1)(b)) for keeping information for certain services or in relation to certain service related matters.

Implementation plans and compliance
Optus is concerned that post implementation disputes about interpretation and capability could result in a provider which had successfully executed against an approved implementation plan being subject to compliance risk or jeopardy.

Optus therefore recommended that the effect of a data retention implementation plan be expanded to play a central role in any compliance or interpretive dispute in the initial three year period of the data retention scheme. Optus also recommended that the CAC be afforded a role to investigate and issue an opinion or certificate which would be considered prima facie evidence of the compliance by the service provider with proposed subsection 187A(1).

Cost of the scheme (and who should bear it)
Noting the likely substantial capital and compliance costs, Optus recommended that the Government should make a substantial contribution to costs incurred by providers in implementing data retention obligations. Optus also recommended that the effectiveness of Division 3 can be improved if guidance is added for the Communications Access Co-ordinator to positively exercise powers to initiate of his or her own volition the consideration of exemptions or variations to obligations in situations that may reduce the ‘financial and administrative burdens on participants in the Australian telecommunications industry’. This threshold is consistent with the Regulatory Policy at section 4 of the Telecommunications Act 1997.

Financial implications
The Bill’s Replacement Explanatory Memorandum states that the ‘Bill will have financial impacts on service providers who will be required to meet the new minimum data retention obligations’. However, despite acknowledging that the Government will make ‘a substantial contribution’ to the costs of implementing and operating the Scheme, the Replacement Explanatory Memorandum is silent as to the financial implications for the government.

PJCIS Report
The PJCIS had previously recommended that ‘costs incurred by providers should be reimbursed by the Government’. The PJCIS noted that (as part of its 2013 inquiry) it had received estimates from relevant service providers about the potential cost of implementing a metadata retention scheme, which, at that time, were premised on the assumption that the retention of web browsing histories would be mandated and hence would

---

have involved the collection and retention of ‘a stupendous volume of data’ (the Bill does not mandate retention of web browsing histories, but does not prohibit it either).\textsuperscript{331}

Those estimates, made in 2012 and – importantly –made without the benefit of considering a proposed data set having or draft legislation - ranged between $400 million to $700 million.\textsuperscript{332} Hence, the PJCIS noted that they ‘do not necessarily reflect the cost’ of the proposed Scheme, as presented by the Bill and proposed data set.\textsuperscript{333} For example, the proposed Scheme mandates the collection of IP address allocation records (instead of web browsing histories) which the PJCIS noted can be collected and retained for very little cost.\textsuperscript{334}

### Estimated cost as noted by the PJCIS

After examining the differences underlying the costs estimates it received as part of its 2013 Inquiry to the current costs estimates, the evidence provided by witnesses to the inquiry and view put by submitters, the PJCIS noted:

- the upfront capital costs required to ensure compliance with the proposed Scheme will cost the relevant service providers between $188.8 million and $319.1 million\textsuperscript{335}
- reducing the retention period from two years to 12 months would only have a ‘modest impact’ that may result in a ‘decrease the cost of the scheme by only five to six percent’\textsuperscript{336}
- there were concerns that the proposed Scheme would ‘impose disproportionate costs for smaller service providers’ who may have ‘limited capacity to absorb any significant capital expenses’ and thus could have an ‘anti-competitive impact’\textsuperscript{337}
- relevant service providers generally argued that the cost of complying with the proposed Scheme should be funded by Government\textsuperscript{338}
- without Government funding, relevant service providers are likely to pass on some of all of the costs incurred as a result of complying with the proposed Scheme to consumers\textsuperscript{339} and
- currently, relevant service providers are entitled to recover the actual costs they incur when complying with a metadata authorisation on a ‘no cost, no profit’ basis.\textsuperscript{340}

After considering the above, the PJCIS concluded that it may not be in the public interest for the Government to fully fund the costs of implementing the proposed Scheme for two main reasons. First ‘as a number of service providers have acknowledged’ the telecommunications services offered enable ‘serious criminal activity and threats to national security’ and hence there ‘is an argument that service providers should bear some of the cost of addressing these external harms’ that their services facilitate.\textsuperscript{341} Second, there is ‘a strong economic argument’ that costs of complying with the proposed Scheme ‘should be borne by the party best able to mitigate’ them. It is argued that ensuring that the relevant service providers bear some of the cost of complying with the proposed Scheme will impose a ‘degree of cost discipline’ which would ameliorate the risk of some service providers ‘gold plating’ their compliance solutions (instead of developing efficient or technically innovative solutions) as has been experienced in other sectors.\textsuperscript{342}

\textsuperscript{331} PJCIS, \textit{Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014}, 27 February 2015, p. 174, para [5.92] and p. 175, para [5.94].
\textsuperscript{332} Ibid., p. 175, para [5.92].
\textsuperscript{333} Ibid., para [5.94].
\textsuperscript{334} Ibid., p. 176, para [5.95].
\textsuperscript{335} Ibid., p. 177, para [5.104].
\textsuperscript{337} PJCIS, \textit{Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014}, 27 February 2015, p. 178, paras [5.106] and [5.108].
\textsuperscript{338} Ibid., p. 180, para [5.112].
\textsuperscript{339} Ibid, para [5.113].
\textsuperscript{340} Ibid., p. 182, para [5.119].
\textsuperscript{341} Ibid., p. 182, para [5.124].
\textsuperscript{342} Ibid., p. 183, para [5.123].
PJcis Recommendation
As a result, the PJcis recommend that ‘the Government make a substantial contribution to the upfront capital costs of service providers implementing their data retention obligations’.343 More specifically it also recommended that the model for funding service providers’ capital costs associated with complying with the proposed Scheme:

• provides sufficient support for smaller service providers
• minimises any potential anti-competitive impacts or market distortions
• provides appropriate incentives for service providers to implement efficient solutions to data retention
• does not result in service providers receiving windfall payments to operate and maintain existing, legacy systems and
• takes into account companies that have recently invested in compliant data retention capabilities in anticipation of the Bill’s passage.344

Unresolved issue: on-going cost
As noted by the PJcis, currently section 314 of the Telecommunications Act 1997 provides that Australian service providers are able to recover the costs of complying with metadata authorisations on a ‘no profit, no loss’ basis.345 Given that the goal of the proposed Scheme is to ensure that metadata sought by national security and law enforcement agencies is consistently available when requested, it would appear logical to assume that:

• agencies will be able to access metadata on a more frequent basis and
• thus will incur greater costs as a result of having to consistently pay the service providers costs for complying with metadata access authorisations.

However, no information or modelling detailing forecast increases to the operating costs of national security and law enforcement agencies as a result of the above appears to have been released. As a result, the on-going financial costs of the proposed Scheme remain an unresolved issue.

Does the Cybercrime Convention prevent metadata being used only in relation to serious offences?
In its 2015 Report, the PJCHR rejected the Attorney-General’s reasoning that the Cybercrime Convention prevents Australia from limiting access to metadata to instances where it is required to investigate serious crimes or serious matters on the basis that:

• any obligations under the Convention on Cybercrime ‘must be considered against Australia’s obligations under the ICCPR in relation to the right to privacy, and in particular that any limitations on the right to privacy are required to be proportionate’346 and
• that, in its view, ‘it would be unusual if precedence were to be given to a Council of Europe Convention on Cybercrime above Australia’s obligations under international human rights law.’347

In relation to the second point, in evidence before the PJcis Inquiry into the Bill the President of the Australian Human Rights Commission, Professor Gillian Triggs noted that:

A final point I want to make is a matter that has come up relatively recently—so we are perhaps all novices in this area—and that concerns the Council of Europe's Convention on Cybercrime. This is a convention of 2001, and Australia is a party to it. There is an obligation to allow access to what is stated to be specific criminal conduct. It does not say what specific criminal conduct is, but that is not relevant for the moment. There is a core obligation under that convention to allow access, and that is being used as a reason for permitting access in a way that can breach human rights. That is our concern. What I want to draw to your attention, if I may, is that article 15 of that convention specifically provides that the obligation to allow access for the purposes of specific criminal activity is

343. Ibid., p. 184, recommendation 16.
344. Ibid.
347. Ibid., p. 58, para [1.204].
subject to human rights protections and, in particular, is subject to the International Covenant on Civil and Political Rights. (emphasis added)

The PJCHR expressed a similar view to that outlined above (based on observations of the actions taken by EU-member parties to the Convention on Cybercrime in response to the ECJ’s decision in Digital Rights Ireland). Specifically it noted that one of the reasons the EU-DRD was struck down by the ECJ was because it was a disproportionate interference with the right to privacy and:

One of the reasons that scheme was held to be disproportionate was that it did not include any objective criteria to ensure that only competent national authorities could access retained data, and could then only use it for the prevention, detection or criminal prosecution of offences that, given the extent and seriousness of the scheme’s interference with the fundamental human rights in question, may be considered to be sufficiently serious to justify such interference. The committee notes that EU members are required to take necessary measures to comply with the framework set out by this judgement. (emphasis added).

As a result, the PJCHR concluded that ‘any obligations upon parties to the Convention on Cybercrime are not determinative of the compatibility of the proposed data retention scheme with the right to privacy’ (a view, as noted above, that appears to be supported by the President of the Australian Human Rights Commission). For the reasons outlined below, it appears that this view is correct.

The Cybercrime Convention’s main goal is to establish a ‘common criminal policy’ to protect society against and combat computer-related or cybercrimes globally through criminalising such acts and harmonising national legislation, enhancing law enforcement and judicial capabilities, adopting powers sufficient for effectively combating such criminal offences, and facilitating co-operation in their detection, investigation and prosecution at both the domestic and international levels. To meet its object the Cybercrime Convention provides for surveillance methods such as interception and data preservation.

**Data preservation versus data retention**

As one commentator has pointed out, it is important to distinguish between data preservation and data retention.

Data preservation normally refers to and would require that ‘during the normal course of a criminal investigation, law enforcement agencies would be enabled to instruct an internet service provider (ISP) to put aside specified data that is already in the ISP’s possession until legal authorisation for disclosure has been obtained.’ Thus the ISP is only under an obligation ‘to preserve the data in storage if requested to do so by a law enforcement body in relation to a specified data relating to a particular case.’

Data retention refers to the collection and storage of all or a large portion of data traffic as a routine blanket matter. The Cybercrime Convention provides for the request for preservation and disclosure of stored data and for the preservation of data for a maximum period of up to 90 days. However it contains no mandatory data retention obligation.

---

348. Professor G. Triggs (President, Australian Human Rights Commission), Evidence to Parliamentary Joint Committee on Intelligence and Security (PJCS), Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 29 January 2015, p. 71.
349. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General [C-293/12 & C-594/12] [2014] [ECJ], (Digital Rights Ireland).
351. Ibid., p. 59, para [1.205].
354. Ibid.
355. Ibid.
356. Ibid.
357. Ibid.
358. Ibid.
Australia’s obligations under the Cybercrime Convention

A reading of the Cybercrime Convention beyond Article 14(2) provides an enhanced understanding of the nature and scope of Australia’s obligations under the Cybercrime Convention. The obligation imposed by Article 14(2) to cooperate extends not only to the crimes established in the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offence.\(^\text{359}\) The Explanatory Report to the Cybercrime Convention states:

... the general scope of the obligation to co-operate is set forth in Article 23: co-operation is to be extended to all criminal offences related to computer systems and data (i.e. the offences covered by Article 14(2)), as well as to the collection of evidence in electronic form of a criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable.

However, it should be noted that Articles 24 (Extradition), 33 (Mutual assistance regarding the real time collection of traffic data) and 34 (Mutual assistance regarding the interception of content data) permit the Parties to provide for a different scope of application of these measures.\(^\text{360}\)

Article 14(1) of the Cybercrime Convention limits the scope of procedural powers by requiring that such powers are ‘for the purpose of specific criminal investigations and proceedings’. The Explanatory Report to the European Convention clarifies for States parties that the power and procedures under the Cybercrime Convention are limited to use for ‘an investigation in a particular case’.\(^\text{361}\) [Emphasis added]

Limits on Australia’s obligations under the Cybercrime convention

Article 15 requires that all powers and procedures must be subject to conditions that provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations undertaken under the ICCPR (to which Australia is a party), and other applicable international human rights instruments, and which incorporate the principle of proportionality and, among other things, the right against self-incrimination, access to legal privileges, and the specificity of individuals or places which are the object of European Convention measures.\(^\text{362}\)

Article 15(2) specifies that this includes independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. The Explanatory Report clarifies that State parties are expected to apply ‘principles of their law, such as limitations on over breadth of production orders and reasonableness requirements for searches and seizures’ and that:

National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards.\(^\text{363}\)

Also, ‘the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.’\(^\text{364}\)

Conclusion: restricting the disclosure or use of metadata to serious offences is permitted

In response to its concerns about the data retention period and the types of offence which metadata could be used to investigate outlined above, the PJCHR recommended that to avoid the disproportionate limitation on the right to privacy that would result from a two year mandatory data retention and allowing metadata to be used in the investigation of any offence, the Bill be amended to limit disclosure authorisation for existing metadata to instances where:

\(^{359}\) Article 23, Conventti on on Cybercrime, opened for signature Budapest 23 November 2001, ETS No. 185 (entered into force 1 July 2004).
\(^{360}\) Explanatory Report to the Convention on Cybercrime, ETS No. 185, paragraph 243.
\(^{361}\) Ibid, paragraphs 146 and 147.
\(^{362}\) Ibid., paragraph 147.
\(^{363}\) Ibid., paragraph 146.
\(^{364}\) Ibid., paragraph 146.
• it is **reasonably necessary** for the investigation of specified

• for the investigation of specified **serious crimes, categories** of serious crimes or the investigation of **serious matters** by the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO) and the Australian Competition and Consumer Commission (ACCC). ³⁶⁵

In this regard, the above recommendation was similar to recommendation 25 made by the PJCIS. However, the PJCIS did not directly link its recommendation that the Bill be amended to require that an officer authorising access to metadata must ‘have regard to... the gravity of the conduct being investigated, including whether the investigation relates to a serious criminal offence’ to the appropriateness of the two-year retention period in the same way that the PJCHR did. ³⁶⁶

Nonetheless the PJCIS’s recommendation reinforces the view that appropriate access thresholds are a key tool that can be used to ensure the proposed Scheme does not impose a disproportionate limitation on the right to privacy that would result from a mandatory two year retention period, and therefore breach Australia’s international human rights obligations.

Article 15(2) clearly foreshadows that signatories can impose certain conditions and safeguards on procedures or powers enacted to give effect to the Cybercrime Convention (for example, the power to disclose metadata to foreign law enforcement agencies). The use of the phrases ‘grounds justifying application’ and ‘limitation of scope... of such power of procedure’ clearly encompass developing criteria or grounds that justify the disclosure of metadata or otherwise limit access to it or the uses to which it can be put.

In addition, given that Article 15(1) clearly provides that the principle of proportionality applies to the obligations imposed by the Cybercrime Convention (and proportionality can be resolved by reference to the purposes for which the data is used), it would appear that the view that the Cybercrime Convention does not actually prevent Australia from imposing threshold limitations on access to (or use of) metadata such as those proposed by the PJCHR is correct. Indeed it could be argued that they not only foreshadow such restrictions, but specifically allow them.

**Statement of Compatibility with Human Rights**

A detailed and thorough Statement of Compatibility with Human Rights can be found at pages 5 to 31 of the Replacement Explanatory Memorandum to the Bill. As required under Part 3 of the **Human Rights (Parliamentary Scrutiny) Act 2011** (Cth), the Government has assessed the Bill’s compatibility with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of that Act. The Government considers that the Bill is compatible.

The view that the Bill as originally drafted (and as amended) is compatible with key human rights is not without controversy. As detailed above, key interest groups, stakeholders and Parliamentary Committees have stated that in their view, the Bill as originally drafted imposed (amongst other things) a disproportionate limitation on the right to privacy. Further, it is arguable that even with the amendments made in the House of Representatives, the Bill still imposes a disproportionate limitation on the right to privacy and fails to give effect to the right to a remedy.

**Key issues and provisions**

The analysis below is based on the Bill as amended in the House of Representatives on 19 March 2015, rather than the Bill as drafted.

**Schedule 1, Part 1: Data Retention**

Proposed amendments made to the **TIA Act** include the insertion of proposed Part 5-1A – **Data retention**. This Part will require service providers to keep certain information and documents (metadata) for a specified period.

**Obligation to retain metadata**

Proposed section 187A will require a service provider to keep or cause to be kept, information of a kind (or documents containing information of that kind) specified ‘in or under’ proposed section 187AA. Proposed


paragraph 187A(3) provides that the metadata retention obligations will apply to a service if it is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy (or both) and:

• it is operated by a carrier or internet service provider and
• the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services.

Importantly however, proposed paragraph 187A(3)(b)(iii) provides that the metadata retention obligations will also apply to any service for which a declaration made by the Attorney-General under proposed section 187A(3A) is in force, as discussed below under the heading ‘Service declaration power’.

Definition of metadata to be retained

This section was amended to reflect the concerns, noted earlier in this Digest, that the Scrutiny Committee, PJCIS and PJCHR expressed about using regulations to define the metadata that must be retained. The table in proposed section 187AA sets out the kinds of information that a service provider must retain (or cause to be retained) under proposed subsection 187A(1). The types of metadata set out in the table in proposed subsection 187AA(1) (the data set) are identical to the first two columns of proposed data set as amended by Industry Working Group (IWG), with the exception of the addition of some explanatory notes (discussed below). The PJCIS noted that in relation to the proposed data set as amended by the IWG:

A number of service providers assured the Committee that the level of detail provided in the Government’s proposed data set, in conjunction with the information provided through the IWG process, was sufficient for them to design and implement a data retention system.

The types of metadata included in the data set are described as being ‘categories of information’ that are of ‘significant utility to law enforcement and national security investigations’ and hence are ‘critical data they require to safeguard national security and prevent or detect criminal activity’. The types of metadata that will be required to be retained are detailed below.

Subscriber, account, service and device information relating to the relevant service

Table item 1 in proposed subsection 187AA(1) deals with subscriber, account, service and device information. It requires service providers to retain information such as the name and address of a subscriber, billing or payment information, contact information and any identifiers that relate to the service or account such as the unique number attached to a mobile phone or the IP address allocated to an internet access account or service.

In relation to these types of metadata, the PJCIS stated that it accepted:

... that requiring service providers to retain each of the types of subscriber information set out in the proposed data set, subject to the IWG’s recommended amendments, is necessary and proportionate for the purposes of safeguarding national security and the enforcement of the criminal law.

The source of a communication

Table item 2 in proposed subsection 187AA(1) deals with the source of communications. It requires service providers to retain identifiers for the source of a communication. Examples include a phone number from which a call or SMS was made, identifying details of an account, service or device (for example a username), IP

---

369. PJCIS, Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 82, para [3.43].
addresses and port numbers or other device or service identifiers that uniquely identifies the source of a communication.373

The destination of a communication

Table item 3 in proposed subsection 187AA(1) deals with destination of communications. It requires service providers to retain identifiers of the account, service or device to which a communication has been (or was attempted to be) sent, forwarded, routed or transferred. Examples include a phone number which received a call or SMS, identifying details of an account, service or device (for example a username), IP addresses and port numbers or other device or service identifiers that uniquely identifies the recipient of a communication.374 The Supplementary Explanatory Memorandum notes that this ‘explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed.375

The date, time and duration of a communication, or of its connection to a relevant service

Table item 4 in proposed subsection 187AA(1) deals with the date, time and duration of a communication (or connection to a relevant service). It requires service providers to retain date and time information (including the time zone) of a communication with sufficient accuracy to identify the start and end of the communication, or the connection and disconnection from the relevant service.376

The type of a communication or of a relevant service used in connection with a communication

Table item 5 in proposed subsection 187AA(1) deals with the type of communication or relevant service used in connection with a communication. It requires service providers to retain metadata that enables the identification of the type of communication (for example, SMS or MMS messages), the type of the relevant service (for example, VoIP or GPRS) and the features of relevant service that were (or would have been) used by or enabled for the communication (for example, call forwarding, data volumes etc.).

The note to Table item 5 in proposed subsection 187AA(1) clarifies that this item will only apply to the service provider operating the relevant service, as per proposed paragraph 187A(4)(c) and hence ensures that service providers are only required to retain metadata to the extent that it is available to them. This ensures that service providers are not required to keep metadata about communications that are carried or enabled by means of services that they themselves do not provide (that is, that passes ‘over the top’ of the service they provide). As a result, Table item 5 reflects recommendation 6 of the PJCIS Report.377

The location of equipment, or a line, used in connection with a communication

Table item 6 in proposed subsection 187AA(1) deals with the location of equipment or a line used in connection with a communication. It requires service providers to retain location-related metadata such as the location of the equipment or line at the start and end of a communication.378 In relation to the level of location detail required to be retained, the Supplementary Explanatory Memorandum notes that:

Service providers will not be required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the locations records to be kept by service providers will not allow continuous monitoring or tracking of devices.379

379. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 21, table item 6, column 3.
Examples provided in table include cell towers and Wi-Fi hotspots. As noted by the PJCIS, retaining this type of metadata is particularly controversial as reflected by the fact that ‘a number of submissions’ called ‘for location information to not be retained as part of any data retention regime.’ However, the PJCIS concluded that it:

... accepts that requiring service providers to retain each of the types of subscriber information set out in the proposed data set, subject to the IWG’s recommended amendments, is necessary and proportionate for the purposes of safeguarding national security and the enforcement of the criminal law…. [t]he Committee acknowledges that location records are a sensitive category of telecommunications data included in the proposed data set. The Bill and proposed data set significantly curtail the detail and frequency of the location records that service providers would be required to retain.  

Metadata definition declaration power

Proposed subsection 187AA(2) provides the Attorney-General with the power to modify the data set, and hence define the metadata to be retained by service providers. However, this power it is subject to a number of limitations set out in proposed subsections 187AA(3)-(5).

Reflecting recommendation 3 of the PJCIS Report, proposed subsection 187AA(3) provides that such declarations are only in effect for 40 sittings days of either House of Parliament.  

The PJCIS had originally recommended that the Bill be amended to provide that in circumstances where a declaration extending the metadata retention obligations to a class service provider was made ‘legislation should be brought before the Parliament before the expiry of the 40 sitting days’. In other words, the PJCIS sought to link such declarations to the subsequent introduction of an amending Bill and resulting formal Parliamentary processes and considerations.

The amended Bill does directly not address that aspect of the PJCIS’s recommendation. Put simply, there is no requirement that a Bill reflecting the declaration must (or even should) be introduced to the Parliament (noting that the PJCIS couched their recommendation in discretionary terms). This gives the Government discretion as to whether to proceed with the decalred amendment to the data set on a permanent basis. Clearly, if the Government does not introduce a Bill reflecting the amendments made by the determination, those amendments will lapse after 40 sitting days.

Proposed subsection 187AA(4) provides that ‘if’ a Bill seeking to amend proposed subsections 187A(4), 187AA(1) (which includes the table that contains the data set) or 187AA(5) is introduced the Parliament, proposed subsection 187AA(4) provides that the Minister:

• must refer the Bill to the PJCIS for review and
• the PJCIS must be provided a minimum of 15 sitting days of a House of Parliament after the introduction of the Bill to report on its review of such a Bill.

Again, the Bill differs slightly from the PJCIS recommendation in that it had recommended that such amendments ‘should’ (rather than ‘must’) be referred to the PJCIS for review and report. However, viewed as a whole, proposed subsections 187AA(2) to (5) balances the Attorney-General power to define types of metadata that must be collected and retained via declarations (thus ensuring the proposed Scheme is flexible and responsive to changes) with the desire of Parliament to be able to fulfil its law-making and oversight functions (as well as providing greater clarity around what constitutes ‘infrastructure’) in response to recommendations 2 and 3 in the PJCIS Report.

381. Ibid., pp. 96-97, paras [3.91-3.92].
384. Ibid.
Service declaration power

Proposed subsections 187A(3A) to (3C) allow the Attorney-General to declare that the metadata retention obligations created by the Bill apply to additional services not covered by proposed section 187A(3). Whilst the declaration power appears broad, it is constrained somewhat by the requirements imposed by proposed paragraphs 187A(3)(a) and (c); namely that such a service must:

- be a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both and
- the person operating the service must own or operate, in Australia, infrastructure that enables the provision of any of its relevant services.

Proposed subsection 187A(3B) reflects recommendation 14 of the PJCIS Report and provides that such declarations will only be in effect for 40 sittings days of either House of Parliament. However, the PJCIS also recommended that the Bill be amended to provide that in circumstances where a declaration extending the metadata retention obligations to a class of service provider was made ‘legislation should be brought before the Parliament before the expiry of the 40 sitting days’. In other words, the PJCIS sought to link such declarations to the subsequent introduction of an amending Bill and resulting formal Parliamentary processes and considerations.

The amended Bill does directly not address that aspect of the PJCIS’s recommendation. Put simply, there is no requirement that a Bill reflecting the declaration must (or even should) be introduced to the Parliament (noting that the PJCIS couched their recommendation in discretionary terms). This gives the Government discretion as to whether to proceed with the declaration of the service on a permanent basis. Clearly, if the Government does not introduce a Bill reflecting that declaration, it will lapse after 40 sitting days.

Proposed subsection 187A(3C) provides that ‘if’ a Bill seeking to amend proposed subsection 187A(3) is introduced the Parliament, proposed subsection 187A(3C) provides that the Minister:

- must refer the Bill to the PJCIS for review and
- the PJCIS must be provided a minimum of 15 sitting days of a House of Parliament after the introduction of the Bill to report on its review of such a Bill.

Again, the Bill differs slightly from the PJCIS recommendation in that it had recommended that such amendments ‘should’ (rather than ‘must’) be referred to the PJCIS for review and report. As noted above, some concerns about the clarity of proposed subsection 187A(3) was expressed by the PJCIS and some interest groups. In particular, there was a view that the Bill should be amended to define the term ‘infrastructure’ in greater detail, and thus clarify when a service provider would ‘be considered to ‘operate infrastructure’ (and hence be bound by the metadata retention obligations).

Those concerns have been addressed by item 5 of Part 2 of Schedule 1 of the Bill, which defines ‘infrastructure’ as ‘any line or equipment used to facilitate communications across a telecommunications network’. Importantly, section 5 of the TIA Act defines ‘line’ by reference to the Telecommunications Act 1997, which in turns defines it as ‘a wire, cable, optical fibre, tube, conduit, waveguide or other physical medium used, or for use, as a continuous artificial guide for or in connection with carrying communications by means of guided electromagnetic energy’.

The Government argues that the effect of introducing the definition of ‘infrastructure’ is to ensure that:

---

386. Ibid.
387. Ibid.
388. Ibid.
Servers used to operate an ‘over the top’ service such as VoIP would fall within the definition of infrastructure. However, ‘infrastructure’ is not intended to include business premises. For example the headquarters of a company, taken in isolation, would not satisfy the definition of ‘infrastructure’.390

Viewed as a whole, proposed subsections 187A(3A) to (3C) and item 5 of Part 2 of Schedule 1 of the Bill balances the Attorney-General’s power to define the type of service providers that must collect and retain metadata via declarations (thus ensuring the proposed Scheme is flexible and responsive to changes) with the desire of Parliament to be able to fulfil its law-making and oversight functions (as well as providing greater clarity around what constitutes ‘infrastructure’) in response to recommendations 11 and 14 in the PJCIS Report.

Application of the proposed scheme to ‘over the top’ services

Proposed paragraph 187A(4)(c) ensures that service providers are only required to retain metadata to the extent that it is available to them. This ensures that service providers are not required to keep metadata about communications that are carried or enabled by means of services that they themselves do not provide (that is, that passes ‘over the top’ of the service they provide). As a result, proposed paragraph 187A(4)(c) reflects recommendation 6 of the PJCIS Report.391

No requirement to retain content

Of significance is an exclusionary subsection, proposed subsection 187A(4) which outlines that a service provider is not required to keep information that contains the ‘contents or substance of a communication’.392

Amongst other things, the section puts beyond doubt that service providers are not required to keep information about the content or substance of a communication or subscribers’ web browsing history.393 There is also explicit clarification by proposed subsection 187A(5) that attempted communications are taken to be sent communications. This might include an unanswered phone, a destination mobile being switched off, and free or ‘unlimited’ internet, apps or phone calls. These are communications for data retention purposes (proposed paragraph 187A(5)(b)).

Importantly however, the Bill does not prevent service providers from collecting web browsing histories. Further, due to the ambiguity surrounding the definition of metadata in the TIA Act, the Bill does not resolve the issue of national security authorities or enforcement agencies potentially accessing web-browsing histories or other types of metadata that some consider to be ‘content’.

Certain services exempted from metadata retention obligations

Proposed section 187B will exclude entities such as governments, universities and corporation from the requirement to retain metadata on their own internal networks, and also ensures that business such as cafes offering free Wi-Fi are not required to retain metadata.

Proposed subsection 187B(2) provides that the CAC may declare that proposed subsection 187A(1) applies to a service that would otherwise be excluded, and hence the metadata retention obligations will apply to that service. As noted by the PJCIS, a number of submissions to its Inquiry raised both concerns about this power and the exclusion of certain Wi-Fi services from the metadata retention obligations. As a result, the PJCIS recommended that the Bill 2014 be amended to:

• require the CAC to consider the objects of the Privacy Act 1988 when considering whether to make a declaration under proposed subsection 187B(2), and, if there is any uncertainty or a need for clarification, consult with the Australian Privacy Commissioner on that issue before making such a declaration and

390. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 36, para [158].

391. Attorney-General’s Department (AGD), Report 1 of the Data Retention Implementation Working Group, op. cit., Attachment A, p. 4; Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 15, para [60].


393. Notes to proposed paragraphs 187A(4)(a) and (b).
• require the CAC to notify the PJCIS of any declaration made under proposed subsection 187B(2) as soon as practicable after it is made.  

Proposed subsection 187B(2A) and paragraph 187B(3)(ba)-(bb) implement that recommendation and provide that prior to making a declaration, the CAC ‘may consult the Privacy Commissioner’ and, if that occurs, ‘must have regard to... any submissions made by the Privacy Commissioner because of the consultation under subsection 2A.’

The PJCIS recommended that the CAC notify the PJCIS of any such declaration directly ‘as soon as practicable after it is made’. Instead of providing for the CAC to directly notify the PJCIS, proposed subsections 187B(6)-(7) requires the CAC to give written notice of such a declaration to the Minister, who will then, in turn, give the written notice to the PJCIS ‘as soon as practicable’.

Confidentiality of retained metadata

Application of the Privacy Act 1988 to retained metadata

Proposed section 187LA provides that the Privacy Act 1988 applies to service providers to the extent that their activities relate to retained metadata. In addition, proposed subsection 187LA(2) provides that retained metadata is, for the purposes of the Privacy Act 1988, personal information (provided it relates to the individual or a communication to which they are a party).

As a result, service providers (in addition to their encryption obligations discussed below) will be bound by the Australian Privacy Principles (APPs). This will ensure that, amongst other things, service providers will have specific obligations in relation to the collection, use, disclosure, de-identification and destruction of the retained metadata. Further, individuals will be able to request access to their personal retained data in accordance with APP 12.

Proposed section 187BA requires service providers to ensure the confidentiality of metadata they collect and retain by encrypting it and ‘protecting the information from unauthorised interference or unauthorised access.’ This reflects part of the PJCIS’s recommendation 37. However, the Bill does not include any provisions dealing with the creation of regulations that impose ‘an appropriate standard of encryption.’ As noted in the Supplementary Explanatory Memorandum:

This item does not prescribe a particular type of encryption; the decision about how to implement the encryption required by this proposed item will be a matter for the service provider to determine, in light of all the circumstances including, in particular, the technical configuration of the system or systems used to keep information required to be retained under proposed section 187A, and whether a particular method or set of methods of encryption will be adequate to protect the confidentiality of that information.

394. PJCIS, Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., recommendation 13, p. 160, para 5.33
395. Proposed paragraph 187B(3).
397. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 29, para [117].
398. Proposed paragraph 187B(5).
399. PJCIS, Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., recommendation 37: ‘The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require service providers to encrypt telecommunications data that has been retained for the purposes of the mandatory data retention regime. To give effect to this recommendation, the Committee recommends that the Data Retention Implementation Working Group develop an appropriate standard of encryption to be incorporated into regulations, and that the Communications Access Co-ordinator be required to consider a provider’s compliance with this standard as part of the Data Retention Implementation Plan process. Further, the Communications Access Co-ordinator should be given the power to authorise other robust security measures in limited circumstances in which technical difficulties prevent encryption from being implemented in existing systems used by service providers.’ (emphasis added).
401. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 24, para [84].
This would appear to suggest that the Government has decided not to implement part of the PJCIS’s recommendation 37; namely that:

... the Committee recommends that the Data Retention Implementation Working Group develop an appropriate standard of encryption to be incorporated into regulations...  

However, section 300 of the TIA Act allows regulations to be made that are ‘necessary or convenient to be prescribed for carrying out or giving effect to this Act’. As such, when proposed section 187BA is read in conjunction with section 300 of the TIA Act, it will be possible for such regulations to be issued, and hence to implement recommendation 37 of the PJCIS report (although it appears that it is not the intention of the Government to use regulations to specify encryption standards at this point in time). Further, the Bill contains a number of provisions that give effect to the third part of recommendation 37: allowing the CAC to authorise other ‘robust security measures in limited circumstances in which technical difficulties prevent encryption being implemented in existing systems used by service providers.’ This issue is examined in detail under the heading ‘Data retention implementation plans’ below.

Proposed two-year retention period
As discussed above under the headings ‘Appropriate retention period’, ‘The length of time data is to be retained’ and ‘Retention period and use of retained metadata to investigate minor offences’, the appropriate length of time that metadata should be stored was a controversial issue that both the PJCIS and PJCHR examined in detail.

Proposed section 187C provides when the types of metadata set out in the data set must start being collected, and how long they must subsequently be retained. Importantly however, proposed subsection 187C(3) clarifies that service providers are able to retain metadata for a longer period of time, should they choose to do so. In that case, it would still be available to national security, criminal law enforcement and enforcement agencies under the existing TIA Act metadata access provisions.

In addition, other provisions in the Bill will also allow the Minister or CAC to vary (but only to shorten) the period of time a service provider must retain certain types of metadata under proposed section 187C.

Certain subscriber and account related information or documents
In relation to the types of subscriber information (such as a contract relating to the service) specified in paragraphs (a) and (b) in column 2 of table item 1 in proposed subsection 187AA(1), service providers must keep the information or documents from when they were created until two years after the closure of the relevant account.

In effect this means that such information or documents associated with an account are ‘available throughout the life of the account’ and for two years after an account is closed. As noted by the Government, this is intended to ensure that ‘necessary information is available to establish a connection between communications data to be retained and the subscriber to the communications service.’

Importantly however, proposed subsection 187C(2) provides that regulations can prescribe the subscriber information discussed above is only required to be retained for a period of two years after it comes into existence, instead of period of time commencing when it comes into existence and ending two years after the closure of the account. It does not allow a longer retention period to be specified.

---

403. Telecommunications (Interception and Access) Act 1979, subsection 300(b).
405. See: proposed paragraph 187K(1)(c) and proposed subsection 187C(2).
406. Proposed paragraphs 187C(1)(a)(i) and (ii).
407. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 25, para [88].
408. Ibid.
Other types of metadata
In relation to the other types of metadata specified in the table in proposed subsection 187AA(1), the two year retention period commences when the information or document comes into existence and ends two years after that. 409

In summary, a two year retention period commences when the information or document comes into existence. If the information relates to subscriber data and account information, the two year period ends after the closure of the account to which it relates. If it is other information or documents, the two year period ends two years after it came into existence.

Data retention implementation plans
The Replacement Explanatory Memorandum outlines that:

Data retention implementation plans are intended to be plans that will allow the telecommunications industry to design a pathway to full compliance with their telecommunications data retention obligations within 18 months of the commencement of those obligations, while also allowing for interim measures that result in improved data retention practices. 410

Effect of data implementation plans
An approved data retention implementation plan between the service provider and the CAC will have the effect of not requiring the service provider to comply (for a specified time of up to 18 months) with:

• proposed subsection 187A(1) (type of metadata to be retained)
• proposed section 187BA (confidentiality of retained metadata) or
• proposed section 187C (time period for the retention of metadata). 411

Applying for data implementation plan approval
Proposed section 187E provides that a service provider may apply to the CAC for approval of a data retention implementation plan for one or more of the services they operate. Proposed section 187L ensures the confidentiality of such applications.

The CAC is a position already operating under the TIA Act, established as the primary point of liaison for interception agencies, telecommunications carriers and carriage service providers in relation to telecommunications interception issues. Section 6R of the TIA Act provides that the CAC is the Secretary of the Attorney-General’s Department or another person as specified in writing by the Attorney-General.

In the absence of an implementation plan, service providers will be required to immediately comply with the metadata collection, retention and confidentiality obligations once they commence. 412 As part of an application for approval of a data retention implementation plan, the service provider must specify (in relation to each service) the following:

• an explanation of its current relevant data retention practices and
• an explanation of its current practices for ensuring the confidentiality of retained information and documents, including in relation to the information or documents it would otherwise have had to retain under section 187A (had the implementation plan not been in force). 413

As noted in the Replacement Explanatory Memorandum, proposed paragraph 187E(2)(a) ensures that the CAC has sufficient knowledge of the service provider’s existing practices so as to be able to ascertain what, if any, changes will be required to meet its obligations under proposed Scheme. 414

409. Proposed paragraph 187C(1)(b).
410. Replacement Explanatory Memorandum, p. 49, para [227].
411. Proposed section 187D and 187H.
412. Replacement Explanatory Memorandum, p. 50, para [230].
413. Proposed paragraph 187E(2)(a).
414. Replacement Explanatory Memorandum, p. 50, para [230].
The service provider must also provide details of the interim arrangements (if any) that it proposes to implement prior to achieving full compliance, in relation to the retention of metadata and ensuring its confidentiality, and when it expects to achieve full compliance with proposed sections 187A, 187BA and 187C (but that cannot be any later than the expiry date of the plan). However, where a service provider has obtained relevant exemptions from its data retention obligations from the CAC under proposed Division 3 of Part 5-1A, it will not be required to provide this information.

**Pre-approval consultation requirements**

**Proposed section 187G** provides that the CAC must provide a copy of the data implementation plan proposed by the applicant service provider to the enforcement agencies and security authorities that are ‘in the opinion’ of the CAC ‘likely to be interested in the plan’. In addition, the CAC ‘may’ give a copy of the plan to ACMA. Where an enforcement agency or security authority requests that a plan be amended, and the CAC considers that request ‘to be a reasonable one’, the CAC must:

- request the service provider to make the amendment within 30 days after receiving the request and
- *may* give the service provider a copy of the comment or summary of the comment provided by the enforcement agency or security authority related to the requested amendment.

In turn, the service provider may either accept or reject the request to amend the plan. Where it rejects the proposed amendments to its plan, the CAC must refer the request and service provider’s response to ACMA, for final determination. Upon receipt of ACMA’s determination, the CAC must then approve the amended plan or refuse to approve the plan. In either case, the CAC must notify the service provider accordingly.

**Considerations relevant to data implementation plan approval**

**Proposed section 187F** provides that before making a decision to approve the plan or request that the plan be amended (following the consultation process with relevant enforcement agencies, security authorities and if required, ACMA) the CAC must take into account the following factors:

- the desirability of the service provider achieving substantial compliance with its data collection, retention, and confidentiality obligations as soon as is practicable (which would take into account any interim arrangements proposed by the service provider, as well as the time by which the provider proposes that each service covered by the plan will be fully compliant)
- the extent to which the plan would reduce the regulatory burden imposed on the service provider by the proposed Scheme
- if the service provider is not complying with its data collection, retention or confidentiality obligations in relation to one or more of its services—the reasons why the service provider is not complying and
- the interests of law enforcement, national security, the objects of the Telecommunications Act 1997 and ‘any other matter’ that the CAC ‘considers relevant’.

**Proposed subsections 187F(3) and (4)** have the effect of providing that where the CAC does not make a decision and communicate that decision within 60 days, it will:

- be deemed that the CAC has made and notified the service provider of the decision the service provider asked for, but
- a ‘deemed decision’ remains in force only until the CAC makes and communicates to the service provider its actual decision on the application.

---

415. Proposed paragraphs 187E(2)(b) and (c) and proposed subsection 187E(3).
416. Proposed paragraph 187E(2)(e); Replacement Explanatory Memorandum, p. 50, para [235].
417. Proposed subsection 187G(1).
418. Proposed subsection 187G(2).
419. Proposed subsection 187G(3).
420. Proposed subsections 187G(4) and (5).
421. Proposed subsection 187G(5); Replacement Explanatory Memorandum, p. 54, para [256].
422. Proposed subsection 187F(2).
In addition, proposed section 187J provides that once approved, a service provider may apply to the CAC for approval to amend its plan. Where this occurs, the application is treated in the same way as an application made under proposed section 187F. Importantly, as noted by the Replacement Explanatory Memorandum:

The CAC’s decision is not reviewable under the Administrative Decisions (Judicial Review) Act 1977 (the ADJR Act) as decisions under the TIA Act are not decisions to which the ADJR Act applies (see paragraph (d) of Schedule 1 to the ADJR Act). The exclusion of these decisions from the ADJR Act does not prevent decisions made under the TIA Act from being judicially reviewable under paragraph 75(v) of the Constitution and s 39B of the Judiciary Act 1901 (Cth).

Duration of data implementation plans

Proposed section 187H provides that a data implementation plan for a relevant service comes into effect when the CAC notifies the service provider of the approval of its plan. Where the service provider was operating the service to which the plan applies at the commencement of Part 1 of Schedule 1 of the Bill, the plan ceases to be in force 18 months after Part 1 of Schedule 1 of the Bill commenced.

Alternatively, where the service provider was not operating the relevant service covered by the plan at the commencement of Part 1 of Schedule 1 of the Bill, the plan ceases to be in force 18 months after the day the service provider started to operate the service after the commencement of Part 1 of Schedule 1 of the Bill.

Penalties for failing to comply with a data implementation plan

Proposed section 187M provides that a failure to comply with the metadata collection obligations imposed by proposed subsection 187A(1) or a data implementation plans are civil penalty provisions for the purposes of the Telecommunications Act 1997. Enforcement options for non-compliance could include remedial directions, formal warnings and infringement notices.

Exemptions from data retention and confidentiality obligations

The Replacement Explanatory Memorandum outlines that:

The exemption framework complements and sits alongside the implementation plan framework, providing further flexibility to ensure data retention obligations may be qualified to the extent appropriate having regard to national security and law enforcement considerations and the objects of the Telecommunications Act 1997.

Effect of exemptions or variations to metadata retention and confidentiality obligations

Proposed subsection 187K(1) provides that the CAC may (on its own initiative or in response to an application made by a service provider):

• exempt a service provider from its obligations under proposed Part 5-1A
• vary the obligations imposed on it under proposed Part 5-1A or
• vary the applicable metadata retention period imposed by proposed section 187C.

Importantly, any such exemptions or variations can either apply to the service provider generally, in relation to a specified relevant service or, in the case of the metadata retention period, either to all types of information and documents generally or only to information or documents that relate to a specified relevant service.

The effect of proposed section 187K is that the CAC can either vary a service provider’s obligations (or exempt it from them entirely) in relation to:

• proposed subsection 187A(1) (the type of metadata to be retained)
• proposed section 187BA (ensuring confidentiality of retained metadata) or

423. Proposed subsection 187J(2).
424. Replacement Explanatory Memorandum, p. 52, para [245].
427. The Replacement Explanatory Memorandum, outlines the enforcement options at paragraphs [293]-[296], (pp. 59-60).
• proposed section 187C (the period of time metadata must be retained).

Further, any approved exemption or variations can be made either unconditionally or subject to conditions specified by the CAC.\textsuperscript{429} However, variations cannot be used to require a service provider to retain types of metadata outside that required to be collected and retained under proposed section 187A or to retain metadata for longer than the maximum retention period imposed by proposed section 187C.\textsuperscript{430}

**Applying for exemptions or variations to metadata retention and confidentiality obligations**

**Proposed subsection 187K(5)** provides that a service provider may apply to the CAC for an exemption or variation to its obligations imposed by proposed Part 5-1A. Proposed section 187L ensures the confidentiality of such applications.

Proposed subsection 187K(5) provides that where a service provider applies for a variation or exemption the CAC must provide a copy of the application to the enforcement agencies and security authorities that are ‘in the opinion’ of the CAC ‘likely to be interested in the plan’.\textsuperscript{431} In addition, the CAC ‘may’ give a copy of the plan to ACMA.\textsuperscript{432}

**Considerations relevant to approving exemptions or variations**

Proposed subsections 187K(7) and (8) provide that when making a decision under proposed subsection 187K(1) the CAC ‘must take into account’ the following:

• the interests of law enforcement, national security and the objects of the Telecommunications Act 1997
• the service provider’s history of compliance with proposed Part 5-1A
• the service provider’s costs, or anticipated costs, of complying with proposed Part 5-1A
• any alternative metadata retention or information security arrangements that the service provider has identified and
• ‘any other matter’ that the CAC ‘considers relevant’.

As noted by the Supplementary Explanatory Memorandum, proposed paragraph 187K(7)(e) (which deals with information security arrangements):

... acknowledges that encryption, in particular, will not always be the most appropriate information security measure, especially in relation to legacy systems that were not designed to be encrypted. The purpose of this provision is to ensure that the CAC is able to consider alternative information security arrangements that a service provider has identified as being appropriate to implement when considering whether to partially exempt, or to vary, a service provider’s information security obligations under proposed section 187BA.\textsuperscript{433}

Hence, arguably proposed paragraph 187K(7)(e) is contrary to the PJCIS’s recommendation 37.

**Approval and review**

Proposed subsections 187K (5) and (6) have the effect of providing that where the CAC does not make a decision and communicate that decision within 60 days, it will:

• be deemed that the CAC has made and notified the service provider of the decision the service provider asked for, but
• a ‘deemed decision’ remains in force only until the CAC makes and communicates to the service provider its actual decision on the application.

Proposed subsection 187KA(1) provides that a service provider may apply to ACMA for a review of a decision made by the CAC under proposed subsection 187K(1). Proposed section 187L ensures the confidentiality of such

\textsuperscript{429} Proposed subsection 187K(3).
\textsuperscript{430} Proposed subsection 187K(1).
\textsuperscript{431} Proposed paragraph 187K(5)(a)(i).
\textsuperscript{432} Proposed paragraph 187K(5)(a)(ii).
\textsuperscript{433} Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 27, para [103].
applications. **Proposed subsection 187KA(2)** provides that ACMA must either confirm the decision, or substitute another decision that could have been made by the CAC.

However, prior to making a decision ACMA must give a copy of the application for review of the decision to the CAC, the enforcement agencies or security authorities that were given a copy of the original application under review and any other enforcement agencies or security authorities that are ‘in the opinion’ of ACMA ‘likely to be interested in the application’.\(^{434}\) In addition, ACMA ‘must take into account’ the same considerations imposed on the CAC noted above, including the interests of law enforcement, national security and the objects of the *Telecommunications Act 1997*, as well as ‘any other matter it considers relevant’.\(^{435}\)

**Review and annual reporting of the operation of Part 5-1A**

**Proposed subsection 187H(2)** provides that the implementation phase is the period of 18 months starting on the commencement of **proposed Part 5-1A**.

**Proposed section 187N** will require that the Parliamentary Joint Committee on Intelligence and Security commence a review of the operation of **proposed Part 5-1A** on or before the second anniversary of the end of the implementation phase (that is, no later than three and a half years after **proposed part 5-1A** commences). The review must be concluded on or before the third anniversary of the implementation phase (that is, no later than four and a half years after **proposed part 5-1A** commences). This implements Recommendation 30 of the PJCIS Report.

In addition, **proposed subsections 187N(3), (4), and (5)** provide that the head of an agency, until the PJCIS review of the proposed Scheme is completed, must keep:

- a copy of all authorisations made under Chapter 4 of the *TIA Act*
- a copy of all journalist information warrants (and authorisations made under those warrants) made under Chapter 4 of the *TIA Act* and
- information reported each year to the Minister relating to the agency’s access to historic metadata.

The Supplementary Explanatory Memorandum states that: ‘[t]his will ensure that the PJCIS review of the data retention scheme in proposed section 187N will have access to comprehensive information held by agencies on their access to telecommunications data’ and that it ‘implements recommendation 31 of the PJCIS Report’.\(^{436}\)

Annual reporting will be required on the operation of **proposed Part 5-1A** for each financial year as required by **proposed subsection 187P(2)**.

**Financial assistance to service providers**

**Proposed section 187KB** provides the legal basis for any financial assistance provided to service providers for upfront capital costs required to implement their data retention obligations.

**Schedule 1, Part 2: other amendments**

**Part 2** of the **Schedule 1** of the Bill contains a number of consequential and other amendments. Key amendments are examined below.

**ASIO Reporting requirements**

**Items 1A-1D** amend the *Australian Security and Intelligence Organisation Act 1979* (ASIO Act) to require that the number of journalist information warrants issued during the reporting period and the number of authorisations made under those journalist information warrants are included in ASIO’s annual reports.

\(^{434}\) Proposed subsection 187KA(3).

\(^{435}\) Proposed subsections 187KA(4) and (5).

Expanded role of the PJCIS

Items 1E-1G amend the *Intelligence Services Act 2001* (the *ISA*) to, amongst other things, ‘implement the Government’s response to recommendation 34’ of the PJCIS Report. Pages 31 to 32 of the Supplementary Explanatory Memorandum adequately explain the operation of these provisions.

New threshold for access to retained metadata

As noted above under the heading ‘Does the Cybercrime Convention prevent metadata being used only in relation to serious offences?’, the PJCHR’s recommendation that the Bill be amended to limit disclosure of metadata to cases where it is reasonably necessary for the investigation of serious matters, was rejected by the Government on the basis that any such restriction would conflict with Australian’s obligations under the Cybercrime Convention. For reasons outlined above, that interpretation appears to represent an overly narrow reading of the Cybercrime Convention. Put simply, the Cybercrime Convention does not prevent Australia from imposing the types of thresholds proposed by the PJCHR, and in fact, envisages such restrictions.

However, item 6J partially addresses the access-threshold issue by omitting the existing requirement from section 180F of the *TIA* Act that an officer authorising the disclosure of metadata must ‘have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable’.

That requirement is replaced with a new, higher threshold, namely that the authorising officer must ‘be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate’. Item 6K then inserts proposed paragraph 180F(aa) which will require the authorising officer to ‘have regard’ to the gravity of any conduct in relation to which a metadata authorisation is sought, including the following factors:

- the seriousness of any offence in relation to which the authorisation is sought
- the seriousness of any pecuniary penalty in relation to which the authorisation is sought
- the seriousness of any protection of the public revenue in relation to which the authorisation is sought and
- whether the authorisation is sought for the purposes of finding a missing person.

Whilst arguably the above amendment may have the effect of imposing a higher threshold on metadata access, it nonetheless falls short of clearly restricting access to metadata and its use to the investigation of serious crimes and serious matters as recommended by the PJCHR and as foreshadowed by the Cybercrime Convention itself. As a result, it is arguable that despite the amendments proposed by items 6J and 6K, issues of proportionality in relation to the use of metadata to investigate relatively minor offences remain.

Access to retained data in connection with civil litigation

Items 3A-3C in Part 2 of Schedule 1 of the Bill amend the *Telecommunications Act 1997* to prohibit civil litigants from being able to access metadata that is retained by a service provider solely for the purpose of complying with the proposed Scheme, and thus give effect to recommendation 23 of the PJCIS Report.

Pages 33 to 35 of the Supplementary Explanatory Memorandum adequately explain the operation of these provisions.

Access to journalists’ metadata

Item 6L of Schedule 1 of the Bill will insert proposed Division 4C – *Journalist information warrants* into Part 4-1 of the *TIA* Act. As noted earlier in this Digest, the PJCIS had recommended that the issue of using metadata to determine a journalist’s source be the subject of a separate review that included an examination of international best practice, and specifically practices in the UK. However, the ALP insisted on the creation of a warrant regime specifically to deal with access to journalists’ metadata, for the purpose of determining their sources. Item 6L is designed to give effect to that demand.

---

437. Ibid., p. 31.
**PJCIS Report and position on accessing journalists’ metadata**

An interim issued raised by proposed Division 4C is its appropriateness. As noted by the PJCIS, in the course of its Inquiry ‘a number of submitters expressed significant concerns with agencies accessing privileged or otherwise sensitive telecommunications data.’440 These concerns were not confined only to journalists’ metadata, but also to metadata associated with other professionally privileged or otherwise sensitive communications such as lawyer-client, doctor-client or Members of Parliament and their correspondents.441 The PJCIS, after considering the issues raised by submitters, concluded that:

... certain telecommunications data has the potential to possess an additional level of sensitivity because of the nature of the relationship of those communicating, including client legal privilege that applies to certain communications between lawyers and their clients, and journalist relationships with confidential sources.442

However, the PJCIS concluded that there was no ‘need for additional legislative protection in respect of accessing telecommunications data that may relate to a lawyer’ but that due to the ‘importance of recognising the principle of press freedom and the protection of journalists’ sources’ that further consideration be given to the matter before a final recommendation is made.443

**Current position in the United Kingdom**

After considering similar issues, the UK Government has proposed (pending potential further legislative reform) that prior to accessing metadata, an authorising officer must give:

... special consideration to necessity and proportionality, [and] must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of privacy, and clearly note when an application is made for the communications data of a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion.444 (emphasis added)

Further, it is also a proposed requirement that:

For each item of communications data included within a notice or authorisation, the relevant public authority must also keep a record of the following: .... whether the data relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion).445 (emphasis added)

Clearly, the policy approach taken by the UK differs substantially from that reflected in proposed Division 4C. Put simply, the proposed UK approach does not single out journalists for special ‘protection’ from metadata access powers. Instead, it treats a number of professions and vocations that handle ‘privileged or otherwise confidential information’ in a consistent manner. A similar point was made by the AGD.446

**Why are journalists special?**

Since the announcement of the intention to create a warrant regime governing access to journalists’ metadata for the purpose of identifying their sources, a number of peak bodies have expressed concern. For example, the Law Institute of Victoria noted that in its view:

---

440. Ibid., p. 251, para [6.193].
441. Ibid., pp 251-251, paras [6.194-196].
442. Ibid., p. 257, para [6.210].
444. UK Government, Home Office (UK Home Office), Draft Code of Practice: Acquisition and Disclosure of Communications Data, Home Office, 9 December 2014, para 3.73. The Draft Code of Practice [Draft CoP] was then laid before the UK Parliament on 4 March 2015. As per section 71 of the Regulation of Investigatory Powers Act 2000 (UK) [RIPA], a draft CoP ‘comes into force on the day after the day on which ‘an Order made by the Secretary of State giving it legal force comes into effect.’ Importantly however, subsection 71(9) of the RIPA provides that the ‘Secretary of State shall not make an order containing provision for any of the purposes of this section unless a draft of the order has not yet been approved by a resolution of each House. Whilst the draft CoP has not yet been approved by a resolution of each House, it is likely to closely resemble the final legislative position in the UK.
446. AGD, Submission to the PJCIS, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., pp. 21-22.
Information exchanged by email or calls between the lawyer and associates of the client, experts or potential witnesses, could disclose a defence case, for example. A litigation strategy or case theory could be identified based on witnesses or experts contacted by the lawyer.  

It therefore stated that the Bill ‘must be amended so that a warrant is required to access lawyers’ telecommunications data’. Likewise the Institute of Public Affairs stated that ‘journalists are not a special class that deserve unique privileges. Many other professions value the confidentiality that they have with clients – for instance, lawyers and doctors’.  

It is not immediately apparent (apart from then ‘chilling impact’ argument noted by the PJCIS) why journalists’ metadata is more sensitive (and hence more deserving of the additional projections offered by proposed Division 4C) than that of the professions identified by the UK Government.

**Proposed journalist information warrant regime**

**Proposed Division 4C** creates two types of journalist information warrants (JIWs): those issued to ASIO, and those issued to enforcement agencies. Pages 39 to 46 of the Supplementary Explanatory Memorandum adequately explain the operation of these provisions. However, key features are summarised below.

**Prohibition on accessing journalists metadata**

**Proposed sections 180G** and 180H prohibit an eligible ASIO officer or enforcement agency officer respectively from authorising access to the metadata of a journalist for the purpose of identifying another person they ‘reasonably believe to be a source’ unless a JIW is in force.

**Lack of definition of a journalist**

The Bill does not contain a definition of ‘journalist’. However, the Supplementary Explanatory Memorandum notes that an individual is a journalist for the purposes of the Bill ‘if they are working as a journalist in a professional capacity. Indicators that a person is acting in a professional capacity include regular employment, adherence to enforceable ethical standards and membership of a professional body.’

**ASIO JIW**

**Proposed section 180J** provides that the Director-General of Security may request the Minister to issue a JIW. **Proposed section 180L** provides that the Minister must not issue a JIW unless satisfied that ‘the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source’ after having regard to the following factors:

- the anticipated privacy interference
- the gravity of the matter for which the warrant is sought
- the assistance the information to be sought would provide
- whether other reasonable methods, if any, that would be effective to obtain the information have been used,
- any submissions by a Public Interest Advocate on that application and
- any other relevant matter.

If satisfied, the Minister can issue the JIW and, further, can impose special conditions or restrictions. The maximum duration of a JIW is six months, but the Minister can revoke it at any time prior to its expiration.

---


448. Ibid.


451. Proposed subsections 180G(1) and 180H(1); proposed paragraphs 180G(1)(b) and 180H(1)(b).

452. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 39, para [178].

453. Proposed subsection 180L(2).
**Enforcement agency JIWs**

**Proposed section 180Q** provides that the chief office of an enforcement agency, or an officer nominated by him or her, may apply to an ‘issuing authority’ for a JIW. Section 6DB of the **TIA Act** defines an ‘issuing authority’ as a person appointed by the Minister who is either a Judge of a court created by the Parliament, a magistrate, or certain members of the Administrative Appeals Tribunal.

**Proposed section 180S** provides that information given to the issuing authority in connection with an application for a JIW must be verified under oath or affirmation. **Proposed subsection 180T(2)** then provides that an issuing authority must not issue a JIW unless it is satisfied that the warrant is reasonably necessary to:

- enforce the criminal law
- locate a person reported as missing to the Australian Federal Police or a state Police Force
- enforce a law that imposes a pecuniary penalty or protects the public revenue or
- investigate serious offences or an offence against a Commonwealth, state or territory law punishable by at least a three-year imprisonment term.  

In addition to the above, an issuing authority cannot issue a JIW unless it is also satisfied that ‘the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source’ after having regard to the following factors:

- the anticipated privacy interference
- the gravity of the matter for which the warrant is sought
- the assistance the information to be sought would provide
- whether other reasonable methods, if any, that would be effective to obtain the information have been used,
- any submissions by a Public Interest Advocate on that application and
- any other relevant matter.  

If satisfied, the issuing authority can issue the JIW and, further, can impose special conditions or restrictions. The maximum duration of a JIW is 90 days. **Proposed section 180U** specifically provides that an issuing authority cannot vary a JIW by ‘extending the period of time for which it is to be in force’.

**Role of the Public Interest Advocate**

**Proposed section 180X** creates the new role of a Public Interest Advocate (PIA). As noted by the Supplementary Memorandum, the role of the PIA is to:

... consider and evaluate journalist information warrant applications made by the Organisation and law enforcement agencies pursuant to sections 180L and 180T respectively. The Public Interest Advocate will be able to make independent submissions to the Minister in the case of the journalist information warrants made by the Organisation, and to the issuing authority in the case of the law enforcement agencies, on the proposed undertaking in relation to each application (including conditions or restrictions).

**Proposed subsection 180X(1)** provides that the Prime Minister may declare one or more persons to be PIAs, whilst **proposed subsection 180X(3)** provides that regulations may be used to prescribe matters relating to the performance of the role of a PIA.

---

454. Proposed subsection 180L(3).
455. Proposed section 180N.
457. Proposed paragraph 180T(2)(b).
458. Proposed subsection 180U(3).
459. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 46, para [222].
New offences related to JIWs

Proposed section 182A creates an offence where a person discloses or uses a JIW or information about such a warrant (including whether a JIW was (or is being) applied for). The offence attracts a maximum penalty of two years imprisonment.

Proposed section 182B outlines the circumstances in which disclosures and use of a JIW are permitted. These circumstances are adequately explained on page 47 of the Supplementary Memorandum.

Additional oversight and reporting of JIWs

Proposed sections 185D to 185E require agencies to provide copies of JIWs to the Minister, IGIS and Ombudsman (depending on the agency).

Proposed subsections 185D(3)-(4) and 185D(7)-(8) provide that in the event that the IGIS or the Ombudsman exercise their oversight functions in relation to relevant JIWs, and report to the responsible Minister in accordance with their governing legislation, the Minister must provide any oversight reports to the PJCIS as soon as practicable after receiving them. In addition, the PJCIS may request the IGIS or Ombudsman to brief it on an oversight report received from the Minister.⁴⁶⁰

In addition, items 6Y and 6Z will amend section 186 of the TIA Act to expand the list of information that must be included in the annual reports produced by relevant agencies for tabling in Parliament, in accordance with recommendation 33 of the PJCIS Report. Relevantly, this includes the number of JIWs issued during the reporting period.⁴⁶¹

Schedule 2: Restricting access to stored communications and telecommunications data

The amendments in Schedule 2 of the Bill are primarily aimed at limiting the range of agencies that are able to access metadata and stored communications. The Replacement Explanatory Memorandum noted that by amending the definitions of ‘enforcement agency’ and ‘criminal law enforcement agency’ the Bill:

... will strengthen privacy protections in relation to stored communications by limiting the availability of historic domestic preservation notices to those agencies who can apply for stored communications warrants under the TIA Act as amended...Ongoing domestic preservation notices will continue to be limited to interception agencies.⁴⁶²

Definition of criminal-law-enforcement agency

Item 1 of Part 1 of Schedule 2 of the Bill will remove the references to an ‘enforcement agency’ in subsection 107(J)(1) of the TIA Act and substitute references to a ‘criminal law-enforcement agency’, which will be defined in proposed section 110A. The intention is to limit access to stored communications to agencies with a demonstrated investigative need and practices to safeguard the use and disclosure of information obtained under a stored communications warrant. For the sake of completeness a criminal law-enforcement agency, inserted by item 3 will be:

• the Australian Federal Police
• a Police Force of a state
• the Australian Commission for Law Enforcement Integrity
• the ACC
• the Australian Customs and Border Protection Service
• the Australian Securities and Investments Commission
• the Australian Competition and Consumer Commission
• the Crime Commission
• the Independent Commission Against Corruption

⁴⁶⁰. Proposed section 185E.
⁴⁶¹. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 49, para [244].
⁴⁶². Replacement Explanatory Memorandum, p. 68, paragraph [351].
• the Police Integrity Commission
• the IBAC
• the Crime and Corruption Commission of Queensland
• the Corruption and Crime Commission
• the Independent Commissioner Against Corruption and
• an authority or body for which a declaration under proposed subsection 110A(3) is in force.

Proposed section 110A was amended to reflect recommendation 20 of the PJCIS Report by adding ASIC and ACCC as criminal law-enforcement agencies. The will ensure that ASIC and ACCC can access stored communications (subject to a warrant), prospective metadata and historical metadata.

Ministerial power to declare criminal law-enforcement agencies

Proposed subsections 110A(3) to (11) allow the Attorney-General to declare an authority to be a criminal law-enforcement agency for the purposes of the TIA Act (and hence, for example, able to access metadata and apply for interception warrants).

Proposed subsection 110A(3B) provides that the Minister ‘must not make’ a declaration unless the Minister is satisfied ‘on reasonable grounds that the functions of the authority or body include investigating serious contraventions’. Proposed subsection 110A(4) then provides a list of specific factors which the Minister must take into account including whether:

• access to stored communications, and the making of authorisations under section 180, would be reasonably likely to assist the authority or body in investigating serious contraventions
• the authority or body is required to comply with the APPs or (a binding scheme that provides protection of personal information that meets the requirements of proposed subsection 110(4A))
• the authority or body has agreed to comply with a scheme providing such protection of personal information, in relation to personal information disclosed to it under Chapter 3 or 4, if the declaration is made
• the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of a criminal law-enforcement agency under Chapter 3, and the obligations of an enforcement agency under Chapter 4
• the declaration would be in the public interest and
• any other matters the Minister considers relevant.

Importantly, proposed subsection 110(4A) provides that for the purposes of protecting personal information referred to above (proposed paragraphs 110A(4)(c)(ii) and (iii)) the scheme must be comparable (in terms of the protection provided to personal information) to that provided by the APPs and include a mechanism:

• for monitoring the authority’s or body’s compliance with the scheme and
• that enables an individual to seek recourse if his or her personal information is mishandled.

Proposed subsection 110A(5) then provides that when considering whether to make a declaration, the Minister ‘may’ consult with ‘such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.’ Proposed subsections 110A(6) and 110A(7) then provide that the Minister may impose conditions on a declaration.

Proposed subsection 110A(10) reflects recommendation 17 of the PJCIS Report and provides that such declarations are only to be in effect for 40 sittings days of either House of the Parliament. However, the PJCIS also recommended that the Bill be amended to provide that in circumstances where the Minister declares an authority or body as a criminal-law enforcement body:

463. Supplementary Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, op. cit., p. 50.
In other words, the PJCIS sought to link such declarations to the subsequent introduction of an amending Bill and resulting formal Parliamentary processes and considerations.

The amended Bill does directly not address that aspect of the PJCIS’s recommendation. Put simply, there is no requirement that a Bill reflecting the declaration must (or even should) be introduced to the Parliament (noting that the PJCIS couched their recommendation in discretionary terms). This gives the Government discretion as to whether to proceed with the declaration on a permanent basis. Clearly, if the Government does not introduce a Bill reflecting the declaration, it will lapse after 40 sitting days.

**Proposed subsection 110A(11)** provides that ‘if’ a Bill seeking to amend **proposed subsection 110A(1)** is introduced the Parliament, the Minister:

- **must** refer the Bill to the PJCIS for review and
- the PJCIS must be provided a minimum of 15 sitting days of a House of Parliament after the introduction of the Bill in to report on its review of such a Bill.

Again, the Bill differs slightly from the PJCIS recommendation in that it had recommended that such amendments ‘should’ (rather than ‘must’) be referred to the PJCIS for review and report.

**Definition of law-enforcement agency**

**Proposed section 176A** defines the meaning of ‘enforcement agency’. **Proposed subsection 176A(1)** provides that each criminal law-enforcement agency is an enforcement agency. **Proposed subsections 176A(2) and (3)** allow the Attorney-General to declare an authority to be a law-enforcement agency for the purposes of the TIA (and hence, for example, be able to access metadata).

**Proposed section 176A(3B)** provides that the Minister ‘must not make the declaration’ unless they are satisfied ‘on reasonable grounds’ that the functions of the authority or body include:

- enforcement of the criminal law
- administering a law imposing a pecuniary penalty or
- administering a law relating to the protection of the public revenue.

**Proposed subsection 176A(4)** then provides a list of specific factors which the Minister must take into account including whether:

- access to stored communications, and the making of authorisations under sections 178 or 179 of the TIA would be reasonably likely to assist the authority or body in performing the functions referred to in **proposed subsection 176A(3B)**
- the authority or body is required to comply with the APPs or (a binding scheme that provides protection of personal information that meets the requirements of **proposed subsection 176A(4A)**)
- the authority or body has agreed to comply with a scheme providing such protection of personal information, in relation to personal information disclosed to it under Chapter 3 or 4, if the declaration is made
- whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of a criminal law-enforcement agency under Chapter 3, and the obligations of an enforcement agency under Chapter 4
- the declaration would be in the public interest and
- any other matters the Minister considers relevant.

---

465. Ibid.
466. Ibid.
Importantly, **proposed subsection 176A(4A)** provides that for the purposes of protecting personal information referred to above (**proposed paragraphs 176A(4)(c)(ii) and (iii)**) the scheme must be comparable (in terms of the protection provided to personal information) to that provided by the APPs and include a mechanism:

- for monitoring the authority’s or body’s compliance with the scheme and
- that enables an individual to seek recourse if his or her personal information is mishandled.

**Proposed subsection 176A(5)** then provides that when considering whether to make a declaration, the Minister ‘may’ consult with ‘such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.’ **Proposed subsections 176A(6) and (7)** then provide that the Minister may impose conditions on a declaration.

**Proposed subsection 176A(10)** reflects recommendation 21 of the PJCIS Report and provides that such declarations are only to be in effect for 40 sittings days of either House of the Parliament. However, the PJCIS also recommended that the Bill be amended to provide that in circumstances where the Minister declares an authority or body as a criminal-law enforcement body:

> ... an amendment to specify the authority or body as an enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days.  

In other words, the PJCIS sought to link such declarations to the subsequent introduction of an amending Bill and resulting formal Parliamentary processes and considerations.

The amended Bill does not directly address that aspect of the PJCIS’s recommendation. Put simply, there is no requirement that a Bill reflecting the declaration must (or even should) be introduced to the Parliament (noting that the PJCIS couched their recommendation in discretionary terms). This gives the Government discretion as to whether to proceed with the declaration on a permanent basis. Clearly, if the Government does not introduce a Bill reflecting the declaration, it will lapse after 40 sitting days.

**Proposed subsection 176A(11)** provides that ‘if’ a Bill seeking to amend **proposed subsection 176A(1)** is introduced, the Parliament, the Minister:

- **must** refer the Bill to the PJCIS for review and
- the PJCIS must be provided a minimum of 15 sitting days of a House of Parliament after the introduction of the Bill in to report on its review of such a Bill.

Again, the Bill differs slightly from the PJCIS recommendation in that it had recommended that such amendments ‘should’ (rather than ‘must’) be referred to the PJCIS for review and report.

**Summary of criminal law enforcement and law enforcement agency declaration powers**

Viewed as a whole, **proposed sections 110A and 176A** provide the Attorney-General the power to temporarily declare an authority or body a criminal law-enforcement agency or law enforcement agency (thus ensuring the Proposed scheme is flexible and responsive to changes) and balances that power with the desire of Parliament to be able to fulfil its law-making and oversight functions in response to recommendations 17 and 21 in the PJCIS Report.

**Schedule 3 - Oversight by the Commonwealth Ombudsman**

Division 1 of **Schedule 3** will create obligations for the chief officer of a criminal law-enforcement agency to keep records for three years or until the time that the Ombudsman reports under **proposed section 186J**, whichever is earlier. The records that must be kept are listed under **proposed section 151** and include preservation notices, stored communications warrants, authorisations, mutual assistance requests, evidentiary certificates et cetera. Further kind of documents and material can be prescribed by legislative instrument by the Minister.

---


468. Ibid., recommendation 21.

469. Ibid.
While the scrutiny is prima facie appropriate, it is not clear how the increased workload will be able to be afforded by the Commonwealth Ombudsman’s office.
### Appendix: A

#### Table 7: PJCIS recommendations and amendments made to the Bill

<table>
<thead>
<tr>
<th>Recommendation number</th>
<th>Recommendation</th>
<th>Related amended provision and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Committee recommends that the Government provide a response to the outstanding recommendations from the Committee’s 2013 Report of the Inquiry into Potential Reforms of Australia’s National Security Legislation by 1 July 2015.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to include the proposed data set in primary legislation.</td>
<td>Proposed subsections 187A(1)(a) and 187(2)</td>
</tr>
<tr>
<td>3</td>
<td>To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare items for inclusion in the data set under the following conditions: • The declaration ceases to have effect after 40 sitting days of either House • An amendment to include the data item in legislation should be brought before the Parliament before the expiry of the 40 sitting days and • The amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report.</td>
<td>Proposed subsections 187AA(2)-(5)</td>
</tr>
<tr>
<td>4</td>
<td>The Committee recommends that the proposed data set published by the Attorney-General’s Department on 31 October 2014 be amended to incorporate the recommendations of the Data Retention Implementation Working Group.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that service providers are not required to collect and retain customer passwords, PINs or other like information.</td>
<td>[See explanation to Item 1 of table in Item 8 of supplementary EM]</td>
</tr>
<tr>
<td>6</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that service providers are only required to retain telecommunications data to the extent that such information is, in fact, available to that service provider.</td>
<td>Proposed 187A(4)(c)</td>
</tr>
</tbody>
</table>

---

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

Warning: All viewers of this digest are advised to visit the disclaimer appearing at the end of this document. The disclaimer sets out the status and purpose of the digest.
<table>
<thead>
<tr>
<th>Recommendation number</th>
<th>Recommendation</th>
<th>Related amended provision and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that service providers are not required to keep web-browsing histories or other destination information, for either incoming or outgoing traffic.</td>
<td>[See explanation to Item 3 of table in Item 8 of supplementary EM]</td>
</tr>
<tr>
<td>8</td>
<td>The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to provide greater clarity in defining ‘sessions’ in proposed subsection 187A(7) of the Bill.</td>
<td>[Note item 7 of supplementary EM removes proposed subsection 187A(7), which appears in substantially same form in proposed subsection 187AA(6). See paragraph 72 to supplementary EM for some discussion of ‘session’ in regards to this]</td>
</tr>
<tr>
<td>9</td>
<td>The Committee recommends that the two-year retention period specified in section 187C of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be maintained.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 clarify the requirements for service providers with regard to the retention, de-identification or destruction of data once the two year retention period has expired.</td>
<td>[See paragraph 118 to supplementary EM]</td>
</tr>
<tr>
<td>11</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to define the term ‘infrastructure’ in greater detail, for the purposes of paragraph 187A(3)(c).</td>
<td>Item 41 inserts definition into subsection 5(1) of TIA Act.</td>
</tr>
<tr>
<td>12</td>
<td>The Committee recommends that the Attorney-General’s Department and national security and law enforcement agencies provide the Parliamentary Joint Committee on Intelligence and Security with detailed information about the impact of the exclusion of services provided to a single area pursuant to subparagraph 187B(1)(a)(ii) as part of the Committee’s review of the regime, pursuant to section 187N of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>The Committee recommends that proposed section 187B in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be</td>
<td>Proposed subsections 187B(2A), 187B(3)(ba) and (bb), 187B(6) and (7)</td>
</tr>
<tr>
<td>Recommendation number</td>
<td>Recommendation</td>
<td>Related amended provision and notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>amended to require the Communications Access Co-ordinator to consider the objects of the Privacy Act 1988 when considering whether to make a declaration under proposed subsection 187B(2). If there is any uncertainty or a need for clarification, the Co-ordinator should consult with the Australian Privacy Commissioner on that issue before making such a declaration. Further, the Co-ordinator should be required to notify the Parliamentary Joint Committee on Intelligence and Security of any declaration made under 187B(2) as soon as practicable after it is made.</td>
<td>Proposed subsection 187A(3A), (3B) and (3C)</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare additional classes of service providers under the following conditions:  • The declaration ceases to have effect after 40 sitting days of either House,  • An amendment to include the class of service provider in legislation should be brought before the Parliament before the expiry of the 40 sitting days, and  • The amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report.</td>
<td>Proposed subsection 187KA</td>
</tr>
<tr>
<td>15</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 and accompanying Explanatory Memorandum be amended to enable the Communications Access Co-ordinator to refer any disputes over proposed implementation plan exemptions or variations to the Australian Communications Media Authority for determination.</td>
<td>Reference to 187KA inserted into paragraph (1)(b) of item 9 in Part 3 of Schedule 1 of Bill</td>
</tr>
<tr>
<td>16</td>
<td>The Committee recommends that the Government make a substantial contribution to the upfront capital costs of service providers implementing their data retention obligations. When designing the funding arrangements to give effect to this recommendation, the Government should ensure that an appropriate balance is achieved that accounts for the significant variations between the services, business models, sizes and financial positions of different companies within the telecommunications industry. In particular, the Committee recommends that the Government</td>
<td>Proposed section 187KB</td>
</tr>
<tr>
<td>Recommendation number</td>
<td>Recommendation</td>
<td>Related amended provision and notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>ensure that the model for funding service providers:</td>
<td>Proposed subsections 110A(3A) and (3B)</td>
</tr>
<tr>
<td></td>
<td>• provides sufficient support for smaller service providers, who may not have sufficient capital budgets or operating cash flow to implement data retention, and privacy and security controls, without up-front assistance</td>
<td>Proposed paragraph 110A(4)(a)</td>
</tr>
<tr>
<td></td>
<td>• minimises any potential anti-competitive impacts or market distortions</td>
<td>Proposed subsections 110A(10) and 110A(11)</td>
</tr>
<tr>
<td></td>
<td>• accounts for the differentiated impact of data retention across different segments of the telecommunications industry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• incentivises timely compliance with their data retention obligations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• provides appropriate incentives for service providers to implement efficient solutions to data retention</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• does not result in service providers receiving windfall payments to operate and maintain existing, legacy systems and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• takes into account companies that have recently invested in compliant data retention capabilities in anticipation of the Bill’s passage.</td>
<td></td>
</tr>
</tbody>
</table>

17 The Committee recommends that criminal law-enforcement agencies, which are agencies that can obtain a stored communications warrant, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*. To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as a criminal law-enforcement agency subject to the following conditions:

- the declaration ceases to have effect after 40 sitting days of either House
- an amendment to specify the authority or body as a criminal law-enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days and
- the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sittings days for review and report.

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 110A(4)(b)-(f), and must also be satisfied on
<table>
<thead>
<tr>
<th>Recommendation number</th>
<th>Recommendation</th>
<th>Related amended provision and notes</th>
</tr>
</thead>
</table>
| 18                    | The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or its Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 110A(4)(c)(ii) of the Telecommunications (Interception and Access) Act 1979 include a mechanism:  
• for monitoring the authority or body’s compliance with the scheme and  
• to enable individuals to seek recourse if their personal information is mishandled.  
The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements. | Proposed subparagraph 110A(4)(c)(ii) (as amended by items 63-65) |
| 19                    | The Committee recommends that the Attorney-General’s Department review whether:  
• the agencies which may access the content of communications (either by way of interception warrants or stored communications warrants) under the Telecommunications (Interception and Access) Act 1979 should be standardised and  
• the Attorney-General’s declaration power contained in proposed section 110A of the Telecommunications (Interception and Access) Act 1979 in respect of criminal law-enforcement agencies should be adjusted accordingly.  
The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by the end of the implementation phase of the data retention regime. | Proposed subparagraph 110A(1)(e) |
<p>| 20                    | The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to list the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) as criminal law-enforcement agencies under proposed section 110A of the Telecommunications (Interception and Access) Act 1979. | Proposed subsection |
| 21                    | The Committee recommends that enforcement | Proposed subsection |</p>
<table>
<thead>
<tr>
<th>Recommendation number</th>
<th>Recommendation</th>
<th>Related amended provision and notes</th>
</tr>
</thead>
</table>
|                        | agencies, which are agencies authorised to access telecommunications data under internal authorisation, be specifically listed in the Telecommunications (Interception and Access) Act 1979. To provide for emergency circumstances the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as an enforcement agency subject to the following conditions:  
• the declaration ceases to have effect after 40 sitting days of either House  
• an amendment to specify the authority or body as an enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days and  
• the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report. Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 176A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include enforcement of the criminal law, administering a law imposing a pecuniary penalty, or administering a law relating to the protection of the public revenue. | 176A(3B)  
Omitted proposed paragraph 176A(4)(a)  
Proposed subsections 176A(10) and 176A(11) |
| 22                    | The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or the Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 176A(4)(c)(ii) of the Telecommunications (Interception and Access) Act 1979 include a mechanism:  
• for monitoring the authority or body’s compliance with the scheme and  
• to enable individuals to seek recourse if their personal information is mishandled. The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or | Proposed subparagraph 176A(4)(c)(ii) (as amended by items 71 to 73) |
<table>
<thead>
<tr>
<th>Recommendation number</th>
<th>Recommendation</th>
<th>Related amended provision and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime. To enable appropriate exceptions to this prohibition the Committee recommends that a regulation making power be included. Further, the Committee recommends that the Minister for Communications and the Attorney-General review this measure and report to the Parliament on the findings of that review by the end of the implementation phase of the Bill.</td>
<td>Proposed subsections 280(1B) and (1C), 281(2) and (3) to the <em>Telecommunications Act</em> (see Part 2, Schedule 1 of Bill)</td>
</tr>
<tr>
<td>24</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime. Telecommunications service providers should be able to recover their costs in providing such access, consistent with the model applying under the <em>Privacy Act</em> in respect of giving access to personal information.</td>
<td>Proposed section 187LA</td>
</tr>
<tr>
<td>25</td>
<td>The Committee recommends that section 180F of the <em>Telecommunications (Interception and Access) Act 1979</em> be replaced with a requirement that, before making an authorisation under Division 4 or 4A of Part 4-1 of the Act, the authorised officer making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate. In making this decision the authorised officer should be required to have regard to: • the gravity of the conduct being investigated, including whether the investigation relates to a serious criminal offence, the enforcement of a serious pecuniary penalty, the protection of the public revenue at a sufficiently serious level or the location of missing persons • the reason why the disclosure is proposed to be authorised and • the likely relevance and usefulness of the information or documents to the investigation.</td>
<td>Amended section 180F, proposed subparagraph 180F(aa) of <em>TIA Act</em> (amending items 6A and 6B)</td>
</tr>
<tr>
<td>Recommendation number</td>
<td>Recommendation</td>
<td>Related amended provision and notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>The Committee acknowledges the importance of recognising the principle of press freedom and the protection of journalists’ sources. The Committee considers this matter requires further consideration before a final recommendation can be made. The Committee therefore recommends that the question of how to deal with the authorisation of a disclosure or use of telecommunications data for the purpose of determining the identity of a journalist’s source be the subject of a separate review by this Committee. The Committee would report back to Parliament within three months. In undertaking this inquiry, the Committee intends to conduct consultations with media representatives, law enforcement and security agencies and the Independent National Security Legislation Monitor. The review will also consider international best practice, including data retention regulation in the United Kingdom.</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Act 1979 be amended to require agencies to provide a copy to the Commonwealth Ombudsman (or Inspector General of Intelligence and Security (IGIS) in the case of ASIO) of each authorisation that authorises disclosure of information or documents under Chapter 4 of the Act for the purpose of determining the identity of a journalist’s sources. The Committee further recommends that the IGIS or Commonwealth Ombudsman be required to notify this Committee of each instance in which such an authorisation is made in relation to ASIO and the AFP as soon as practicable after receiving advice of the authorisation and be required to brief the Committee accordingly.</td>
<td>Proposed section 187A (item 1) &lt;br&gt;*Proposed paragraphs in Part 4-1 Division 6 of TIA Act &lt;br&gt;Proposed sections 185D and 185E of TIA Act (item 6X, Schedule 1 of Bill)</td>
</tr>
<tr>
<td>28</td>
<td>The Committee recommends that the Attorney-General’s Department oversee a review of the adequacy of the existing destruction requirements that apply to documents or information disclosed pursuant to an authorisation made under Chapter 4 of the Telecommunications (Interception and Access) Act 1979 and held by enforcement agencies and ASIO. The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by 1 July 2017.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>The Committee recommends that the Government consider the additional oversight responsibilities of the Commonwealth Ombudsman set out in the Telecommunications (Interception and Access)</td>
<td></td>
</tr>
<tr>
<td>Recommendation number</td>
<td>Recommendation</td>
<td>Related amended provision and notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Amendment (Data Retention) Bill 2014 and ensure that the Office of the Commonwealth Ombudsman is provided with additional financial resources to undertake its enhanced oversight responsibilities.</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require the Parliamentary Joint Committee on Intelligence and Security to commence its review no later than the second anniversary of the end of the implementation period. The Committee considers it is desirable that a report on the review be presented to the Parliament no later than three years after the end of the implementation period.</td>
<td>Proposed subsection 187N(1)</td>
</tr>
<tr>
<td>31</td>
<td>At the time of the review required to be undertaken by the Parliamentary Joint Committee on Intelligence and Security under proposed section 187N of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, the Committee recommends that the Attorney-General request the Committee to examine the following issues: • the effectiveness of the scheme • the appropriateness of the dataset and retention period • costs • any potential improvements to oversight • regulations and determinations made • the number of complaints about the scheme to relevant bodies and • any other appropriate matters. To facilitate the review, the Committee recommends that agencies be required to collect and retain relevant statistical information to assist the Committee’s consideration of the above matters. The Committee also recommends that all records of data access requests be retained for the period from commencement until the review is concluded. Finally the Committee recommends that, to the maximum extent possible, the review be conducted in public.</td>
<td>Proposed subsections 187N(3), (4) and (5)</td>
</tr>
<tr>
<td>32</td>
<td>The Committee recommends that the Attorney-General coordinate the provision of a standing secondee or secondees to the secretariat of the Parliamentary Joint Committee on Intelligence and Security, in recognition of the additional oversight and review requirements associated with the</td>
<td></td>
</tr>
<tr>
<td>Recommendation number</td>
<td>Recommendation</td>
<td>Related amended provision and notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 and the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.</td>
<td>Proposed subsection 187P(1A)</td>
</tr>
<tr>
<td>33</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require the annual report prepared under section 187P to include: • costs of the scheme • use of implementation plans • category of purpose for accessing data, including a breakdown of types of offences • age of data sought • number of requests for traffic data and • number of requests for subscriber data. The Committee also recommends that the Attorney-General’s Department provide the Committee with an annual briefing on the matters included in this report.</td>
<td>Proposed subsection 94(2A) of the ASIO Act (amending items 1A-1D in Schedule 1 of Bill) Amended section 186, proposed subsection 186(1E) of TIA Act (items 6Y and 6Z of Bill)</td>
</tr>
<tr>
<td>34</td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to provide that the Committee may inquire into any matter raised in the annual report prepared under proposed section 187P, including where this goes to a review of operational matters. Legislative change to the Intelligence Services Act 2001 should be implemented to reflect this changed function. The Committee further recommends that the Commonwealth Ombudsman and Inspector-General of Intelligence and Security provide notice to the Committee should either of them hold serious concerns about the purpose for, or the manner in which, retained data is being accessed.</td>
<td>Proposed paragraphs 29(1(bc), (bd) and (be), subsections 29(4) and 29(5), paragraphs 29(5)(a) and 29(5)(b) of Intelligence Services Act 2001 (amending items 1E-1G in Schedule 1 of Bill) Proposed paragraphs in Part 4-1 Division 6 of TIA Act Proposed sections 185D and 185E of TIA Act (item 6X, Schedule 1 of Bill)</td>
</tr>
<tr>
<td>35</td>
<td>Having regard to the regulatory burden on small providers with an annual turnover of less than $3 million, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require all service providers to be compliant, in respect of retained data, with either the Australian Privacy Principles or binding rules developed by the Australian Privacy Commissioner.</td>
<td>Proposed section 187LA</td>
</tr>
<tr>
<td>36</td>
<td>The Committee recommends that the Government enact the proposed Telecommunications Sector</td>
<td></td>
</tr>
<tr>
<td>Recommendation number</td>
<td>Recommendation</td>
<td>Related amended provision and notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>37</strong></td>
<td>The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require service providers to encrypt telecommunications data that has been retained for the purposes of the mandatory data retention regime. To give effect to this recommendation, the Committee recommends that the Data Retention Implementation Working Group develop an appropriate standard of encryption to be incorporated into regulations, and that the Communications Access Co-ordinator be required to consider a provider’s compliance with this standard as part of the Data Retention Implementation Plan process. Further, the Communications Access Co-ordinator should be given the power to authorise other robust security measures in limited circumstances in which technical difficulties prevent encryption from being implemented in existing systems used by service providers.</td>
<td>Proposed section 187BA Reference to proposed 187BA inserted into proposed sections 187D, 187E, 187F and 187K</td>
</tr>
<tr>
<td><strong>38</strong></td>
<td>The Committee recommends introduction of a mandatory data breach notification scheme by the end of 2015.</td>
<td></td>
</tr>
<tr>
<td><strong>39</strong></td>
<td>The Committee recommends that, following consideration of the recommendations in this report, the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be passed.</td>
<td></td>
</tr>
</tbody>
</table>
Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Warning: All viewers of this digest are advised to visit the disclaimer appearing at the end of this document. The disclaimer sets out the status and purpose of the digest.