Chair's Minority Additional Comments

Access to telecommunications data

1.1 In addition to a regime that allows for warranted access to telecommunications content (as discussed in Chapter 3), the *Telecommunications (Interception and Access) Act* 1979 (TIA Act) also provides for agencies to access telecommunications data (metadata). A key difference between the regimes is that access to this data does not require a warrant; instead an 'authorised officer' (defined below) within an 'enforcement agency' can authorise access.[1] In considering whether or not to grant an authorisation, an 'authorised officer' is required by law to give consideration to privacy.

1.2 These additional comments discuss the ability of 'enforcement agencies' to access telecommunications data via authorisation and considers whether there is a need for change. The terms 'telecommunications data' and 'metadata' are used interchangeably.

An overview of the telecommunications data access regime

1.3 Part 13 of the *Telecommunications Act 1997* (Telecommunications Act) imposes obligations on 'eligible persons' to protect the confidentiality of information relating to the contents of communications and the affairs and personal particulars of other persons.[2]

1.4 The term 'eligible person' is defined in section 271 of the Telecommunications Act. 'Eligible person' for the purposes of Part 13 of the Telecommunications Act is: a carrier; or a carriage service provider; or an employee of a carrier; or an employee of a carriage service provider; or a telecommunications contractor; or an employee of a telecommunications contractor.

1.5 If these provisions are breached, the 'eligible person' is guilty of an offence. However, the TIA Act sets out circumstances where the relevant sections in Part 13 of the Telecommunications Act[3] will not prohibit the disclosure of information or a document.[4] These circumstances are set out in Division 3 (in relation to ASIO), Division 4 (in relation to 'enforcement agencies') and Division 4A (in relation to foreign law enforcement) of Chapter 4 of the TIA Act.

---

1 'Enforcement agency' is defined in section 5 of the TIA Act. Notably it includes any body whose functions include: (i) administering a law imposing a pecuniary penalty; or (ii) administering a law relating to the protection of public revenue. See also: paragraph 3.10 of Chapter 3 which sets out the definition.

2 See sections 276, 277 and 278, Telecommunications Act.

3 Sections 276, 277 and 278, Telecommunications Act.

4 However, the TIA Act does not permit the disclosure of this information if it is the contents or substance of a communication, or a document to the extent that the document contains the contents or substance of a communication. See: section 172, TIA Act.

1.6 The Division 4 provisions specify that 'enforcement agencies' can access telecommunications data by prescribing that an 'authorised officer' of an 'enforcement agency' may authorise disclosure of specified information if the disclosure of the information would be 'reasonably necessary' for:

- enforcement of a criminal law;[5] or
- enforcement of a law imposing a pecuniary penalty or for the protection of public revenue.[6]

1.7 Before making an authorisation under Division 4, the authorised officer is required, by section 180F of the TIA Act, to have regard to:

> [W]hether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters: (a) the likely relevance and usefulness of the information or documents; (b) the reason why the disclosure or use concerned is proposed to be authorised.[7]

1.8 As set out in Chapter 3, submitters raised concerns in relation to the standardisation of the proportionality tests used across the TIA Act given that the proportionality test applied in authorising access to telecommunications data is significantly lower than the proportionality test involved in seeking to intercept live communications or access stored content. In the case of content, the proportionality test relates back to serious offence and serious contravention respectively. In the case of authorising access to telecommunications data, a much lower threshold can be established by linking necessity of accessing the information with 'enforcement of a law imposing a pecuniary penalty or for the protection of public revenue'.

What is telecommunications data?

1.9 The term 'telecommunications data', also referred to as metadata, communications data and communications associated data, is not defined in the TIA Act. However, the term is generally accepted as being 'information about the process of a communication, as distinct from its content'.[8]

1.10 The department explained that although 'telecommunications data' is not defined in the Act, the term has 'come to encompass a broad range of different types of information' and that the department uses a working definition.[9] The working

---

5 Section 178, TIA Act.

6 Section 179, TIA Act. Division 4 of the TIA Act also provides for authorised officer of the Australian Federal Police or a state police force to authorise disclosure for the purposes of locating missing persons and for an authorised officer of a criminal law enforcement agency to authorise access to prospective information if satisfied that disclosure of the information is reasonably necessary for the investigation of: a serious offence; or an offence against the Commonwealth, a state or territory law punishable by imprisonment for at least three years.

7 Section 180F, TIA Act.

8 Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 Annual Report 2012-13*, p. 44.

9 Attorney-General's Department, *Submission 26*, p. 21.

definition is: information or documents that are not the content of a communication, and includes the following types of information, which fall into the following two categories and relate to communications for telephones (both fixed and mobile) and the internet:

- Information that allows a communication to occur:
  - the internet identifier (information that uniquely identifies a person on the internet) assigned to the user by the provider;
  - for mobile service: the number called or texted;
  - the service identifier used to send a communication, for example the customer's email address, phone number or VoIP number;
  - the time and date of a communication;
  - general location information, that is, cell tower; and
  - the duration of the communication.
- Information about the parties to the communications is information about the person who owns the service. This would include:
  - name of the customer;
  - address of the customer;
  - postal address of the customer (if different);
  - billing address of the customer (if different);
  - contact details, mobile number, email address and landline phone number; and
  - same information on recipient party if known by the service provider.[10]

1.11 Section 172 of the TIA Act makes it clear that access to telecommunications data is not intended to allow access to the content or substance of a communication. The committee heard, however, that what is now captured as telecommunications data is a far broader subset of information than was captured in 1979. Appendix 4 sets out an example, provided by iiNet Limited, of the telecommunications data that is generated by a website, a Facebook page and a tweet.

1.12 Electronic Frontiers Australia argued that this technological change has altered the nature of metadata to the extent that telecommunications metadata, in many circumstances, is more sensitive than the content of a communication:

> In terms of looking at the current context of where we are compared to when this Act was written in 1979, obviously there have been a few changes in the way people communicate…In line with that, we reject pretty strongly the assertion that taking the powers of this Act from 1979, a

10 Attorney-General's Department, *Submission 26*, p. 46. The department expressly stated that the definition of telecommunications data 'does not include information relating to a person's web browsing or the contents or substance of their communications'. See: *Submission 26*, p. 46.

> context where mobile phones did not exist and the internet was still a pipedream, and extending those powers into a context of ubiquitous mobile devices and internet usage is not in any way a logical extension of the law to, as it were, keep up with technology on a like-for-like basis. We strongly believe that in fact this represents a very dramatic escalation of surveillance deep into all aspects of people's lives and goes far beyond anything originally envisaged when this act was drafted.[11]

1.13 Electronic Frontiers Australia provided the following example of the extent to which the volume of metadata had changed since 1979:

> [W]hen this Act was originally drafted, the information that you would get would be the fact that a phone call was made from No. A to No. B at a certain time and lasted a certain duration. That is four pieces of information. As soon as you widen that into a mobile phone context, all of a sudden you have got a location at each point, which is an entirely new thing, where literally people's locations can be tracked. Then, if you go beyond that into non-telephonic communications, all of a sudden the amount of information that has been collected starts to explode. You start to have potentially dozens, if not hundreds, of different points of data that can tell all sorts of things about what is going on. It is really quite a different scale, a different scope, a different context, and it needs to have very different rules.[12]

1.14 The Internet Society of Australia (ISOC-AU) was of a similar view and stated that it could not agree with the argument that metadata is not content:

> Over recent times much discussion has also taken place on metadata, with assertions that metadata does not include the content of communication. We contend that, without appropriate technological standards defined by an independent standards body, this claim is inherently untrue. Information gathered by existing mechanisms about the material that transits across an internet network—for example, by using the web page addresses visited by a user—inherently contains specific addresses for many, many elements within the page, even third-party elements in turn requested by the page, such as advertising.
>
> Thus, the amount revealed about an individual, their family, workmates and broader community is potentially very large. In many cases also this data is dynamic and changes from moment to moment, and often today even depends on the types of other sites visited by users, with the advent of cookie correlation—none of which is under any control by the individual users. This is further complicated by the emergence of apps, where users

11 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 35.

12 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 38.

> have extremely little knowledge of the level of security or the pervasiveness and the types of actions going on in the background.[13]

1.15 The department acknowledged that changes in technology did have implications for identifying the distinction between telecommunications data and content:

> At times, the distinction between 'telecommunications data' and 'content of a communication' may become less clear. This is particularly the case for information that, while not obviously the 'substance' of a communication, could contain or reveal substantive information, such as:
>
> - email subject lines—subject lines can be used to convey the substance of a communication, and
> - Uniform Resource Locators (URLs)—the details of which web page a person visited can reveal the content that a person accessed.[14]

1.16 The department informed the committee that in situations where it is unclear, its advice to agencies, industry participants and the public, has been that:

> [A]ny information that contains or reveals the content of a communication is protected by the prohibitions on interception and access to content under sections 7 and 108 of the TIA Act.[15]

Using telecommunications data

1.17 As set out in Division 4 of Chapter 4 of the TIA Act, access to telecommunications data by authorisation is intended to be used when disclosure is considered reasonably necessary for the enforcement of a criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.

1.18 Throughout its inquiry, the committee heard that the use of telecommunications data by law enforcement agencies is often vital in subsequently establishing the grounds for obtaining access to the content of a communication, via warrant, pursuant to Chapter 2 or 3 of the TIA Act. For example, the Australian Commission for Law Enforcement Integrity (ACLEI), explained the usefulness of metadata in the early stages of an investigation:

> I would like to emphasise the importance of access to data at the preliminary stages of an investigation. Investigations such as Operation Heritage seek to uncover the full extent of a corrupt network, but often start with only snippets of information or credible allegations. Data about who a person of interest is talking to is often a critical first step that provides a foundation for further investigation including, at a much later stage, seeking

---

13 Ms Narelle Clark, President, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 32. ThoughtWorks expressed similar views explaining that technology has changed communications such that 'really there is no distinction between metadata and content'. See, Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 4.

14 Attorney-General's Department, *Submission 26*, p. 45.

15 Attorney-General's Department, *Submission 26*, p. 45. Sections 9 and 108 of the TIA Act prohibit access to communications and therefore access would require a warrant.

> a warrant for interception. It also allows us to rule out at an early stage people who are unlikely to be complicit, thereby preventing the need for unnecessary investigation and deeper intrusion of privacy.[16]

1.19 Queensland Police expressed a similar view regarding the utility of telecommunications data:

> The warrantless data we capture regularly is used to in order to assist you reaching the threshold to obtain the warrant, so in nearly all cases you would be using the warrantless information to assist you to gather the information which aided you to reach the threshold you needed to obtain the warrant for telephone interception. That is one of its most common uses. Obtaining data from your phone that is able to tell us about connections between people at different times, aids in painting the picture which, added with other intelligence and evidence, raises you to the threshold of being able to obtain a warrant. That is one of those distinctions I think we need to make between the warrantless and warrant based processes.[17]

1.20 The Board of the ACC similarly described to the committee how, in its view, accessing telecommunications data without a warrant enables law enforcement agencies to only seek access to content (via a warrant) where necessary:

> [W]hat [telecommunications data] often does is confirm someone's involvement in crime. After that confirmation we often go to the next level, which is obtaining a warrant et cetera for content. So at a fundamental level what it often does for us is confirm that a person is involved with a group of people who are committing, for example, organised crime. Then we build on that as far as obtaining a warrant for content down the track. Fundamentally what it is used for is that confirmation of involvement. I think it was mentioned by one of my colleagues that it should not be underestimated how many citizens are excluded from ongoing intrusive law enforcement interests because of that fundamental check. It [is] still sensitive information—there is no question about that—but we do exclude a considerable number of people in that first-step process.[18]

1.21 The Board of the ACC emphasised that it understood the need to protect metadata and expressed its view that this data, although not content, is by no means 'innocuous':

> We do not believe that this is innocuous. We accept that you can build a picture. What we are saying is that it is a building block in many ways for further, more intrusive powers which are, quite appropriately, warranted. It

16 Mr Philip Moss, Integrity Commissioner, Australian Commission for Law Enforcement Integrity, *Committee Hansard,* 23 April 2014, p. 6.

17 Assistant Commissioner Peter Crawford, Queensland Police Force, *Committee Hansard*, 22 April 2014, p. 15.

18 Mr Paul Jevtovic APM, Acting Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 22 April 2014, p. 16.

> is not open for us to access that information without thresholds having been crossed. They are not inconsiderable thresholds that we have to cross.[19]

1.22 A similar view was expressed by Mr Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra. Mr MacGibbon, a former federal agent with the AFP:

> …impress[ed] upon the committee the extreme and extraordinary importance of metadata to assist law enforcement investigations. However, anyone who accesses metadata from a law enforcement point of view understands the gravity and the granularity of the information that is provided.[20]

1.23 The department explained to the committee that telecommunications data has a 'set of irreplaceable characteristics that often make it the most appropriate tool for agencies'. The department identified these characteristics as being:

- it is low risk—unlike the use of undercover officers, informants or physical surveillance, agencies can obtain valuable information without placing their officers, agents or operations at risk
- it is less resource intensive—many other investigative techniques would require agencies to deploy teams of specialist officers to obtain basic information about a target and their associates; lawful access to telecommunications data allows agencies to prioritise the use of these scarce resources for the most critical investigations, and
- it is less privacy intrusive—telecommunications data allows agencies to obtain factual information about communications, such as with whom, when and where a person was communicating, which is useful at the early stages of an investigation. However, as telecommunications data does not include the content of a communication it does not disclose more sensitive information about a person's motivations or intentions, such as what a person was talking about or why they were communicating.[21]

Growth in access to telecommunications data

1.24 Throughout the inquiry, the committee received evidence from submitters critical of the growing number of authorisations being issued to 'enforcement agencies'

---

19 Acting Commissioner Andrew Colvin, Australian Federal Police, *Committee Hansard,* 22 April 2014, p. 15.

20 Mr Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra, *Committee Hansard*, 26 September 2014, p. 26.

21 Attorney General's Department, *Submission 26,* p. 22. The department also explained that in the case of cybercrime investigations—such as, online fraud, identity theft and child exploitation investigations—law enforcement agencies rely heavily on telecommunications data. Cybercrime includes: crimes where computers or other communications technologies are integral to the offence, such as online fraud, identity theft and the distribution of child exploitation material, and crimes targeting computers, such as hacking or unauthorised access to data. See: *Submission 26*, p. 22.

for access to telecommunications data. Illustrating the extent of the use of authorisations, for the 2012-13 financial year the department reported that:

- law enforcement agencies[22] authorised access to telecommunications data in 312,929 cases;
- Commonwealth enforcement agencies[23] made 6,254 authorisations for access to telecommunications data; and
- state and territory enforcement agencies[24] authorised access to telecommunications data on 691 occasions.[25]

1.25 Given the growth in access to metadata the view that all telecommunications data should be accessed by warrant, making access subject to independent judicial oversight (for example, a judge or nominated Administrative Appeals Tribunal (AAT) member), was considered throughout the inquiry.[26]

1.26 In response to this suggestion the department stated it considered:

> …that a more holistic approach, including limiting the range of agencies permitted to access traffic data and requiring such access to be subject to independent oversight…would enable Parliament to strengthen the existing regime without degrading agencies' capabilities or imposing a disproportionate burden on agencies and issuing authorities.[27]

---

22 Law enforcement agencies that accessed telecommunications data by authorisation in 2012-13 included (but is not limited to): the Australian Federal Police (AFP), Tasmanian Police, NSW Police, South Australia Police, Northern Territory Police, Victoria Police, Western Australia Police, the Australian Crime Commission, and the Australian Commission for Law Enforcement Integrity. See: p. 47 http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf (accessed 9 August 2014).

23 Some of the Commonwealth enforcement agencies that accessed telecommunications data by authorisation in 2012-13 included: the Australian Competition and Consumer Commission, Australian Securities and Investments Commission, Australian Taxation Office, Customs, Department of Health, and the Insolvency and Trustee Service of Australia (now known as the Australian Financial Security Authority). See: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf (accessed 9 August 2014).

24 Among the state and territory enforcement agencies that accessed telecommunications data by authorisation in 2012-13 were the Victorian Department of Environment and Primary Industries, Worksafe Victoria, RSPCA (Victoria), RSPCA (Queensland), Bankstown City Council, Corrective Services NSW and the Western Australia Department of Commerce. See: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf (accessed 9 August 2014).

25 http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf (accessed 9 August 2014). See: pp. 47–48.

26 See: Australian Privacy Foundation, *Submission 36*, pp. 5, 9; ThoughtWorks Australia, *Submission 5*, p. [2]; The Pirate Party, *Submission 10*, pp. 5–7.

27 Attorney General's Department, *Submission 26*, p. 22.

1.27 The department's suggestion that the threshold for access to telecommunications data be reviewed and some form of independent oversight be introduced into the regime was similar in some respects to recommendation 5 of the PJCIS's June 2013 report.

The need to review the threshold for access to telecommunications data

1.28 In its June 2013 report, the PJCIS recommended that the threshold for access to telecommunications data be reviewed with a 'focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated' as the threshold on which access is allowed.[28]

1.29 The Corruption and Crime Commission of Western Australia supported this recommendation:

> The Commission fully supports Recommendation 5 and further supports a stronger threshold for access to traffic data as opposed to a lower threshold for access to subscriber data. The Commission considers this will strengthen the privacy protections within the TIA Act.[29]

1.30 Electronic Frontiers Australia suggested that thresholds for access to telecommunications data 'should be set taking into account the principle of proportionality' and:

> …ensure that access is only available in relation to a reasonably serious offence—for example, a criminal offence attracting a certain maximum term of imprisonment or a civil offence attracting a predetermined minimum penalty—and where there is a reasonable suspicion of the people involved in such an offence.[30]

1.31 ThoughtWorks Australia similarly argued that 'the number of agencies that can access this data needs to be confined to only those truly undertaking law enforcement and national security activities'.[31]

1.32 In its submission to the inquiry, the department expressed concern with the recommendation of the PJCIS to use 'gravity of conduct' as a threshold for access on the basis that to do so would be inconsistent with Australia's international legal obligations under the Council of Europe's Convention on Cybercrime.[32] The department explained that instead of this approach it would prefer the 'imposition of

---

28 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 26.

29 Corruption and Crime Commission of Western Australia, *Submission 14*, p. 11.

30 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

31 ThoughtWorks Australia, *Submission 5*, p. [2].

32 Attorney General's Department, *Submission 26*, p. 21. The AFP raised similar concerns in relation to the Council of Europe Convention on Cybercrime. See: *Submission 25*, Attachment E, p. 3.

safeguards, including restricting the range of agencies permitted to access such data'[33] and that options be explored to:

> - create certainty about which agencies are permitted to access account-holder data or traffic data
> - ensure that agencies accessing any type of telecommunications data have a demonstrated need to do so, and
> - ensure that all agencies with data-access powers are subject to appropriate oversight…[34]

1.33 The Australian Privacy Commissioner, Mr Timothy Pilgrim, however, in his evidence in respect of the mandatory data retention Bill currently before Parliament noted that if proportionality considerations are not considered in reviewing the threshold for access to telecommunications data, additional safeguards may be required in the legislation:

> In my submission, I did not advocate for the imposition of warrants. I took this position on the proviso that the bill be amended to limit the purposes for which telecommunications data can be used and disclosed to the investigation of serious crime and threats to national security. However, since lodging that submission, I note that the Attorney-General's Department has suggested that to meet Australia's obligations under the Council of Europe's cybercrime convention access to telecommunications data cannot be limited in this way. If that is the case then I consider that further thought needs to be given to what additional safeguards might be put in place when access is for the purpose of investigation of minor offences.[35]

1.34 Similar concerns were raised by the Parliamentary Joint Committee on Human Rights (PJCHR) during its examination of the Bill and led that committee to recommend that the Bill be amended:

> …so as to avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of any offence…to limit disclosure authorisation for existing data to where it is 'necessary' for the investigation of specific serious crimes, or categories of serious crimes.[36]

1.35 The committee heard from other stakeholders that were supportive of reviewing the threshold for access to telecommunications data as suggested by the PJCIS. For example, Blueprint for Free Speech expressed its support for a review stating:

---

33 Attorney General's Department, *Submission 26*, p. 21.

34 Attorney General's Department, *Submission 26*, p. 21.

35 Mr Timothy Pilgrim, Australian Privacy Commissioner, *House of Representatives Committee Hansard*, 29 January 2015, p. 47.

36 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, pp. 16–17.

> …there must be proper public consultation about the detail around which agencies should have continued access to telecommunications data, and…[the] proper description of the basis for this access and the threshold for same. This information should not be concealed from the broader Australian community, and Australians must have a say in this decision process.[37]

1.36 In addition to calls for a review of the proportionality test involved in authorising access to telecommunications data, submitters also voiced support for refining the definition of 'enforcement agency' to reduce the number of agencies that could access the data without a warrant. For example, the Office of the Public Interest Monitor of Victoria supported calls for a reduction in the number of agencies accessing telecommunications data without a warrant, stating:

> There has been recent media attention and significant criticism of the ability of agencies to obtain telecommunications data and the consequential implications on the privacy of those who utilise telecommunications services. Local councils can access telecommunications data under the TIA Act on the basis that disclosure of the said data is reasonably necessary for the enforcement of a law imposing a pecuniary penalty. The matters in respect of which telecommunications data is obtained by some agencies does not appear commensurate with the invasion of privacy occasioned by the disclosure of such data. A reduction in the number of agencies able to access telecommunications data by using the gravity of the conduct which may be investigated utilising telecommunications data as a threshold on which access is allowed is supported.[38]

1.37 The Australian Mobile Telecommunications Association (AMTA) and the Communications Alliance advised the committee that there was a need for 'clarity around which agencies are eligible to have access to telecommunications data' and that this could result in cost efficiencies for industry.[39]

1.38 The Internet Society of Australia (ISOC-AU) was of a similar view:

> The existing provisions do not make clear which agencies have the right to gain access to metadata. Should metadata be defined then there must be a clear understanding of which agencies are eligible to access communications information, and the proportionality of [the] suspected crime must also be correspondingly high.[40]

1.39 Electronic Frontiers Australia also suggested that the highly invasive nature of this information warranted tighter restrictions to access:

> …and, ideally, a clearly defined list of agencies that are able to request access to data. As mentioned, there may be cases where agencies outside that list can apply via an approved agency, as it were, to do that, but we

---

37 Blueprint for Free Speech, *Submission 4*, pp. 3–4.

38 Office of the Public Interest Monitor Victoria, *Submission 17*, p. 5.

39 AMTA and the Communications Association, *Submission 16*, p. 6.

40 Ms Narelle Clark, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 33.

> think that there do need to be some very tight restrictions around that. We also agree that there should be very tight, very stringent and very clearly defined thresholds for access to data.[41]

1.40 It is noted that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 which is currently before Parliament, seeks to limit the number of agencies that can access telecommunications data by redefining 'enforcement agency'. The Bill, however, does not address the need to review the proportionality test in respect of accessing telecommunications data.

Introduction of oversight for telecommunications data

1.41 In addition to calls for a review of the threshold for access to telecommunications data, the committee repeatedly heard concerns raised by stakeholders about the lack of oversight and transparency in the telecommunications data access regime.

1.42 Under the existing legislative framework, telecommunications data can be accessed by any agency that meets the definition of 'enforcement agency', (which includes 'a body whose functions include: (i) administering a law imposing a pecuniary penalty; or (ii) administering a law relating to the protection of public revenue'),[42] where the disclosure is considered reasonably necessary for the enforcement of the law or the protection of public revenue and the authorised officer has had regard to the privacy implications of the disclosure.

1.43 Unlike the warrant regimes of Chapters 2 and 3 of the TIA Act, Chapter 4 of the TIA Act does not contain any legislative framework for direct oversight of the authorisation process. Similarly, the legislation does not require that information accessed must be destroyed when it is no longer necessary, unlike the Act's requirements for content[43] and as is required by Australian Privacy Principle (APP) 11.[44]

---

41 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36. This suggestion was also made by Mr Alastair MacGibbon (see, *Committee Hansard*, 26 September 2014, p. 26) and Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (see, *Committee Hansard*, 26 September 2014, p. 18).

42 Section 5, TIA Act.

43 Section 79 of the TIA Act and section 150 of the TIA Act prescribe that 'restricted records' (any information obtained by interception) and records or information obtained by accessing a stored communication are required to be destroyed if it is no longer likely to be required.

44 Australian Privacy Principle (APP) 11—security of personal information:

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure.

1.44 There are reporting requirements for access to data. The TIA Act requires the 'enforcement agency' to keep a record of authorisations and report those to the Minister at the end of each year. Although the number of authorisations is published in an annual report tabled by the Minister, no further detail is provided. As the authorisation process occurs internally within each enforcement agency, there is no external oversight of or transparency about how agencies are complying with the obligations to balance access with privacy.

1.45 The Commonwealth Ombudsman, who has a role in overseeing warranted access to telecommunications content, commented on the lack of oversight of access to telecommunications data. The Ombudsman explained that his office did not have any inspection role in relation to metadata and agreed that the oversight and reporting regime for telecommunications data could be improved. He suggested that there may also be an educational role that his office could play.[45] The then Secretary of the Attorney-General's Department also explained that in his view there was a need for greater transparency in relation to the authorisation process for accessing telecommunications data.[46]

1.46 The figures outlined at paragraph 4.24 indicate that, if the Commonwealth Ombudsman were to have a role in relation to inspecting access to metadata, his office would face an enormous workload. However, the Ombudsman suggested that the resourcing challenges presented by the number of authorisations for access to metadata that would need inspection could be met by an 'appropriate sampling program':

> That would be the normal approach to a volume responsibility along those lines. And then, if we form some views, they would need to be couched in language which said we had done that which we could, in the circumstances with which we are confronted.[47]

1.47 An officer from the Commonwealth Ombudsman added that in addition to a sampling program:

> …we would have to look at the risks associated with that inspection regime. It may well be that the most appropriate means would be looking at processes rather than focusing on records per se, so looking at high-level

---

11.2 If: (a) an APP entity holds personal information about an individual; and (b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and (c) the information is not contained in a Commonwealth record; and (d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information; the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified. Source: Part 4 of Schedule 1 to the *Privacy Act 1988*.

45 Mr Colin Neave, Commonwealth Ombudsman; Mr Simon Pomery, Assistant Director, Commonwealth Ombudsman, *Committee Hansard*, 23 April 2014, pp. 29–30.

46 Mr Roger Wilkins AO, Secretary, Attorney-General's Department, *Committee Hansard*, 23 April 2014, p. 4.

47 Mr Colin Neave, Commonwealth Ombudsman, *Committee Hansard*, 23 April 2014, p. 29.

> processes in combination with doing a sample may alleviate some of the risks that would occur from not looking at a greater number.[48]

1.48 Electronic Frontiers Australia expressed its support for the introduction of a better oversight and reporting regime in relation to access to telecommunications data:

> We also support calls for more detailed reporting of access to data…We also see no reason why access to communications data by intelligence agencies should not be reported…at least on a statistical basis. We cannot see any harm in doing that. We agree that there needs to be more effective external and independent oversight of this process. We would also suggest that there need to be very clear rules about what happens to data that has been accessed through this process, how long it is retained by the agencies and how it is disposed of and so forth.[49]

1.49 The Chair notes that the government has proposed changes to the oversight arrangements for accessing telecommunications data by authorisation in the Bill currently before Parliament. This is discussed in more detail later.

Should access to 'telecommunications data' require a warrant?

1.50 It is widely considered that there is a need to review the threshold for access to telecommunications data accessed without a warrant. Some witnesses suggested to the committee that the need for such a review in the context of a legislative framework mandating retention of defined data attributes has become even more important. For example, the Australian Privacy Foundation explained:

> In terms of metadata, I think it is easy, when we say 'All metadata should be covered by warrants', for the law enforcement agencies to come back and say, 'That's completely ridiculous; it's administratively impossible for us to go for warrants for all of those 320,000 authorisations.' I think one of the questions that needs to be asked is: how many of those are just for customer name and address? I do not think any of us are suggesting that you should have to go for a warrant just to say to a telco, 'Do you have a customer Nigel Waters?' So, we could get rid of that sort of furphy and say that maybe 50 or 60 per cent of requests are in that category and that it is no different from any other business that the police might go to and ask for customer information. But when you get into the details of their billing records, their transactions and all the other associated metadata, then it is our position that that should be subject to the warrant regime.[50]

1.51 This view was supported by Electronic Frontiers Australia:

> We support the implementation of a warrant process for access to metadata in any substantive form…outside of simple customer information. We do

48 Mr Simon Pomery, Assistant Director, Commonwealth Ombudsman, *Committee Hansard*, 23 April 2014, p. 29.

49 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

50 Mr Nigel Waters, Australian Privacy Foundation, *Committee Hansard*, 29 July 2014, p. 31.

> not think there is a need for wider access to that, but for anything involving any substantive amount of metadata we would certainly support that.[51]

1.52 The MEAA explained that it agreed with the extension of the warrant regime to data which is 'information that allows a communication to occur',[52] on the basis that such an approach would provide valuable protections for journalists:

> Clearly, being required to get a warrant-anything that raises the bar to access this information is obviously very valuable. It also would then require them [law enforcement agencies] to answer certain questions that a judge would have to ask under the Evidence Act in terms of confidentiality of sources. For example, if you are seeking a warrant to get metadata about a particular journalist's phone, then they [the agency] would also have to jump through the hoops under the shield laws.[53]

1.53 Calls for requiring access to telecommunications data to be restricted via warrant or changes to the definition of 'enforcement agency' are largely the result of changes to metadata brought about by advancing technologies and the view of stakeholders that in many circumstances, metadata should be regarded as the equivalent of content.[54]As a result, it is in this context that the debate around accessing metadata via an authorisation, rather than warrant needs to be had.

1.54 This section outlined the existing legislative framework that provides for enforcement agencies to access telecommunications data by means of an authorisation. It discussed evidence received which indicated that information captured as telecommunications data today is far greater and more revealing than the information which was available when the Act was first introduced pointing to a need for reform. Reform of access to telecommunications data becomes even more important in light of calls for mandatory data retention, which is discussed in in the next section of these additional comments.

---

51 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

52 'Information that allows a communication to occur' would include: the internet identifier assigned to the user by the provider; for mobile phone services – the number called or texted; the service identifier used to send a communication; the time and date of a communication; general location information/cell tower; and the duration of the communication. See, paragraph 4.10.

53 Mr Christopher Warren, Media, Entertainment and Arts Alliance, *Committee Hansard*, 21 July 2014, p. 23.

54 For more discussion refer to paragraphs 4.11 to 4.14.

Chair's views and recommendations: existing regime for authorising access to telecommunications data

1.55 The Chair's views and recommendations set out below are made in respect of his findings on the current form of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

1.56 The Chair acknowledges the enormous complexity involved in updating telecommunications interception legislation and recognises that the issues involved are technical and challenging. In forming these recommendations, the Chair has been guided by the underlying premise that the individual right to privacy must be balanced with the need to ensure community safety and national security. However, there are difficult compromises to be struck between these competing rights, as well as a range of practical considerations affecting both law enforcement agencies and telecommunications providers. Notwithstanding these difficulties, the existing TIA Act is complex and difficult to navigate; it should be re-written.

1.57 The need for reform has arisen as a result of piecemeal amendments over a 35 year period. Although these legislative changes sought to respond to the needs of law enforcement and anti-corruption bodies, they have not sufficiently considered the impact of parallel advancements in technology.

1.58 Evidence to the committee clearly illustrated that ad-hoc reform in the absence of consideration of changing technologies has resulted in a regime characterised by complexity, duplication and, in some cases, inadequate oversight and privacy protections. Moreover, it has led to an inexorable creep in the range of agencies permitted to access intercepted material and the purposes for which they are permitted to do so. As a result, the Chair considers that comprehensive reform of the telecommunications legislation is required, particularly so the legislation is well-placed to deal with the continued evolution of telecommunications technology and usage. Continued piecemeal amendment of the existing TIA Act is not feasible.

1.59 The Chair sees merit in the introduction of a single attribute-based warrant regime for content and metadata that is 'information that allows a communication to occur', but notes that a carefully considered definition of the attributes included and an appropriate proportionality test is required.

1.60 The introduction of a single attribute-based warrant regime should be coupled with the introduction of a Commonwealth public interest monitor and a review of the oversight regime governing both warranted and warrantless access. The Law Council of Australia provided examples of specific legislative changes that could be incorporated which the Chair considers would address the concerns of stakeholders in respect of oversight of the warranted access regime.[55] The Chair recommends that consideration be given to the evidence taken during this inquiry regarding the design of a single attribute-based warrant regime.

55 Law Council of Australia, *Supplementary Submission 34*, p. 2.

1.61 The Chair agrees with calls for an objects clause clearly articulating the purpose of the Act and its dual objectives of providing access to communications content and data to enable the investigation of serious crime and threats to national security and protecting the privacy of communications.

1.62 The Chair was persuaded that the introduction of a Commonwealth Public Interest Monitor, serving a similar role to that played in Queensland and Victoria, would help ensure that the introduction of attribute-based warrants does not reduce privacy protections under the existing regime.

Recommendation 1

1.63 The Chair recommends that the *Telecommunication (Interception and Access) Act 1979* be amended to include an objects clause modelled on Article 17 of the International Convention on Civil and Political Rights and the privacy principles contained in the *Privacy Act 1988*.

Recommendation 2

1.64 The Chair recommends that the *Telecommunication (Interception and Access) Act 1979* be comprehensively redrafted to enact a single attribute-based warrant regime applying to content and data that is 'information that allows a communication to occur'. Warrants under that regime should be limited to the investigation by law enforcement, anti-corruption or national security agencies of:

- **serious criminal activity; or**
- **activity that may have serious and immediate implications for national security.**

1.65 'Basic subscriber data' would continue to be accessed by enforcement agencies via the authorisation regime.

Recommendation 3

1.66 The Chair recommends that the *Telecommunication (Interception and Access) Act 1979* should be amended to establish a Commonwealth Public Interest Monitor to have oversight of the warrant regime under the Act.

Mandatory data retention

This section examines the policy of mandatory data retention in the context of the government's proposed regime set out in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. The terms 'telecommunications data' and 'metadata' are used interchangeably.

Background

1.67 In 2012, when requesting that the Parliamentary Joint Committee on Intelligence and Security (PJCIS) undertake an inquiry into a package of potential reforms to Australia's national security legislation, the then Attorney-General directed the PJCIS to consider:

> Applying tailored data retention periods for up to 2 years for part of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts.[56]

1.68 In its June 2013 report, the PJCIS stated that it had 'grappled with the issue of how best to reconcile the important national security interests…and on the other hand…the very significant alteration of the relationship between the state and the citizen, which the introduction of such a regime would arguably involve'.[57] That committee did not form a view on the need for the introduction of mandatory data retention, but rather, stated that the matter should be left for government.[58]

1.69 On 30 October 2014, the Abbott Government introduced the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Bill) into the House of Representatives.[59] On introducing the Bill, the Minister for Communications explained:

> The bill contains a package of reforms to prevent the further degradation of the investigative capabilities of Australia's law enforcement and national security agencies. The bill will require companies providing telecommunications services in Australia, carriers and internet service providers to keep a limited, prescribed set of telecommunications data for

---

56 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 139.

57 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 190. The PJCIS noted in its report that its task was made more difficult in the absence of any draft legislation.

58 In noting that mandatory data retention should be a decision for government, the PJCIS did recommend that if the government was persuaded to introduce a mandatory data retention regime, an exposure draft of the proposed legislation should be referred to the committee for examination. See: PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, pp. 192–193.

59 The Hon Malcolm Turnbull MP, Minister for Communications, *Votes and Proceedings*, Thursday 30 October 2014, p. 951.

> two years. The bill amends the *Telecommunications Interception and Access Act 1979*…and the *Telecommunications Act 1997*…[60]

1.70 The proposed mandatory data retention regime set out in the Bill would introduce a requirement that telecommunication service providers in Australia retain telecommunications data (metadata) for a period of two years. Rather than define 'telecommunications data', the Bill would 'allow regulations to prescribe a consistent, minimum set of records that service providers who provide services in Australia must keep for two years'.[61] Under the Bill, content and web browsing data would be specifically excluded from the retention requirement.[62]

1.71 The Bill also proposes a new definition of 'enforcement agency' and 'criminal law enforcement agency' for the purposes of existing Chapter 4 (accessing telecommunications data) and Chapter 3 (in relation to preservation notices) of the TIA Act. The proposed definitions, which would seek to limit the number of agencies that can access this data, include the introduction of a ministerial discretion that would enable the Minister to declare an agency to be an 'enforcement agency' or 'criminal law enforcement agency' for the purposes of the Act.[63]

1.72 In addition, the Bill proposes the introduction of a new oversight regime for the Commonwealth Ombudsman where the Ombudsman would oversee the authorisation regime, including an obligation to report annually on the regime to the Minister and the Parliament.[64]

Why is mandatory data retention being proposed?

1.73 Telecommunications data is generally collected as a matter of course by carriers and carriage service providers in the provision of communication services. This information has traditionally been used for billing purposes. However, as technology and the way in which services are provided has changed, this data is no longer always required for business purposes and in some instances is not being retained at all. This has led to calls, primarily from national security and law enforcement agencies, for the introduction of a mandatory data retention regime. It also explains the view of those agencies that, what would be required is not the introduction of a new obligation, but rather the mandating of data to ensure consistency in the data set retained, both in terms of data and the period of retention. This is reflected in the Bill currently before Parliament.

1.74 In his second reading speech the Minister explained the government's view of the vital role of metadata to public and national security:

---

60 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12560.

61 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12561.

62 Proposed new subsection 187A(4).

63 Proposed new sections 110A and 176A.

64 Proposed new sections 186A to 186J.

> Access to metadata plays a central role in almost every counterterrorism, counterespionage, cybersecurity and organised crime investigation. It is also used in almost all serious criminal investigations, including investigations into murder, serious sexual assaults, drug trafficking and kidnapping. The use of this kind of metadata, therefore, is not new. However, as the business models of service providers are changing with technology they are keeping fewer records. And they are keeping those records for shorter periods of time because they do not need them any longer, in many cases, for billing. Many of the records that are still kept are kept because of legacy systems put in place years ago. In June 2013, the Parliamentary Joint Committee on Intelligence and Security concluded that this diminution in the retention of metadata is harming law enforcement and national security capabilities, and that these changes are accelerating.[65]

1.75 Throughout its inquiry the committee received much evidence from law enforcement agencies indicating universal support for the introduction of mandatory data retention for the reasons cited by the Minister. For example, the Board of the Australian Crime Commission (ACC), in stating its support for a regime that required data to be retained for a 'uniform length of time across all telecommunication service providers', explained:

> Telecommunications data is an effective and efficient tool used by law enforcement to identify and investigate organised criminal activity and serious crime and reveal the true extent of a criminal network which would otherwise remain unknown.[66]

1.76 Victoria Police, another advocate for mandatory data retention, voiced strong support for the implementation of such a regime 'given the changes in the patterns of community usage of mobile phones (being that many persons use mobile phones daily and frequently for conversations or internet access) and changes in industry business practices'. Victoria Police added:

> …in many instances, carriers only retain data for commercial purposes such as billing. Data which is of interest to law enforcement is often not retained. Where data is retained, it is for varying periods of time. The community expectation for criminal activity to be sufficiently investigated and prosecuted justifies data retention to mitigate the risk that evidence will be unavailable.[67]

1.77 The Australian Commission for Law Enforcement Integrity (ACLEI) also supported calls for mandatory data retention:

> ACLEI sees merit in a legislated data retention requirement on telecommunications service providers, which would provide clarity as to how long a period of time service providers will retain telecommunications

---

65 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard,* 30 October 2014, p. 12560.

66 Mr Paul Jevtovic APM, Acting Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 22 April 2014, p. 9.

67 Victoria Police, *Submission 6*, p. 4.

> data, and ensure that such data can be properly accessed for law enforcement purposes. This data is already in the possession of service providers for their usual business practices, such as billing, which is generally destroyed after a short period of time.[68]

1.78 ACLEI provided an example of how the lack of a mandatory data retention regime had affected its ability to investigate corruption:

> In a recent ACLEI corruption investigation, it appeared that sensitive information about a law enforcement agency may have been unlawfully disclosed to a third party by use of an anonymous website contact form.
>
> ACLEI was able to identify the IP address of the computer from which the alleged unlawful disclosure had been made, but when ACLEI sought to match the IP address to a particular internet user, the relevant internet service provider advised that—in accordance with usual business practices—the information had been destroyed when it was no longer necessary.
>
> There were no other means available to ACLEI to match the IP address to a person. If the service provider had been under an obligation to keep its telecommunications data for more than a few months, the data might have been available to ACLEI for the purposes of the corruption investigation.[69]

1.79 Despite widespread support among law enforcement and national security agencies for the introduction of mandatory data retention, concerns have been consistently raised since such a regime was first mooted, and again, following the release of the government's proposed legislation in late October 2014. Concerns are generally related to the following three themes:

- the scope of the proposed mandatory data retention regime;
- the cost involved; and
- the privacy implications of implementing a two year retention regime.

1.80 These matters are addressed below in the context of the government's proposed regime.

Scope of the proposed mandatory data retention regime

1.81 Part 1 of Schedule 1 of the Bill seeks to insert a new Part 5-1A into Chapter 5 of the TIA Act.[70] Proposed Division 1 of Part 5-1A sets out the scope of the proposed mandatory data retention regime.

1.82 Proposed new section 187A contains the obligation on service providers to keep 'information of a kind prescribed by regulations, or documents containing information of that kind'[71] for the period prescribed by proposed new section 187C

---

68 ACLEI, *Submission 11*, p. 5.

69 ACLEI, *Submission 11*, p. 5.

70 Explanatory Memorandum (EM), p. 34.

71 Proposed new subsection 187A(1).

and identifies that the kinds of information that would be required to be retained by regulations must relate to one or more of the following matters:

> (a) characteristics of any of the following:
>
> (i) the subscriber of a relevant service;
>
> (ii) an account relating to a relevant service;
>
> (iii) a telecommunications device relating to a relevant service;
>
> (iv) another relevant service relating to a relevant service;
>
> (b) the source of a communication;
>
> (c) the destination of a communication;
>
> (d) the date, time and duration of a communication, or of its connection to a relevant service;
>
> (e) the type of a communication, or a type of relevant service used in connection with a communication;
>
> (f) the location of equipment, or a line, used in connection with a communication.[72]

1.83 The Explanatory Memorandum (EM) to the Bill sets out that telecommunications data would not be defined in the TIA Act so as to remain technology-neutral and that a 'regulation-making power is required to ensure that the legislative framework gives service providers sufficient technical detail about their data retention obligations while remaining flexible enough to adapt to future changes in communication technology'.[73]

1.84 The EM further explains 'data retention will create a consistent obligation for record-keeping across the telecommunications industry' and that although '[s]ome service providers may initially need to modify their systems to ensure they meet this minimum standard':

> The minimum obligation imposed by this legislation is consistent with the types of data and subscriber information currently held by service providers for billing, quality assurance and other business purposes.[74]

1.85 Proposed new section 187B identifies service providers that would be exempt from the data retention obligations proposed under section 187A(1). The purpose of proposed new section 187B:

> …will be to ensure that entities such as governments, universities and corporations will not be required to retain telecommunications data in relation to their own internal networks (provided these services are not offered to the general public), and that providers of communications services in a single place, such as free Wi-Fi access in cafes and restaurants

---

72 Proposed new subsection 187A(2).

73 EM, p. 36.

74 EM, p. 34.

> are not required to retain telecommunications data in relation to those services. However, the [Communications Access Co-ordinator] CAC can declare that data from such services must nevertheless be retained.[75]

1.86 The mandatory data retention regime being proposed by the government's Bill has been criticised on the basis that the:

- term 'telecommunications data' remains unclear;
- costs of implementing such a regime remain unknown; and
- retention period being proposed is arbitrary and further undermines privacy.

1.87 There has, however, been widespread support for the inclusion in the Bill of a revised definition of 'enforcement agency' (which would have the effect of limiting the number of agencies who can access telecommunications data via authorisation), and the proposed introduction of an oversight regime in respect of telecommunications data.

What is telecommunications data?

1.88 Many submitters contended that due to changes in technology, metadata (telecommunications data) should now be regarded as content. They contend that the definition of 'telecommunications data' should take this into account. Mr Steve Dalby, the Chief Regulatory Officer at internet service provider iiNet Limited, explained how the analogy of the 'envelope and the letter' no longer holds up:

> The complex, voluminous, often sensitive and private nature of the data sought under a mandatory data retention regime exposes the hollowness of the claim that communications data or metadata is 'just like the envelope without its contents'. The difficulty with such a poor analogy is that it attempts to compare a piece of paper, the envelope, with a chain of events and multiple links to myriad other data, meticulously described and recorded. In the case of Twitter, this may include who wrote the tweet, their biography, their location, when it was written, how many other tweets have been written on that user's account, where the author was when the tweet was posted, what time it was, whom it was sent to, where the author is normally based and, surprisingly in the case of Twitter, the 140 characters of the content of the tweet as well.[76]

1.89 Mr Dalby further explained to the committee that as metadata 'underlies all communications':

> It is fundamentally misleading to downplay the degree of intrusion of data retention regimes such as those that operate at the European directive level. A false assertion is that such regimes do not include the actual content of what our customers might be communicating. These inaccurate distinctions are dangerous and inappropriate. It is misleading to assert that such data is

---

75 EM, p. 47.

76 Mr Steve Dalby, Chief Regulatory Officer, iiNet Limited, *Committee Hansard*, 29 July 2014, p. 21.

> 'only metadata' or 'just metadata'. Metadata reveals even more about an individual than the content itself.[77]

1.90 Blueprint for Free Speech raised similar concerns that it is:

> …easy to try to triangulate information about a particular person, or to imply particular activities or conduct, purely from metadata. If you have enough of it you can build a story and then imply context, which is in itself dangerous.[78]

1.91 Electronic Frontiers Australia agreed with the view that 'metadata is often a proxy for content':

> We also strongly disagree with the assertion that metadata is less invasive than providing access to content. As the Attorney-General's Department itself admitted in its submission:…telecommunications data can contain particularly sensitive personal information justifying special legal protection. We completely and wholeheartedly agree with that. Clearly, it can be used to build a picture of a target, their network of associates, where they shop, where they eat, where they sleep…[79]

1.92 Mr Lawrence also cited the following research by David Seidler who made the following point about data retention:

> Although on its face, metadata might appear anonymised and trivial, the development of big data analysis techniques (for which metadata is "perfect fodder") means that the insights it provides after manipulation might well meet this definition—of being content, that is.[80]

1.93 More dramatically, Ms Lindy Stephens, Global Director of People Operations at ThoughtWorks, cited former Central Intelligence Agency (CIA) and National Security Agency (NSA) Director General Michael Hayden as having said, 'We kill people based on metadata'.[81] Ms Stephens also referred the committee to statements made by former NSA General Counsel Mr Stewart Baker that 'metadata absolutely tells you everything you need to know about somebody's life. If you have enough metadata, you don't really need content'.[82]

1.94 Industry groups cautioned the committee in respect of the potential privacy impacts on consumers of data retention. AMTA submitted that:

> [A] data retention scheme will involve an increased risk to the privacy of Australians and provide an incentive to hackers and criminals. Data

---

77 Mr Steve Dalby, iiNet Limited, *Committee Hansard*, 29 July 2014, p. 20.

78 Mr Simon Wolfe, Head of Research, Blueprint for Free Speech, *Committee Hansard*, 23 April 2014, pp. 50–51.

79 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

80 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

81 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 5

82 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 5.

> retention is at odds with the prevailing policy to maximise and protect privacy and minimise the data held by organisations.
>
> Industry believes it is generally preferable for consumers that telecommunications service providers retain the least amount of data necessary to provision, maintain and bill for services.[83]

1.95 The Media, Entertainment and Arts Alliance (MEAA) also outlined its opposition to mandatory data retention explaining that it was particularly apprehensive as to how such a regime would affect the free press:

> The inevitable impact of collection, storage and surveillance through metadata is that it will be impossible for a journalist to liaise with a source, for a source to connect with a journalist or for a journalist to connect with a source without it being be able to be found and be identified, without them going through quite extraordinary encryption processes—and, even there, I think there is probably a question mark over how effective that would be.[84]

The need for a definition of 'telecommunications data' in the primary legislation

1.96 Throughout the duration of the committee's 15 month inquiry, stakeholders consistently raised the need for a clear definition of 'telecommunications data' to be legislated, particularly in the event of the government seeking to implement mandatory data retention.

1.97 Dr Roger Clarke of the Australian Privacy Foundation identified the complexity of defining metadata, explaining to the committee:

> The term 'metadata'…derives from the library sphere. It is data about data, and it has gradually been absorbed into discussions about the internet, because obviously librarianship has moved on to the internet during the last 20 years…It merely means data about data. That is the only consolidated meaning that it has. With respect to any given communication, your answer as to what is metadata and what is content will be different. There is not one answer to: what is metadata? There are 40 or 50 answers and, in fact, some of them can be disputed at length. That has been lost in this debate. Everybody is assuming that metadata is a thing that can be legislated for. It is not technologically neutral. It is absolutely unclear what metadata will mean in each of these different contexts.[85]

---

83 Australian Mobile Telecommunications Association and the Communications Alliance, *Submission 16*, pp. 12–13.

84 Mr Christopher Warren, Federal Secretary, Media, Entertainment and Arts Alliance, *Committee Hansard*, 21 July 2014, p. 22.

85 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 2 February 2015, p. 26. Similar concerns were raised by the Internet Society of Australia (ISOC-AU): At this point in time there are…no clear technical specifications for metadata in the internet protocol world. In [classic] telephony there were call detail records which are defined under International Telecommunications Union standards...It is clear, it is simple and it is available. In the internet world that type of description does not exist for the myriad of types of communications and communication services that we have. Source: Ms Narelle Clark, President, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 35.

1.98 Other submitters also acknowledged the complexity of defining 'telecommunications data', and they too cited the importance of clearly defining the term. Mr Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra, explained:

> …defining metadata is…clearly the critical thing. What information do we consider to be metadata, in terms of the legislation, and what do we not? Once that distinction is made it becomes a much clearer picture, though it may not satisfy everyone. Metadata is anything and everything that you are really gathering; it is information from the use of technology.[86]

1.99 Electronic Frontiers Australia was of a similar view:

> It is clearly a pretty critical starting point that we get a clear definition of metadata. In the telephonic context it is fairly straightforward, but if we go beyond that into non-telephonic communications we have some very serious concerns that it is even technically feasible to effectively separate metadata from content, particularly in the case of email communications.[87]

1.100 Although stakeholders explained the need for a clear definition of 'telecommunications data' on the basis that clarity is required to ensure certainty for industry, protect privacy, and enable the costs of mandatory data retention to be accurately forecast, the Bill currently before the Parliament, while identifying the categories of information that metadata might include, relies on regulations to set out the specific details.

1.101 The Attorney-General's Department (department) explained that this approach had been taken to ensure the legislation remains technology neutral:

> The regulations provide an ability to update the dataset in the event that it is required due to changes in telecommunications services and the fundamental nature of those, and industry have told us consistently that the industries are evolving at a rapid rate and there is considerable change on the horizon. The inclusion of the dataset in regulations provides an ability to update the dataset whilst ensuring it is limited to the six key categories include on the face of the bill.[88]

1.102 Despite the department's explanation, the approach of delegating the substance of the Bill to subordinate legislation has been criticised by many stakeholders, many reiterating the need for a definition to be included in the primary legislation.[89]

---

86 Mr Alastair MacGibbon, *Committee Hansard*, 26 September 2014, p. 35.

87 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36. See also: Ms Narelle Clark, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 35.

88 Ms Anna Harmer, Acting First Assistant Secretary, National Security Law and Policy Division, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, p. 46.

89 The committee notes that Optus however 'consider[ed] the use of regulations to spell out more detail of the intended data set [was] appropriate'. Source: Optus, *Submission 86 to the PJCIS inquiry*, p. 7.

1.103 The Law Council of Australia (Law Council) stated that in its view, the delegation of the definition of telecommunications data to regulations was inappropriate:

> The Law Council's Rule of Law Principles require that where legislation allows for the Executive to issue subordinate legislation in the form of regulations, the scope of that delegated authority should be carefully confined and remain subject to Parliamentary supervision. Such a requirement ensures that Executive powers are defined by law, such that it is not left to the Executive to determine for itself what powers it has and when and how they may be used. As a matter of good legislative practice, significant matters should be specified in primary legislation which generally undergoes extensive consultation, not potentially subject to change by Ministerial decision and regulation.[90]

1.104 The Law Council further set out why it considered it inappropriate for the data set to be defined in regulations:

> The categories of information which should be captured by the scheme will raise significant questions of policy and have very substantial financial, as well as privacy, implications. The 'kinds of information' (within defined categories) that might be required to be captured and kept are uncertain. Although the Government has provided an initial proposal (in the form of a draft Regulation) the data set is still in draft form and can be changed at any time. Given that service providers can be subjected to civil penalties for failing to comply with obligations under the scheme (see for example section 187M) and the impact of the scheme on individuals, the Law Council considers that it is inappropriate for the kind of telecommunications data to be prescribed by regulations. Both the categories of the data to be retained and the specific data set should be set out in the Bill itself.[91]

1.105 In addition, the Law Council cited the report of the Scrutiny of Bills Committee which stated that 'paragraph 187A(1)(a)…inappropriately delegate[d] legislative power'[92] and accordingly, made the following recommendations:

- The Bill should clearly define the types of telecommunications data and the specific data set to be retained.
- The power to prescribe by way of regulation the mandatory data set should be removed from the Bill.
- The Bill should define the distinction between the 'content and substance' of a communication (referred to in clause 187(4)(a) of the Bill), as opposed to 'telecommunications data'.[93]

---

90 Law Council of Australia, *Submission 126 (Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014),* p. 13.

91 Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 13.

92 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 16 of* 2014, 26 November 2014, pp. 2–5. See also: Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 13.

1.106 A similar concern was raised by the Australian Human Rights Commission (AHRC) in its submission to the PJCIS inquiry. In its submission, the AHRC, while acknowledging the rationale for using regulations, stated that:

> …the definition of telecommunications data is a critical feature of the Bill and should not be left to be described by Regulations. The Commission considers that the telecommunications data required to be retained by telecommunication services providers should be included in the legislation itself.[94]

The cost of data retention

1.107 Throughout its inquiry the committee sought to establish the costs that would be involved should the government proceed with its plan to introduce mandatory data retention. At the committee's final public hearing on 2 February 2015 and after the introduction of the Bill, the department was unable to provide any indication to the committee of the possible cost of a mandatory data retention regime to taxpayers. In fact, in response to questioning as to whether or not the Parliament will know how much the scheme will cost before the Bill is debated, the department advised:

> That will ultimately be a matter for the Attorney and the government…As with all budgetary matters, it is a matter for the budget process and the government and the cabinet.[95]

1.108 On introducing the Bill, the Minister stated:

> There has also been a great deal of conjecture about how much data retention may cost…the government is committed to ongoing, good faith consultation with industry and expects to make a substantial contribution to both the cost of implementation and the operation of this scheme.[96]

1.109 On 18 February 2015, the Prime Minister, the Hon Tony Abbott MP, was quoted as saying that 'keeping the data would cost less than $400 million a year'.[97] In its report tabled on 27 February 2015, the PJCIS set out that '[i]ndicative costing estimates for industry's implementation of the data retention scheme, based on PricewaterhouseCoopers analysis, suggested that the upfront capital cost of the regime would be between $188.8 million and $319.1 million'.[98]

---

93 Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 14.

94 Australian Human Rights Commission (AHRC), *Submission 42 to the PJCIS inquiry*, p. 7.

95 Ms Katherine Jones, Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, p. 54.

96 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12561.

97 Emma Griffiths, ABC News, 'Data retention plan could cost almost $400 million a year, Tony Abbott says', 18 February 2015, http://www.abc.net.au/news/2015-02-18/data-retention-plan-could-cost-almost-400-million-a-year/6139078 (accessed 3 March 2015).

98 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 182.

1.110 Throughout the course of its inquiry, the committee did however receive evidence from industry participants of the predicted costs associated with the implementation of such a regime. The committee heard that the lack of clarity around what was being proposed, and therefore the costs that the imposition of a mandatory data retention regime may have for industry participants, were of great concern. The Australian Mobile Telecommunications Association (AMTA) and Communications Alliance explained industry's apprehension and its views in relation to these matters as follows:

> …the cost of retaining data beyond any period it would be retained in the normal course of business must be borne by the agencies that require it. Similarly, any costs in relation to security, storage and ability to search retained data must also be borne by the agencies that require it. The Associations note that keeping more data or keeping data for longer periods, may add to costs significantly whereas the added benefits may be incremental, at best.
>
> …The costs of acquiring and retaining particular items of data will vary widely, as will the benefits to [law enforcement and national security agencies] LENSAs.[99]

1.111 iiNet Limited (iiNet) advised the committee that the cost of implementing data retention to its organisation could be as high as '$100 million and growing over time as data grows':

> [$60 million] was our first-year cost, which we calculated…18 months ago. We have done some maths since then and we have seen the proliferation of metadata on websites and other places doubling every 18 months to two years, so our costs would increase. I know the cost of storage is coming down, but we believe that doubling every two years of the volume of data that would need to be collected would mean that this would be an ongoing increase. We are now talking more in the order of $100 million for that first two-year period of data collection…and growing over time as that data grows. And then there is another potential cost on top. If the suggestion is that content is not required—that somebody will be required to process the metadata that is collected to strip out the content—that would be petabytes of data a day for our own organisation. You would need supercomputers to extract that data …The cost of storage might go down a fraction, but if we have to store it in the first place and then redact it it is just costs upon costs.[100]

1.112 AMTA explained that it had previously identified the potential costs of data retention to industry as more than $500 million for 'a new scheme around network infrastructure security and potentially high costs for industry around online copyright enforcement':

---

99 Australian Mobile Telecommunications Association and the Communications Alliance, *Submission 16*, pp. 12–13.

100 Mr Steve Dalby, iiNet Limited, *Committee Hansard*, 29 July 2014, pp. 26–27.

> …in this day and age information flows are not only huge but increasing in some spaces exponentially. They are also borderless in the sense that all of us on a daily basis I am sure traverse many websites and destinations outside of Australia...To give you a picture: data volumes in the mobile space alone are predicted to increase by a factor of 10 between 2013 and 2019. Should we have to build a system to retain data for a lengthy period, it is not just as simple as pushing a button or tapping an existing resource; in actual fact we would have to duplicate the data. That duplication would be required because this data comes from a multitude of IT systems within carriers. To be helpful to law enforcement agencies, it would need to be duplicated and aggregated. Then we have to store it…Then we have to manage it and be able to interrogate it. There are the privacy and security issues that go with that. All of these things are very considerable issues to address.[101]

1.113 iiNet suggested that these costs could end up being passed on to customers, but added that until it is clear what the legislation would require it would be difficult to calculate the ultimate cost:

> We originally calculated the $60 million to be an increase of about $5 per month per customer if we just passed the costs through…we are very confused about what is required so it is very difficult for us to calculate what the costs will be. If we are only required to keep routine metadata for telephone calls we can probably pack up today and not speak again. If, however, the confidential briefing paper that was provided by the Attorney-General's Department is to be interpreted the way we have then yes, there will be massive costs.[102]

1.114 Mr Chris Althaus, Chief Executive Officer of AMTA made similar comments in relation to consumers:

> [T]he costs issue remains a very significant one for industry. All of the matters that relate to interception, and the extension perhaps into a data retention regime, come at significant cost. Industry has to shoulder its burden in that respect, but so too will there be an impost through to consumers, and, we believe, a necessary impost on government. Schemes elsewhere around the world have frequently seen the role of government in funding the establishment of schemes and the national security and law-enforcement agencies paying to use those schemes. That is certainly an issue for consideration in this current debate.
>
> We are going to incur significant costs. Data gathering through a range of currently disaggregated systems within service providers will need to be serviced by a new system, a new capacity. And of course there is significant and ongoing uncertainty around many aspects of that. A lot of those aspects are what we will perhaps describe as a work in progress.[103]

---

101 Mr Chris Althaus, AMTA, *Committee Hansard*, 29 July 2014, pp. 11–12.

102 Mr Steve Dalby, iiNet Limited, *Committee Hansard*, 29 July 2014, pp. 26–27.

103 Mr Chris Althaus, Chief Executive Officer, AMTA, *Proof Committee Hansard*, 2 February 2015, p. 6.

1.115 Industry submitters consistently explained to the committee that the costs from the introduction of a mandatory data retention regime would not be from storage of the data but rather the systems to extract the data and the security that would need to be built to protect the data once stored. For example, Mr James Shaw, Director of Government Relations at Telstra, explained:

> …quite often the focus seems to be around the storage of the data…but that is only a very small part of it. In fact, in terms of the costs of the scheme, it is probably one of the lesser elements of it. There is the whole process of extracting the data from the network, and the data that is being looked at in the context of this regime comes from various network elements. It is not located in one central server within the network. There is a variety of platforms generating different types of data in different formats. That has to be extracted. It then has to be managed and stored, and at the same time it has to be secured. Then it has to be made available in a form that the agencies can usefully use. Then, finally, and most importantly, at the end it has to be disposed of in a way that satisfies the concerns of customers that this data is not hanging around for any longer than is required. So they are all steps in or elements of an overall data retention scheme. You cannot divorce one from the other, but they are separate considerations in how you go about building the scheme.[104]

1.116 Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy at Vodafone Hutchison Australia, was of a similar view:

> The storage component is relatively straightforward to expand. Where the costs are is in the capability to retrieve the information from a very large data set. That is where the costs will kick in as you lengthen the amount of time.[105]

1.117 However, Mr Alastair MacGibbon suggested to the committee that in his experience, the 'cost argument is often overblown'. He explained:

> Given the ability to compress information and the cost of the actual devices for storing information, the cost of storage has gone down exponentially and will continue to do so over the years. I think the biggest cost is probably in architecting their systems to collect information. In many respects they are compelled to at the moment anyway under the current telecommunications interception act requirements.
>
> …The reason why cost should not be an argument in compelling some of these ISPs and telcos to store information is that, as I say, they are currently obliged to have themselves architected in certain ways…[106]

---

104 Mr James Shaw, Telstra, *Committee Hansard*, 26 September 2014, p. 39.

105 Mr Matthew Lobb, Vodafone Hutchison Australia, *Committee Hansard*, 26 September 2014, p. 24.

106 Mr Alastair MacGibbon, *Committee Hansard*, 26 September 2014, pp. 30–31.

1.118 ThoughtWorks raised the concern that data retention could in fact have more far-reaching impacts, directly affecting the bottom line of some businesses as consumers seek out companies that provide greater privacy protections:

> As an Australian business we are concerned that we will see this impact on our industry here in Australia that the US has seen. Essentially, we are talking about customers choosing to store their information in another country because they are concerned about the laws in the US and the subversion of those laws in the US in order to access data.
>
> We are also concerned that if we have stronger laws here that we will lose business. In particular, for things like cloud providers—organisations that store data for other companies—where there has been the biggest impact. But there were all sorts of impacts across the board. Cisco, who make routers and other things that direct internet traffic, saw a decline in their top markets of between 18 and 30 per cent. So we are seeing real impacts on business already, particularly in the US, and it comes from a lack of trust by customers.[107]

Privacy implications of the proposed data retention period

1.119 In contrast to the calls by law enforcement agencies for the implementation of a mandatory data retention regime, many stakeholders raised concerns in respect of privacy and the proposed regime, particularly the prescribed retention period of two years. It was suggested that the introduction of such a regime ran directly counter to the application of Australian Privacy Principle 3, which codifies the long-standing principle that personal data should not be arbitrarily captured and stored:

> The Australian privacy principles were updated and implemented just six months ago, yet mandatory data retention is a policy that would require the explicit rejection of these principles.[108]

1.120 On introducing the Bill, the Minister explained that the two year retention period set out in the Bill had been determined on advice from law enforcement and security agencies, as well as by reference to the experiences of a number of foreign jurisdictions.[109]

1.121 In its submission to the PJCIS committee, the department identified that '[m]ore than 35 Western countries worldwide have legislative data retention schemes' and that the 'most widely implemented data retention scheme is the former EU Data Retention Directive…which imposed an obligation on companies to retain specified data for up to [two] years'.[110] The evidence provided by the department to the PJCIS

---

107 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 7.

108 Mr Simon Breheny, Director, Legal Rights Project, Institute of Public Affairs, *Committee Hansard*, 26 September 2014, p. 8.

109 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12561.

110 Attorney-General's Department, *Submission 27 to the PJCIS inquiry*, p. 38.

identified that the proposed two year period is in fact at the upper limit for retaining data across jurisdictions.[111]

1.122 The proposed period attracted much criticism: stakeholders were consistently of the view that the two-year period should be revised. In its review of the Bill, the Parliamentary Joint Committee on Human Rights (PJCHR) stated that:

> A data 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. This question is resolved by reference to the purposes for which the data is accessed.
>
> For example, despite the acknowledged low frequency of use of data that is more than six months old, and the stated requirement for older data for national security and complex criminal offences, the scheme does not limit access to data which is older than six months to the investigation of national security and complex criminal offences.[112]

1.123 This conclusion led the PJCHR to request 'further advice of the Attorney-General as to whether the two year retention period is necessary and proportionate in pursuit of a legitimate objective'.[113]

1.124 Similarly, the Australian Human Rights Commission (AHRC) raised concerns in respect of the two year retention period noting that:

> In the landmark decision of the Court of Justice of the European Union [EU], which invalidated the EU Data Retention Directive, the Court identified several characteristics of the Directive that rendered the regime a disproportionate interference with the rights to privacy. Relevantly, the Court considered that retention periods should be limited to that which is 'strictly necessary'. Further, retention schemes should distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned.[114]

1.125 The AHRC drew attention to an evaluation report on the EU Data Retention Directive in 2011 that 'only 2 per cent of requested data was over [one] year old across

---

111 See: Attorney-General's Department, *Submission 27 to the PJCIS inquiry*, Appendix A– Summary of data retention and access arrangements in Western countries, pp. 55–56.

112 Parliamentary Joint Committee on Human Rights (PJCHR), *Fifteenth Report of the 44th Parliament*, p. 15. It is expected that the response of the Attorney-General together with the PJCHR's finding on the Bill's compatibility with human rights will be set out in the PJCHR's report of 17 March 2015.

113 PJCHR, *Fifteenth Report of the 44th Parliament*, p. 15.

114 Australian Human Rights Commission (AHRC), *Submission 42 to the PJCIS inquiry*, pp. 8–9. See also, Gilbert + Tobin Centre for Public Law, *Submission 5 to the PJCIS inquiry*, p. 2; Mr Bernard Keene, *Submission 37 to the PJCIS inquiry*, pp. 5–6; Australian Privacy Foundation, *Submission 75 to the PJCIS*, p. 2; Law Institute of Victoria, *Submission 117*, pp. 15–16; Civil Liberties Councils of Australia, *Submission 129 to the PJCIS inquiry*, p. 12; and Mr Jon Lawrence, Electronic Frontiers Australia, *Proof Committee Hansard*, 2 February 2015, p. 15.

the European Union' and noted that as the majority of EU countries (including the United Kingdom) have a one year retention period 'an initial retention period of [one] year would be a more proportionate interference with the right to privacy'.[115]

1.126 The Australian Privacy Commissioner stated that any data retention scheme 'should only require service providers to retain telecommunications data for the minimum amount of time necessary to meet those needs'.[116] The Law Council made a similar recommendation stating that the 'data retention period should be reduced to no longer than the minimal period required by law enforcement and security agencies'.[117]

1.127 The Internet Society of Australia (ISOC-AU) outlined that in its view unless there is 'appropriate technology standards metadata should not be retained beyond strict business need':

> Where metadata is retained there need to be the strictest standards around retention and access. I cannot reinforce that enough. Should access to metadata be granted, considerably higher standards of access and oversight of these processes need to be implemented, including penalties for the breaches of these sorts of standards…Certain things need to be built into the equipment and the application so that we can do this in a clear and consistent manner with appropriate levels of control.[118]

1.128 The telecommunications industry was also of the opinion that the case for a two year data retention period had not been made:

> Industry is, however, far from convinced that a two year retention period for IP related data is either necessary, justifiable, cost-effective, or in the public interest…and 12 months. For internet-related data there is only one country – Poland – that appears to be heading down the path of a 2 year retention period – and that regime is under challenge.
>
> We know that in UK, for example, over a recent 4 year period, 74%+ of disclosures to law enforcement agencies, where the age of data being sought was known, related to data that was less than 3 months old….
>
> [communication service providers] CSPs report that the vast majority of warrantless requests they receive from Australian agencies relate to data that is 6 months old or younger…[119]

---

115 AHRC, *Submission 42 to the PJCIS inquiry*, pp. 8–9. A similar study was cited by the Australian Privacy Commissioner in his submission to the PJCIS inquiry and the Law Council of Australia. See, Office of the Australian Information Commissioner (OAIC), *Submission 92 to the PJCIS inquiry*, p. 15; Law Council of Australia, *Submission 126 to the PJCIS inquiry*, pp. 16–17.

116 OAIC, *Submission 92 to the PJCIS inquiry*, p. 14.

117 Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 17.

118 Ms Narelle Clark, ISOC-AU, *Committee Hansard*, 23 April 2014, pp. 33, 38.

119 AMTA and Communications Alliance, *Submission 6 to the PJCIS inquiry*, p. 7.

1.129 AMTA and the Communications Alliance suggested that rather than the two year period proposed by the Bill, a '[six] month period would be an appropriate minimum time to require the retention of internet-related data' and:

> It might be useful to incorporate within the Bill a requirement for agencies to periodically report to Parliament the number of requests (including distinguishing between a request relating to an individual and requests relating to groups of people) that have been placed with CSPs for retained data that was generated in the preceding 3 month period, 3-6 month period, 6-12 month period, 12-18 month period and 18-24 month period.[120]

No destruction requirement

1.130 Concerns were also raised in relation to the absence of a legislative requirement for data captured by the proposed regime to be destroyed.

1.131 On 12 March 2014, the updated Australian Privacy Principles (APP's) came into force, binding government agencies and other organisations to uphold high-level privacy practices.

1.132 Notably, for the purposes of data retention, APP 3 states, in part, that an:

> [E]ntity must not collect personal information… unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.[121]

1.133 APP 11 prescribes that an entity must:

> [T]ake such steps as are reasonable in the circumstances to protect the [personal] information [it holds] from misuse, interference and loss; and from unauthorised access, modification or disclosure [and that if an entity holding personal information about an individual] no longer needs the information for any purpose for which the information may be used or disclosed by the entity…the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.[122]

1.134 Although the existing TIA Act contains a destruction requirement for restricted records and telecommunications content[123] it does not contain a destruction requirement in respect of telecommunications data. The department confirmed that there is no destruction requirement proposed in the Bill currently before the Parliament:

---

120 AMTA and Communications Alliance, *Submission 6 to the PJCIS inquiry*, pp. 7–8.

121 http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles (accessed 20 August 2014). See also: APP 3, Schedule 1 to the *Privacy Act 1988*.

122 APP 11, Schedule 1 to the *Privacy Act 1988*.

123 See sections 79 and 150 of the TIA Act.

> …in relation to the two-year detention period is that there is no obligation in the bill to destroy that information after two years.[124]

1.135 Throughout its inquiry, this aspect of the existing legislation and the proposed Bill was identified as an area needing reform.

1.136 The Law Council raised this gap in the Bill as a concern given the obligations imposed by the APP's.[125] Telstra also drew attention to its obligations under the Privacy Act suggesting that clarification was required:

> [W]e also operate under a requirement in the Privacy Act to destroy or de-identify data once no longer required for purposes for which they were collected. This could be interpreted as meaning we are legally required to immediately destroy or make amendments to the data retained under the Bill as soon as the two year retention period has ended thereby creating a further rolling obligation and additional cost on industry unrelated to commercial purposes that we have not yet factored into our assessment of the Bill. To help limit this impact, we believe that if there are to be different data retention periods across technologies as part of this scheme, we would recommend that telecommunication service providers be given the option of retaining data for the longest permitted period without breaching the law.[126]

1.137 This section examined the government's announcement to introduce mandatory data retention and the main concerns that have been raised in relation to the government's proposal. The next section looks briefly at the international experience of those jurisdictions which have pursued mandatory data retention.

---

124 Ms Anna Harmer, Attorney-General's Department, *Proof Committee Hansard*, 17 December 2014, p. 7.

125 Law Council of Australia, *Submission 126 to PJCIS inquiry*, pp. 25–26.

126 Telstra, *Submission 112 to the* PJCIS, p. 5.

International developments

1.138 Australia is not the only jurisdiction considering data retention and related privacy issues. However, several data retention regimes in other countries have recently been wound back. This section reflects on the international experience with mandatory data retention.

Is international practice moving away from mandatory data retention?

1.139 On 15 March 2006, the European Parliament and the Council of the European Union issued Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[127] Directive 2006/24/EC also amended Directive 2002/58/EC.[128] In part, it required the European Union (EU) to:

- retain certain categories of data[129] (Article 3) for a period of 'not less than six months and not more than two years from the date of the communication' (Article 6);
- ensure access to data is provided only 'to the competent national authorities in specific cases and in accordance with national law' and that the procedures and conditions followed to access the data accord with the requirements of necessity and proportionality as defined in each Member State's national law subject to EU law, public international law and 'in particular the ECHR as interpreted by the European Court of Human rights' (Article 4); and
- ensure the protection and security of the data, including destroying the data at the end of the retention period (Article 7).[130]

1.140 In an April 2014 ruling, the Court of Justice of the European Union (ECJ) found that the European Data Retention Directive was invalid. The regime was overturned by the ECJ on the grounds that it 'entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the

127 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (accessed 26 February 2015). A copy of Directive 2006/24/EC is set out in Appendix 5.

128 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (accessed 26 February 2015). Directive 2002/58/EC concerned the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (accessed 3 March 2015).

129 The categories of data required to be retained are set out in Article 5 of Directive 2006/24/EC. The definitions for the purposes of the directive are set out in Article 2.

130 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (accessed 26 February 2015).

protection of personal data, without that interference being limited to what is strictly necessary'.[131]

1.141 In a statement advising of its decision, the ECJ stated that 'by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interfere[d] in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data' and that 'the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance'.[132]

1.142 The Court went on to explain that it was then for it to examine 'whether such an interference with the fundamental rights at issue [was] justified' and that it was of the opinion that:

> …by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.
>
> In that context, the Court observe[d] that, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by the directive, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

1.143 The Court also set out that:

> Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.
>
> Firstly, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.
>
> Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have access to the data and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime'

131 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (accessed 26 February 2015). See also: Ms Lindy Stephens, Global Director of People Operations, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 1.

132 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (accessed 26 February 2015).

> as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.
>
> Thirdly, so far as concerns the data retention period, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.
>
> The Court also finds that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data. It notes, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.
>
> Lastly, the Court states that the directive does not require that the data be retained within the EU. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[133]

1.144 The Law Council explained that it shared the concerns of the ECJ and highlighted similarities with the proposed Australian scheme:

> I note with interest the decision of the Court of Justice of the European Union this month that struck down the data retention directive and did so really because of the sorts of concerns that exist in the legal profession here in Australia. The directive there would be similar to a law here that would require data to be kept for perhaps two years. One of the reasons the directive was struck down was that there was no real differentiation of what sort of data was to be kept. Data that was entirely innocent needed to be kept, along with data that might be likely to impact on national security issues or serious crime investigation issues. There was a problem about the length of time that data was to be kept; the proposal in each case considered

133 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (accessed 26 February 2015).

> by the court there was six months. The risk of abuse inherent in that scheme seemed to be at the heart of the decision.[134]

1.145 Despite the decision of the ECJ, the committee also received evidence from Australian law enforcement agencies that in their view, the decision does not necessarily have implications for Australia. The then Acting Chief Executive Officer of the Australian Crime Commission (ACC) addressed some, but not all the issues raised by the ECJ:

> I am aware of the Court of Justice decision. I think what is important is the basis of that decision. There were about four key points that they referenced and my reading of it is that it does differentiate a little from the environment we have here in Australia. I would argue that in a number of those cases we already mitigate some of the risks that were identified. For example, one of the bases that the Court of Justice identified was that there was no protection against the risk of abuse. From my perspective, our oversight regime does protect from the risk of abuse. Whilst I am aware of the Court of Justice decision, I would equally argue that our oversight regime both from a legislative perspective and even a policy perspective differentiates from what the European Union appears to have discovered in their Court of Justice decision.[135]

1.146 The department argued, that '[t]he Court's finding was not because data retention was inherently unconstitutional…Instead, the Court's judgment was based on the lack of appropriate safeguards and limits within the Directive itself…'[136] and that although the invalidation of the Directive had resulted 'in the annulment of a number of data retention laws in member States where the Directive was implemented…many European countries [were] actively working to address the issued identified by the Court. For example, the then Director-General of ASIO told the committee:

> Notwithstanding the decision of the [European Court of Justice], Britain decided just a couple of weeks ago that they would implement that regime. They made no bones about why they need it. The court said it did not contain sufficient safeguards for implementation across EU member-states and the way it was framed violated the principle of proportionality under EU law. But it did acknowledge that data retention genuinely satisfies an objective of general interest, mainly the fight against serious crime and ultimately public security.[137]

1.147 The then Director-General of ASIO added that:

> I suspect the debate, discussion and, indeed, legal processes in Europe are not yet completed. It would be wrong of us to jump to one judgement of the

---

134 Mr Phillip Boulten SC, Law Council of Australia, *Proof Committee Hansard*, 23 April 2014, p. 3.

135 Mr Paul Jevtovic APM, Australian Crime Commission, *Committee Hansard*, 22 April 2014, p. 10.

136 Attorney-General's Department, *Submission 27 to the PJCIS inquiry*, p. 39.

137 Mr David Irvine, ASIO, *Committee Hansard*, 21 July 2014, p. 16.

> European court in relation to one aspect of data retention to rule it out as a gross violation of human rights across the board.[138]

1.148 iiNet Limited (iiNet) explained that, in its view, the shift internationally is away from mandatory data retention and provided examples of how various European jurisdictions had responded to the decision of the ECJ.[139] The Attorney-General's Department (department) provided a concise summary of the data retention regimes in the European Union as they currently stand: the summary indicates those jurisdictions that have annulled mandatory data retention since the decision of the EU Court of Justice:

138 Mr David Irvine, ASIO, *Committee Hansard*, 21 July 2014, p. 16.

139 iiNet Limited, answer to a question taken on notice, received 11 August 2014, p. 1.

Country	Retention period	Access method
Latvia	18 months	Judicial authorisation for traffic data. Police authority for subscriber information.
Liechtenstein	6 months	
Lithuania	6 months	Internal authorisation
Luxembourg	6 months	
Malta	Between 6 and 12 months	Internal authorisation
Netherlands	6 months for IP address allocation 12 months for telephony	Hybrid – Internal authorisation for security agencies and less-intrusive law enforcement requests; prosecutorial warrant for more intrusive law enforcement requests.
Norway	6 months Entered into force on 1 January 2015	
Poland	2 years	Internal authorisation
Portugal	12 months	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Romania	Previously 12 months Annulled as a result of the annulment of the EU Data Retention Directive	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Serbia	12 months	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Slovakia	Between 6 and 12 months Temporarily suspended while under judicial consideration	
Slovenia	Previously 12 months Annulled as a result of the annulment of the EU Data Retention Directive	Internal authorisation
South Africa	3 years	
Spain	Between 6 months and 2 years	Internal authorisation
Sweden	6 months	
Switzerland	6 months Laws before Parliament to increase to 12 months	
Turkey	Between 6 months and 2 years	
United Kingdom	12 months, with extraterritorial application	Internal authorisation for most agencies. However, local authorities require a warrant from a judicial officer.
United States	18 months (telephony only)	Internal authorisation

Country	Retention period	Access method
Austria	Previously between 8 and 14 months Annulled following the annulment of the EU Data Retention Directive	Internal authorisation
Belgium	Between 12 months and 3 years	Warrant issued by a judicial officer or a public prosecutor
Brazil	6 months for web browsing history 12 months for IP address allocation	
Bulgaria	12 months	Warrant issued by a judicial officer
Cyprus	Previously 6 months Annulled in 2011	Warrant issued by a judicial officer
Czech Republic	Previously between 6 and 12 months. Annulled as a result of the annulment of the EU Data Retention Directive Currently drafting new laws	Internal authorisation
Denmark	12 months Denmark previously required internet service providers to also retain web-browsing information for 1 in every 500 packets sent over the internet. This requirement was removed in mid-2014, following advice from agencies and prosecutors that there were technical difficulties in obtaining useful information from only 0.2% of such traffic. Annulled but will reintroduce in January 2015	Warrant issued by a judicial officer
Estonia	12 months	Prosecutor authorisation
Finland	12 months	No authorisation required for subscriber information. Judge's authority for traffic data.
France	12 months	Authorisation from the Interior Ministry (from 1 January 2015)
Germany	Previously 6 months Annulled in 2010 Draft amendments to Telemedia Act for limited data retention	Internal authorisation
Greece	12 months	Warrant issued by a judicial officer
Hungary	12 months	Internal authorisation
Iceland	6 months	
Ireland	Between 12 and 24 months	Internal authorisation
Italy	12 months for IP address allocation 2 years for telephony	Hybrid – public prosecutor or, in the case of organised crime or counter-terrorism, an internal authorisation.

Source: Attorney-General's Department, *submission 27 to the PJCIS inquiry*, pp. 55–56.

1.149 The department was unable to point to any jurisdiction where the winding back of data retention or the requiring a warrant to access metadata had caused law enforcement activities to 'grind to a halt':

> CHAIR: Ms Jones, are you aware that law enforcement has not ground to a halt in Belgium, Bulgaria, Denmark, Greece, Latvia, the Netherlands, Portugal, Romania and Serbia, which are all countries that, according to your very helpful appendix to your submission, have some form of judicial oversight of telecommunications authorisations? Why do you think it would grind to a halt in Australia? What evidence do you have to back that up?
>
> Ms Jones: We have obviously been discussing this with agencies in terms of their operational experience of the importance of being able to access data information as quickly as possible early in the process.
>
> I note that you have listed a number of countries, but we have also looked at the experience in the United Kingdom, where they have recently had to look at the regime that they had in relation to warrants because essentially their operational experience was that it became virtually unworkable and that the number of successful authorisations was significantly reduced. There was a report to the UK Parliament by the Interception of Communications Commissioner that noted that it was causing significant delay in the progress of many investigations.
>
> CHAIR: Do you have any evidence that in any of the countries I just listed law enforcement has ground to a halt or that there has actually been any impact at all on the efficiency of law enforcement?
>
> Ms Jones: We have not discussed the specifics with those countries. Is there anything further you can add?
>
> Ms Harmer: No, we have not engaged directly.
>
> CHAIR: It is a pretty big deal to come in here and make sweeping statements like, 'Law enforcement will grind to a halt unless we are allowed to continue vast, warrantless access to telecommunications data.' It is a pretty big call and you have no evidence that in any of those countries that has been the case.
>
> Ms Jones: We are focused on the experience in the Australian context, on talking with agencies in Australia, and this is an issue that we have discussed before the Parliamentary Joint Committee on Intelligence and Security.
>
> CHAIR: Yes, but you are here now with us. What evidence do you have either in the countries that have a standing data retention regime or in those in Europe that had one that was then annulled—Germany being one example—of improvements in the rate of clearance of crimes? Is there any evidence from any country at all that you could point to where data retention has led to an improvement in the rate of crime clearance?
>
> Ms Harmer: I think one of the challenges in that regard is the extent to which data as a single investigative resource can be said by itself to improve clearance rates. I expect you may have in mind a German report which suggests that there was a limited improvement or what has perhaps been characterised as negligible improvement in clearance rates as a result

> of the introduction of data retention there. What the clearance rate reflects, of course, is the number of crimes solved as opposed to the number of crimes on hand. What access to data does is to provide the starting point for investigations and allow them to proceed further, or indeed to commence at all. In that regard, while there is that German report, I think it was only a fortnight ago that German Chancellor Merkel indicated her intention to lobby the EU for a new data retention directive, noting the very significant importance of data retention from her perspective to German investigations.
>
> CHAIR: You have still managed to avoid the question. Do you have any evidence from any jurisdiction at all that mandatory data retention either reduces crime or improves the rate at which crimes are solved? You may not have it at the table, but is there anything at all that you could point me to?
>
> Ms Harmer: The evidence in support of data retention is not cast in terms of clearance rates; it is cast in terms of—
>
> CHAIR: Or crime rate? I will take any metric you care to name.
>
> Ms Harmer: Perhaps in that regard I could refer you to some of the evidence of the law enforcement agencies who appeared last Friday. From an investigative perspective, it is the case that it is extremely difficult to point to data as one investigative tool having a direct and quantifiable impact on the number of prosecutions and convictions. The way in which law enforcement agencies apply metrics to assess their effectiveness and their prosecutions and convictions is not able to hinge back to a single data point. Accordingly—
>
> CHAIR: I am not talking about a single data point but the whole category of data retention or metadata access in general. It is the opposite of evidence based policy; it is anecdote based policy.
>
> Ms Jones: It is policy based on very strong advice from the agencies who have responsibilities in relation to law enforcement and national security.
>
> CHAIR: Of course they want more power. It is your job and ours to balance that power against proportionality and whether it is useful or not. I am just asking for evidence as to whether it is useful. All right—we will move on.[140]

1.150 In fact, the committee heard that Germany has moved in the opposite direction to mandatory data retention, implementing a policy known as 'datensparsamkeit' or 'data austerity' which places the onus on government agencies, departments and business to 'collect only that data which is necessary and proportionate'.[141]

---

140 Ms Katherine Jones, Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, pp. 52–53; and Ms Anna Harmer , Acting First Assistant Secretary, National Security Law and Policy Division, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, pp. 52–53.

141 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 2.

1.151 ThoughtWorks expressed the view that what is 'necessary and proportionate' is a difficult concept to define and 'does depend on the individual circumstances'.[142] ThoughtWorks cautioned however that as 'technology moves at a pace that is ahead of business and ahead of decisions and laws':

> …people are doing things because they are technologically possible, not because they are a good idea. So we are asking that businesses—and this is what we do ourselves—actually stop and think and make a decision: do they need that particular piece of data in order to serve their customers, in order to provide the services they provide, or is it just something they think they might need in the future?
>
> It is really more about stopping and asking whether you are collecting data just for the sake of it or whether you really need it to do business.[143]

1.152 During its inquiry the committee also received evidence that in a 30 June 2014 report of the United Nations (UN) High Commissioner for Human Rights titled 'The right to privacy in the digital age', the High Commissioner 'strongly emphasis[ed] the complicity of business in mass surveillance and in violating the right to privacy'.[144] ThoughtWorks further explained the concerns of the UN High Commissioner:

> The former high commissioner outlined a few key points in her report…The first one is that she asserts that states have a positive obligation under international law to protect citizens from surveillance by private or state entities and that bulk collection and the very existence of mass surveillance, whether the information is used or not, interferes with the right to privacy. She also asserted that mandatory third-party retention is surveillance and that it is neither necessary nor proportionate and insists that a distinction between content and metadata is no longer persuasive. In other words, there is no longer any real distinction between metadata and content. The crucial finding applies the effective control doctrine under international law to internet infrastructure. So, states are obliged to extend human rights protections to whoever's privacy is interfered with by internet infrastructure on their territory.[145]

1.153 The Chair also noted the similarly titled June 2014 Report of the Australian Law Reform Commission (ALRC) *Serious Invasions of Privacy in the Digital Era*, in which the ALRC advised:

> …privacy has been said to lie at the heart of liberty, and will often support other fundamental rights and freedoms, sometimes it must be balanced with other important interests… [however] privacy should not be casually 'traded off' for the sake of other important interests.[146]

---

142 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 3.

143 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 3.

144 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 1.

145 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 2.

146 ALRC Report 123, June 2014, p. 35.

Alternatives to mandatory data retention

1.154 Submitters to the inquiry also suggested that mandatory data retention should not be pursued before alternatives are considered.

1.155 The Australian Privacy Foundation explained that, in its view, mandatory data retention is not necessary as the existing preservation notice regime set out in the TIA Act 'should be sufficient to provide agencies with what they need'.[147]

1.156 iiNet shared this view stating that '[t]argeted preservation notices used together with stored communications warrants provide an alternative framework to mass data retention that is designed to ensure that any retention and access to private data is necessary and legitimate'.[148] The Institute of Public Affairs (IPA) was of a similar view. In evidence to the committee, the IPA expressed that:

> It is also worth noting that it has not been adequately shown that preservation orders are not adequate to achieve the aims of the law enforcement. Stored preservation orders are targeted, proportional data retention schemes that offer a flexible and privacy-protecting mechanism to law enforcement agencies. It is striking to us how rarely the existence of this mechanism is discussed in the data retention debate when it would seem to resolve all the problems with the TIA act that have been identified by law enforcement agencies.[149]

1.157 This view however was specifically discounted in the Minister's second reading speech when he explained that the '[e]xisting powers and laws are not adequate to respond to this challenge'.[150] The department further explained the government's view that the often cited alternative of the existing preservation regime was insufficient:

> [T]he Department's view, supported by international experience, is that expanding the existing preservation notice regime would not address the capability challenges faced by agencies.
>
> Preservation and data retention are complementary tools, but are aimed at different objectives. The purpose of preservation notices is to 'quick freeze' volatile or perishable electronic evidence that a provider possesses for a short period of time, to allow agencies time to apply for and obtain a warrant to access that information. Evidence cannot be preserved if it was never retained, or if it has already been deleted. For example, a preservation

147 Mr Nigel Waters, Australian Privacy Foundation, *Committee Hansard*, 29 July 2014, p. 31. The preservation notice regime, set out in Part 3-1A of the TIA Act, establishes a system of preserving certain stored communications that are held by a carrier. The purpose of the preservation is to prevent the communications from being destroyed before they can be accessed under certain warrants issued under the Act.

148 iiNet Limited, Answers to questions taken on notice, received 11 August 2014, p. [5].

149 Mr Simon Breheny, Director, Legal Rights Project, Institute of Public Affairs, *Committee Hansard*, 26 September 2014, p. 8.

150 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12560.p.

> notice issued 9 months after a criminal event cannot assist an investigation if the data sought was destroyed after just 1 month's existence.
>
> Preservation notices will not, therefore, address the fact that service providers are not retaining critical types of telecommunications data, or are retaining that data for shorter periods of time. In addition, as the current data authorisation provisions in Chapter 4 of the TIA Act already facilitate timely access to telecommunications data for legitimate investigative purposes, the Australian Government did not need to include preservation notices for telecommunications data in the Cybercrime Act.
>
> By comparison, the purpose of data retention is to introduce a consistent record-keeping requirement across industry to ensure that certain telecommunications data are consistently available. As such, data retention is in fact a prerequisite to preservation of data, rather than preservation offering an alternative to retention.[151]

1.158 This section has looked briefly at the European experience with data retention. The final section sets out the Chair's view and recommendations in respect of the proposed mandatory data retention regime.

151 Attorney-General's Department, *Submission 27* (to the PJCIS inquiry), p. 17.

Chair's views and recommendations: mandatory data retention

Introduction

1.159 The Chair's views and recommendations set out below are made in respect of the policy of mandatory data retention in the context of the government's proposal set out in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Bill).

1.160 The Chair notes that, at the time of tabling its report, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) had finalised its inquiry into the Bill and the government had issued a response. The Chair is heartened by the government's announcement that it supports all 39 recommendations put forward by the PJCIS. However, although the Chair agrees with some of the recommendations of the PJCIS, he considers that others must go further and hopes that the government responds with similar speed and timeliness to this report and recommendations.

Broader reform is required

1.161 The Chair takes the view that the government's announcement that it will seek to implement mandatory data retention makes the need for the rationalisation and updating of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to be considered holistically more pressing. The Chair trusts that this inquiry will assist in moving towards a TIA Act which is more adapted both to contemporary technology and to the public's more evolved expectations in relation to privacy.

1.162 The Chair is opposed to the introduction of a mandatory data retention regime and draws attention to the failed pursuit of such regimes internationally. It is particularly concerning that the government is considering requiring the retention of data even if it serves no business purpose and would therefore only be retained as a result of this new regime. The Chair references the international experience and suggests that the German approach of retaining only that which is both necessary and proportionate, 'datensparsemkeit', should guide policy and law makers.

1.163 The Chair is critical of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 currently before Parliament. The regime being proposed equates to mass surveillance. It should not proceed. The grounds for implementing a policy of mandatory data retention have not been established to the Chair's satisfaction.

1.164 The implications for the right to privacy and freedom of the press must not be traded away without careful consideration or in the absence of adequate legislative safeguards.

1.165 Throughout its inquiry, the committee received evidence clearly illustrating that what was collected as telecommunications data in 1979 was a small fraction of what is collected as telecommunications data in 2015. The evidence illustrated the difficulties of defining 'telecommunications data' yet clearly showed that telecommunications data today provides a much fuller picture of a person's social connections, values, personal preferences and habits. It is clear to the Chair that the

analogy of the envelope and the letter no longer describes the distinction between content and metadata in the digital age.

Recommendation 4

1.166 The Chair recommends that the government not proceed with a mandatory data retention regime and that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be withdrawn.

The need for a definition

1.167 The Chair considers that a definition of 'telecommunications data' or 'metadata' must be settled and incorporated into a redrafted *Telecommunications (Interception and Access) Act 1979* (TIA Act). A definition should be developed by industry, together with government and privacy advocates. Until a definition is settled, the scope, cost and privacy implications of any proposed data retention regime remain unquantifiable.

1.168 The Chair does not support the proposed definition of 'telecommunications data' set out in the Bill currently before the parliament. The Chair agrees with Recommendation 2 of the PJCIS that the Bill should be amended to include the proposed data set in primary legislation.[152] However, the Chair suggests that revisions to the definition of the data set go further and identify those elements within the data set that constitute the 'information that allows a communication to occur'[153]and 'basic subscriber data'[154] and identify that any change to the parameters of the data set must occur through the legislative process.

1.169 The Chair considers that the evidence received by the PJCIS that industry will find it 'very challenging' to separate the content from the metadata for some types of data further supports its view that different elements of the data set have greater privacy implications than others and adds weight to calls for the introduction of a warranted access regime for data that is 'information that allows a communication to occur'.[155]

---

152 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 79.

153 Data that is 'information that allows a communication to occur' includes for example: the internet identifier (information that uniquely identifies a person on the internet) assigned to the user by the provider; for mobile service: the number called or texted; the service identifier used to send a communication, for example the customer's email address, phone number or VoIP number; the time and date of a communication; general location information, that is, cell tower; and the duration of the communication.

154 Data that is 'basic subscriber data' would include for example: name of the customer; address of the customer; postal address of the customer (if different); billing address of the customer (if different); contact details, mobile number, email address and landline phone number; and same information on recipient party if known by the service provider.

155 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 100.

Access to telecommunications data

1.170 The Chair acknowledges that 'basic subscriber data'[156] should be able to be accessed without a warrant but maintains that access to data that is 'information that allows a communication to occur'[157] should occur via warrant.

1.171 The Chair notes that evidence received by the PJCIS during its inquiry into the proposed mandatory data retention regime was overwhelmingly supportive of the introduction of warranted access to metadata yet the PJCIS dismissed that evidence on the basis that it would 'impede the operational effectiveness of agencies…to the detriment of the protection of the Australian community'.[158] The Chair disagrees with this assessment and suggests that differentiating between 'basic subscriber data' and data that is 'information that allows a communication to occur' and requiring the latter category of data to be accessed only via warrant, would in fact better balance the important public interests of privacy and security.

1.172 The Chair notes the government's proposal to amend the definition of 'enforcement agency' for the purposes of accessing telecommunications data and supports the principle of restricting access to telecommunications data through tightening the definition of 'enforcement agency' for the purposes of Chapter 4 of the TIA Act. However, the Chair is opposed to proposed new subsections 176A(3) and 176A(4) which would provide the Attorney-General with a discretion to declare an authority or agency to be an 'enforcement agency' for the purposes of accessing telecommunications data. Furthermore, the Chair considers that access to metadata should also be limited through a revision of the associated proportionality test. The Chair acknowledges Recommendation 25 of the PJCIS report[159] but maintains that it does not go far enough.[160] In the absence of a concurrent revision of the

---

156 For example, data identifying information such as the name, address and contact details of a customer.

157 For example, data including the internet identifier, service identifier, and geo-location data.

158 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 245.

159 Recommendation 25 of the PJCIS report stated:

The Committee recommends that section 180F of the Telecommunications (Interception and Access) Act 1979 be replaced with a requirement that, before making an authorisation under Division 4 of 4A of Part 4-1 of the Act, the authorised 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. 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.

160 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 251.

proportionality test to restrict access to metadata to situations where it is 'necessary' for the investigation of specified serious crimes or categories of serious crimes, reform will be neutered.

1.173 The Chair also notes that throughout this inquiry the government has stated that calls for a revision of this proportionality test would be inconsistent with Australia's obligations under the European Union Convention on Cybercrime. The Chair does not agree with this position and is frustrated by the government's willingness to preference a minor Council of Europe convention over Australia's obligations under international human rights law and the fundamental right to privacy of its citizens.

The proposed retention period

1.174 The Chair is concerned by the data retention period proposed in the Bill of two years. The Chair disagrees with Recommendation 9 of the PJCIS report which recommends that the two-year retention period specified in the Bill be maintained and its finding that two years is 'the minimum amount of time that would be acceptable from a national security and law enforcement perspective'.[161] The Chair believes that the proposed retention period of two years is out of step with international jurisdictions, many of which are moving in the opposite direction. The Chair notes the evidence that both this committee and the PJCIS received, which identified that in the majority of cases where metadata is used for law enforcement purposes, it is less than 12 months old.

A destruction requirement

1.175 The Chair is very concerned by the absence in the Bill of a destruction requirement when data is no longer required. In the Chair's view the absence of a destruction requirement directly contradicts the Australian Privacy Principles (APP's), particularly APP 11. The Chair notes Recommendation 28 of the PJCIS 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 [TIA Act] and held by enforcement agencies and ASIO'.[162] The Chair believes that this recommendation does not go far enough and the Bill should be amended to include an express requirement to destroy data after the data retention period has expired or the information is no longer needed. The Chair does, however, support Recommendation 35 of the PJCIS which calls for the APP's to apply to all service providers regardless of their turnover.[163]

---

161 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, pp. 145–147.

162 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 262.

163 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 297.

Oversight

1.176 The Chair supports the proposed new oversight and inspection regime set out in Schedule 3 of the Bill. The Chair considers however, that Schedule 3 of the Bill should be further strengthened by the inclusion of a requirement that enforcement agencies also retain records in relation to:

- the type and age of metadata requested;
- the offences to which a request relates; and
- any outcomes following the request.

1.177 This data should be included in the annual report of the Attorney-General's department.

1.178 The Chair notes that the requirement for the Commonwealth Ombudsman to inspect records in proposed Chapter 4A, does not identify a timeframe for inspection. The Chair considers that this should be addressed through the inclusion of a provision requiring the Commonwealth Ombudsman to examine the records of each agency which has access to metadata every six months.

1.179 The Chair acknowledges that the introduction of a comprehensive inspection and oversight regime will have significant resourcing implications for the Commonwealth Ombudsman and therefore echoes Recommendation 29 of the PJCIS which calls for additional financial resources for the Commonwealth Ombudsman to ensure it can carry out a broader role of overseeing access to telecommunications data. However, the Chair suggests that the resources sought by the PJCIS in Recommendation 32 would be better allocated to assist the Commonwealth Ombudsman and the Inspector General of Intelligence and Security with the independent statutory oversight functions of those offices.

Protection of press freedom

1.180 In its report on the Bill, the PJCIS recommended that further inquiry is needed before recognition of 'the principle of press freedom and the protection of journalists' sources' in the Bill is finalised.[164] Although the Chair supports this recommendation, he is of the view that this inquiry extend to other professions, for example, medical professionals and lawyers, where the integrity of the profession depends upon privacy and confidentiality. The Chair suggests that this issue be resolved and protections for these classes of professions be included in the Bill before it is considered by the Parliament.

Mandatory data breach notification scheme

1.181 The Chair expresses his support for the PJCIS's recommendation (Recommendation 38) to implement a mandatory data breach notification scheme by the end of 2015 and agrees with the PJCIS that 'there must be a [mandatory data breach notification] scheme in place prior to the implementation of the Bill' as it

164 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 258.

'would provide a strong incentive for service providers to implement robust security measures to protect data retained under the data retention regime'.[165]

Recommendation 5

1.182 If the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 is not withdrawn the Chair recommends that the Bill be amended to:

- **include a definition of 'telecommunications data' in the primary legislation;**
- **identify in the definition of 'telecommunications data' the elements of the data set as either 'information that allows a communication to occur' or 'basic subscriber information';**
- **delete proposed subsections 176A(3) and 176A(4) which provide the Minister with the ability to declare an authority or agency to be an enforcement agency for the purposes of accessing metadata;**
- **amend the proportionality test set out in existing sections 177, 178 and 179 of the *Telecommunications (Interception and Access) Act 1979*. The Australian Privacy Commissioner, Law Council of Australia and the Australian Human Rights Commission are to be consulted in amending the proportionality test associated with accessing telecommunications data;**
- **include a requirement for data that is 'information that allows a communication to occur' to be accessed only via warrant;**
- **reduce the mandatory data retention period from two years to three months;**
- **include a requirement that all data be stored in Australia;**
- **include a requirement to destroy telecommunications data after the mandatory retention period or when it is no longer needed;**
- **include protections for sensitive classes of professionals including journalists and their sources, medical professionals, and lawyers;**

165 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, pp. 298–299.

- **amend proposed section 186A to include a requirement that the following information also be kept by an agency:**
  - **the type of metadata requested;**
  - **the age of the metadata requested;**
  - **the offence(s) which the request related to;**
  - **the outcome following the request;**

  and include a requirement in proposed section 187P that this information be reported in the Attorney-General's annual report to the Parliament;
- **amend proposed section 186B to include a requirement that the Commonwealth Ombudsman examine the records of each agency which has access to metadata every six months;**
- **amend proposed section 187N (Review of operation of Part) to require both the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor to review the data retention regime on a triennial basis; and**
- **introduce a mandatory data breach notification regime.**

Recommendation 6

1.183 The Chair recommends that the government introduce a statutory right to privacy, similar to that which exists in the United Kingdom, rather than relying on international human rights instruments.

Divergent views on '5 Eyes' collaboration

1.184 The Chair notes that there is significant variance between the evidence presented by Australian law enforcement agencies and oversight bodies, and the revelations about international surveillance and information sharing provided by whistleblowers and some elements of the media.

1.185 WikiLeaks publisher Mr Julian Assange, who has been instrumental in publishing a large volume of information from within many governments, told the committee in WikiLeaks' submission[166] that the nature of information-sharing among the so-called "5 Eyes" countries (the United States, Canada, the UK, Australia and New Zealand) had been 'fundamentally misrepresented'. Mr Assange said:

> When asked about the information sharing practices of the 5 Eyes, the Committee heard on 23 April 2014 from Assistant Inspector General Blight from the Office of the IGIS that "... data sharing about Australian persons for ASD is regulated tightly by the Intelligence Services Act and the privacy rules made under that act and that data about Australian persons is subject to quite strict oversight .
>
> In fact, the revelations of Edward Snowden have documented shared and integrated 5 Eyes databases, and that untargeted, bulk interception,

166 WikiLeaks, *Submission 46*.

> collection and sharing of algorithmic analysis of private communications are routine among the 5 Eyes intelligence agencies.
>
> It is absurd that Australian government agencies continue to misrepresent the nature of interception and their access to intercepted data via 5 Eyes sharing arrangements when their equivalents in the UK have acknowledged their role in mass surveillance, including through convenient interpretations of domestic laws to absorb "external communications" which includes all communications transiting Internet platforms and services such as Google, Skype, Facebook, Yahoo not based in the UK.

1.186 Mr Assange particularly drew the committee's attention to documents submitted to the UK Investigatory Powers Tribunal by Mr Charles Blandford Farr, the Director-General of the UK Government's Office for Security and Counter-Terrorism. Mr Blandford Farr's attendance at the Tribunal attracted attention in June 2014 particularly for his comments that UK intelligence services could legally intercept communications through social media and webmail services operated by companies such as Google and Facebook.

1.187 Mr Assange also drew the committee's attention to the US NSA XKEYSCORE surveillance program, the UK Tempora program. He wrote:

> This [XKEYSCORE] program includes a Five Eyes Defeat checkbox that allows analysts to filter out data from one or more of the Five Eyes countries. Such a check box makes sense only in the context of a default sharing of information among the 5 Eyes that inevitably and necessarily circumvents the [Telecommunications (Interception and Access) Act].
>
> [IGIS] Dr. Thom confirmed that the "quite strict oversight" also applied to Australian citizens abroad. The Tempora program also revealed by Snowden refutes this simplistic assumption. Under that program, all 5 Eyes nations access data and metadata resulting from British tapping of fibre optic cable; there are no protections provided to Australians under such indiscriminate collection and sharing arrangements.
>
> Amendments made to the Intelligence Services Act in 2011, including the "WikiLeaks Amendment" so dubbed by employees of the Attorney General's Department, greatly reduced the scope or meaning of protections for Australians overseas and greatly increased the surveillance of their communications permitted.

By expanding the scope of surveillance overreach to anyone that was "in the interest of Australia's national security, Australia's foreign relations or Australia's economic wellbeing," almost anyone could be caught, rendering the 'strict oversight' a gesture, a meaningless gesture in the context of mass surveillance, collection and sharing of intelligence.

Senator Scott Ludlam
Inquiry Chair