4

Data retention period

The retention period

4.1 Subsection 187C(1) of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) provides that service providers must retain most telecommunications data covered by the data set for two years after it comes into existence.

4.1 The exception to this general rule is 'subscriber data', being data covered by paragraph 187A(2)(a), which must be retained from when it is created until two years after the closure of the relevant account. However, subsection 187C(2) provides that regulations may still prescribe the shorter, two-year retention period for specified subscriber data. The Government's proposed data set, included at Appendix A to this report, states that:

> The regulations will also limit the retention of subscriber information described in item 1 (c)-(f) to two years from creation of that data.

4.2 Accordingly, name, address and contractual information would be required to be kept for the life of the account plus two years, and all other telecommunications data covered by the data set would be required to be kept for the shorter, two-year period.

4.3 The Explanatory Memorandum explains why a longer retention period has been included for subscriber data:

> Subscriber records are typically generated when an account or service is opened, and may not be updated for many years. The purpose of this provision is to ensure that subscriber records associated with an account are available throughout the life of the account, and for as long as records relating to communications sent using that account are retained. This is intended to ensure

> that the necessary information is available to establish a connection between a particular communication and the subscriber.[1]

4.4 The Explanatory Memorandum also states that:

> A retention requirement of two years is consistent with the aim of the legislation and is necessary having regard to the reasonable requirements of national security and law enforcement agencies to have telecommunications data available for investigations and the privacy of users of the Australian telecommunications system.[2]

4.5 The Statement of Compatibility with Human Rights further explains the necessity and proportionality of a two-year retention period:

> The retention period reflects international experience that, while the majority of requests for access to telecommunications data are for data that is less than 6 months old, certain types of investigations are characterised by a requirement to access to data up to 2 years old. These include complex investigations such as terrorism, financial crimes and organised criminal activity, serious sexual assaults, premeditated offences and transnational investigations. Against the particular context of the critical importance of telecommunications data in very serious crime types and security threats, the two year retention period provides a proportionate response to that environment.[3]

General discussion

4.6 The Australian Privacy Commissioner provided extensive evidence on this issue, covering the privacy implications of various retention periods, how the Committee should approach assessing the necessity and proportionality of particular retention periods, and his assessment of what retention period is supported by the publicly-available information. As a starting principle, the Commissioner stressed the need to ensure that the retention period is set at the minimum necessary for law enforcement and national security purposes:

> To minimise any impact, I would suggest that the committee should satisfy itself, firstly, that each item of the dataset that service providers would be required to collect and retain under the scheme is necessary and proportionate; and secondly, that the

1 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 48.

2 Data Retention Bill, *Explanatory Memorandum*, p. 48.

3 Data Retention Bill, *Explanatory Memorandum*, p. 18.

> retention period imposed in relation to each item of the dataset is also necessary and proportionate.[4]

4.7 The Commissioner's view was also supported by the Law Council of Australia.[5]

4.8 A number of submissions cited various figures published by the European Commission showing the age breakdown for requests for access to telecommunications data by EU member-States.[6] There was some variability between the figures cited, however, as different submitters selected different date ranges. The Attorney-General's Department produced a table summarising figures released by the European Commission in its report, *Statistics on requests for data under the directive for 2008-2012*, which appear to be the most comprehensive figures available. These figures are set out at Table 4.1 below.

Table 4.1 Summary of age of telecommunications data requested under the EU Data Retention Directive in countries with two-year data retention periods, 2008-12

	Age of telecommunications data requested (months)							
	0–3	*3–6*	*6–9*	*9–12*	*12–15*	*15–18*	*18–21*	*21–24*
Percentage of requests	57.81%	19.59%	8.03%	5.03%	2.80%	2.00%	1.51%	3.24%
Cumulative percentage of requests	57.81%	77.40%	85.43%	90.46%	93.25%	95.25%	96.76%	100.00%

Source *Attorney-General's Department, Submission 27, p. 30.*

4.9 In its submission, the Department provided a detailed justification for a two-year retention period, based on its assessment of the European Commission's review:

> It is essential to distinguish between the frequency with which agencies access older data, and the importance of that data to investigations when it is accessed: where agencies require access to telecommunications data, its value does not decrease with age. While the review found that approximately 90% of requests for access relate to telecommunications data less than twelve months old, this number is skewed heavily by the use of telecommunications data in more straight-forward 'volume crime' investigations that, despite being serious in nature, can frequently

4 Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard,* Canberra, 29 January 2015, p. 46.

5 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard,* Canberra, 30 January 2015, p. 33.

6 See, for example: Australian Human Rights Commission, *Submission 42*, p. 8; Muslim Legal Network (NSW), *Submission 198*, p. 11.

be resolved in a shorter period of time. As such, the above summary obscures the fact that certain types of law enforcement investigations frequently involve longer investigatory periods and therefore require a disproportionate level of access to older telecommunications data.

4.10 The Department explained that these types of investigations included:

- counter-terrorism and organised crime investigations, which are often characterised by long periods of preparation. These investigations often require time to establish a clear pattern of relationships between multiple events to expose not just individual suspects, but entire criminal networks, especially where suspects are practicing sophisticated counter-surveillance techniques
- series of related crimes, where agencies are required to piece together evidence from a wide range of sources, not all of which may be immediately evident
- cyber-crimes and other crimes where access to IP-based telecommunications data is required, due to the greater complexity of these investigations—the EU statistics show agencies are up to 7 times more likely to access IP-based data that is more than 12 months old than mobile telephony data
- trafficking in human beings and drug trafficking, where there is often a complex division of labour between accomplices
- serious corruption of public officials, financial crime and tax fraud, where offences are often only detected following audits, or are only reported to law enforcement agencies following internal investigations, requiring agencies to often access data that is already considerably dated
- repeated extortion, where victims are in a relationship with the offender and often only seek help months or even years after the exploitation commenced
- serious sexual offences, where victims may not report the offence for a considerable period of time after the event—for example, the United Kingdom Government has provided advice that over half of the telecommunications data used by its agencies in the investigation of serious sexual offences is more than six months old
- serious criminal offences, particularly in relation to murder investigations, where extensive historical evidence must be assembled to prove intent or premeditation, and
- transnational investigations, which involve significant challenges for agencies attempting to coordinate investigations across multiple jurisdictions, frequently resulting in delays

> while preliminary information is obtained from foreign agencies.[7]

4.11 The Department added that:

> More broadly, many crimes are not brought to the attention of the relevant authorities until well after the fact, and the normal variability in criminal investigations means that some investigations will continue for considerably longer than average. In such cases, reliable access to telecommunications data can be particularly important, as physical and forensic evidence will frequently degrade with the passage of time.[8]

4.12 The Committee received a number of submissions and heard evidence from a number of witnesses calling for a shorter retention period, either for all or part of the data set.

4.13 Blueprint for Free Speech recommended that, if the Committee recommended passing the Bill, the retention period should be capped at six months to limit the privacy and regulatory impacts. It noted that, for countries subject to the former EU Data Retention Directive:

> the period of storage is typically between 6-12 months. This is well short of the 2-year period proposed by this legislation. In fact, these periods are likely too long. A report on the UK experience demonstrated that in approximately 75% of cases over a 4-year period, the data sought to be accessed was less than 3 months old.[9]

4.14 Similarly, the Law Institute of Victoria argued that the retention period should be reduced to what is 'strictly necessary and proportionate' and argued for a six month period.[10]

4.15 The Australian Privacy Commissioner provided a detailed assessment of what retention period he believed is supported by the publicly-available information:

> Statistical evidence, both international and domestic, seems to suggest that a large proportion of investigations use telecommunications data that is up to or less than one-year old. Acknowledging that there are differing views on what this evidence shows, it could nevertheless support a case for a shorter one-year data retention period. However, the case for a two-year data retention scheme is less clear. It may rest on information that is being made available to the committee but which is not being

7 Attorney-General's Department, *Submission 27*, p. 31.

8 Attorney-General's Department, *Submission 27*, p. 31.

9 Blueprint for Free Speech, *Submission 54*, p. 13.

10 Law Institute of Victoria, *Submission 117.1*, p. 10.

> released publicly—I assume to ensure that it does not prejudice the activities of law enforcement and security agencies. It is therefore important that close consideration be given to whether the evidence provided to the committee establishes that it is necessary to retain each item of telecommunications data for a minimum period of two years or, alternatively, whether a shorter retention period would meet the needs of law enforcement and security agencies.[11]

4.16 However, the Commissioner confirmed that he does not rule out a two-year retention period being justified as necessary and proportionate,[12] and cautioned that the Committee should have regard to the gravity of the matters that require access to older telecommunications data, and not place undue weight on the raw figures showing that such data is accessed in only a minority of cases:

> We should not just limit it to the number of cases because, as we start looking at some of these matters—I am feeling a bit odd here because it seems like I am starting to defend the position of the law enforcement and security agencies—it is about how large an impact they could have on the community. A particular investigation could be one that prevents an attack which could impact on hundreds or thousands of people.[13]

4.17 The Commissioner also observed that, given that the proposed data set makes clear the Government's intention to limit the retention period for items 1(c) to 1(f) of the data set to two years, rather than the life of the account plus two years, 'there does not appear to be a compelling reason for that limitation not to be contained in the Bill.'[14]

4.18 The Australian Human Rights Commission noted the EU Court of Justice's conclusion that retention periods should be limited to that which is 'strictly necessary',[15] and that the proposed two-year retention period is 'at the upper end of retention periods implemented in comparable jurisdictions'.[16] In its submission, the Commission argued that the Bill should be amended to incorporate a one-year retention period on a trial basis, subject to the statutory review by this Committee.[17] However, at a

11 Mr Pilgrim, *Committee Hansard,* Canberra, 29 January 2015, p. 46.

12 Mr Pilgrim, *Committee Hansard,* Canberra, 29 January 2015, p. 55.

13 Mr Pilgrim, *Committee Hansard,* Canberra, 29 January 2015, p. 48.

14 Office of the Australian Information Commissioner, *Submission 92*, p. 15.

15 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [64].

16 Australian Human Rights Commission, *Submission 42*, p. 9.

17 Australian Human Rights Commission, *Submission 42*, pp. 8-9.

public hearing, the Commission's President, Professor Gillian Triggs, noted that international comparison are 'relevant evidence; it is not determinative',[18] and that she 'would not argue too strongly for a year'.[19]

4.19 Professor Triggs went on to argue that 'the debate about the period is missing the core point',[20] and that, as the objective of data retention is to facilitate the better investigation of persons involved in serious crime and threats to security, uniform data retention is a 'crude instrument to deal with a problem that is a very sophisticated one and one where considerably greater lengths of time may be necessary.'[21] In this vein, Professor Triggs proposed that the uniform data retention period be coupled with an independent administrative mechanism to allow the retention period to be extended—potentially by many years—in relation to specific matters, such as the investigation of a serious risk to security or a child exploitation network.[22] The Committee discussed this proposal with Professor Triggs in significant detail.

4.20 The Committee also received evidence from organisations and members of the community in favour of the proposed two-year retention period. For example, Bravehearts noted the importance of a longer retention period for serious criminal investigations and recommended that the retention period be further assessed as part of the mandatory review established by the Bill:

> While the European Union's period and statements from police demonstrate that many investigations are completed within months, serious crimes often necessitate access to older records as the criminal behaviour may span a number of years. This is particularly true for investigations of child sexual exploitation.
>
> We note that the data retention period set in the Bill is at a minimum of two years and support this proposal. In addition, Bravehearts would recommend that after a three year period, as part of a review of the legislation, an assessment be made as to whether the 2 year retention period is the most appropriate length of time.[23]

4.21 Professor George Williams and Dr Keiran Hardy, in their capacity as members of the Gilbert + Tobin Centre of Public Law at the University of

18 Emeritus Professor Gillian Triggs, President, Australian Human Rights Commission, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

19 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

20 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

21 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 71.

22 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, pp. 71-75.

23 Bravehearts, *Submission 33*, p. 4.

New South Wales, expressed the view that, as of 9 December 2014, the Government had not yet justified a two-year retention period:

> The government has reasoned that data less than six months old is the most frequently accessed, but data up to two years old can be necessary for investigations into terrorism and other complex criminal offences. Given that this timeframe is central to the operation of the regime, we believe that a stronger case needs to be made as to why it is necessary. … In particular, a stronger justification for the two-year timeframe could help to reduce public perceptions that the Bill is designed to allow mass surveillance of the population.[24]

4.22 However, in evidence to the Committee on 30 January 2015, Professor Williams advised that he had revised his position, based on the submissions and evidence provided by the Attorney-General's Department and government agencies:

> The first thing I will say is that that statement was made on 9 December, when we did not have access to other submissions that have now provided a much higher degree of detail about this. Indeed, I would say that I am very pleased to see that those agencies are now strongly making the case as to why that two-year period is necessary. One thing I have looked at carefully is the table on page 30 of the Attorney-General's Department's submission, where, based on European data, they have also given an indication as to when certain data is accessed. I do not have a strong view on this issue, because I think it is one that depends very much on operational issues. I think it gets outside of my expertise.
>
> But I suppose the threshold question for me is that, based on the European data, over 90 per cent of all requests are made within the first 12 months. Is the case compelling enough to extend it for another 12 months, given the cost and the extension of the scheme? As the submission indicates, it perhaps might be justified if it can be shown that in fact terrorism investigations, particularly, tend to take place in that second 12-month period. If that is the case then perhaps that threshold I have indicated can be met.[25]

4.23 As discussed in Chapter 6, a joint submission from a number of media organisations argued that the introduction of a data retention regime would increase the difficulty faced by journalists in gathering information

24 Professor George Williams AO and Dr Keiran Hardy, *Submission 5*, p. 2.

25 Professor Williams, *Committee Hansard,* Canberra, 30 January 2015, pp. 7-8.

from confidential sources.[26] However, in evidence, Ms Georgia-Kate Schubert, Head of Policy and Government Affairs for News Corp. Australia, confirmed that the actual retention period is of significantly less concern to journalists than is the underlying ability of law enforcement and national security agencies to be able to identify confidential sources.[27]

Industry interests

4.24 Following a public hearing with the Communications Alliance and the Australian Mobile Telecommunications Association (AMTA), the Committee requested that Telstra, Optus, Vodafone, iiNet, TPG, Next Telecom, M2 Group, and the Inabox Group provide submissions setting out their existing retention practices. These companies represent a broad cross-section of the telecommunications industry, including the major, vertically integrated carriers, large ISPs, enterprise providers, and companies providing dedicated services to small and medium ISPs. The Committee received commercially confidential submissions from Telstra, Optus and Vodafone,[28] as well as an item of correspondence from the Inabox Group.

4.25 The Director-General of Security also provided the Committee with an unclassified summary of ASIO's assessment of existing industry practices in relation to critical categories of telecommunications data (Table 4.2),[29] as well as a more granular, classified assessment.[30]

4.26 The Committee has carefully reviewed the submissions provided by service providers and ASIO, and considers that ASIO's unclassified assessment, reproduced in Table 4.2 below, provides a useful summary of existing retention practices across the telecommunications industry.

---

26 Joint media organisations, *Submission 125*, p. 1. The joint submission was made on behalf of Australian Associated Press, the Australian Broadcasting Corporation, APN News and Media, the Australian Subscription Television and Radio Association, Bauer Media, Commercial Radio Australia, Fairfax Media, FreeTV, the Media, Entertainment and Arts Alliance, News Corp. Australia, the Special Broadcasting Service, The Newspaper Works, and the West Australian.

27 Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp. Australia, *Committee Hansard,* Canberra, 29 January 2015, p. 93.

28 Telstra, *Submission 112.1*; Optus, *Submission 86.1*; Vodafone, *Submission 130.1.*

29 ASIO, *Submission 12.2*, p. 5.

30 ASIO, *Submission 12.2*, Appendix B; and *Submission 12.3*.

Table 4.2 Comparative ranges of retention by main service providers of historical communications data

Matters to which information must relate	Telephony	Internet
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Up to 7 years (and longer)	90 days to 5 years
2. The source of a communication	6 weeks to 7 years 62 days to 7 years (for SMS)	0 days to 5 years
3. The destination of a communication		
4. The date, time and duration of a communication, or of its connection to a relevant service		
5. The type of communication or relevant service used in connection with a communication	Up to 7 years	90 days to 5 years

Source *Australian Security Intelligence Organisation, Submission 12.2, p. 5.*

4.27 The Attorney-General's Department and Communications Alliance separately drew the Committee's attention to the Telecommunications Consumer Protection Code, which requires all carriage service providers who supply telecommunications products to consumers in Australia to retain 'Billing Information' for at least six years.[31] Billing information includes any information necessary for the purposes of:

- calculating and assembling charges incurred by a customer during a billing period,
- applying any debits or credits outstanding or discounts due against the charges, and calculating the net amount payable by the customer,
- issuing and delivering bills to the billing address,
- handling billing enquiries, and
- receiving and receipting payments made by the customer.[32]

4.28 Optus confirmed that, for its networks and services, the general requirement to keep the proposed data set for two years 'is a workable time period for most data types'.[33] Optus also confirmed that, while the extended retention period for subscriber records 'has the potential to create some additional record keeping complexity depending on the compliance approach adopted', this requirement would overall not 'create

31 Telecommunications Consumer Protection Code, p. 47.

32 Telecommunications Consumer Protection Code, p. 12.

33 Optus, *Submission 86*, p. 10.

any significant retention burden as most of this type of information is already kept by Optus for longer than these periods for other legal reasons'.[34]

4.29 A number of industry representatives also noted that, given the significant variation between service providers' commercial retention practices, many service providers do not currently retain some of the types of telecommunications data covered by the proposed data set. For example, Mr Michael Elsegood, appearing as a member of the Communications Alliance and AMTA, explained that:

> On the usage side is where I think there is probably a greater discrepancy. Some service providers might be billing on a fairly bulk basis and would not be collecting fine-detail information about the customer's services. In that sense, they may not have the detailed usage records that might be required out of a data retention regime. On the mobile side, any information about mobile location may not be being stored in systems at all because there is simply no business reason to keep track of where your customers are. From an operational point of view, you may keep that for a very short period of time to deal with customer complaints or technical complaints about the operation of your network. So you might keep some short-term records about how your network has been performing. But in the long term you would not be keeping that sort of stuff.[35]

4.30 The Communications Alliance summarised this issue in the following terms:

> It is a data creation regime as well as a data retention regime, for all of those providers who do not presently retain everything in the dataset.[36]

4.31 This statement was consistent with ASIO's assessment of current retention practices across the telecommunications industry, which notes that some service providers currently retain some categories of telecommunications data for '0 days'.[37] The Attorney-General's Department noted that while all of the categories of telecommunications data contained in the proposed data set 'exist' on providers' networks, as they are 'typically required in the provision of the communications service itself', some types of data

34 Optus, *Submission 86*, p. 10.

35 Mr Michael Elsegood, Member of Communications Alliance and Manager of Regulatory Compliance and Safeguards, Optus, *Committee Hansard,* Canberra, 17 December 2014, p. 37.

36 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard,* Canberra, 17 December 2014, p. 31.

37 See Table 4.2 above.

may exist only 'fleetingly'.[38] In such situations, service providers would be required to begin collecting and retaining such telecommunications data.

4.32 Proposed new subsection 187A(6) of the Bill makes clear that service providers would be required to create any relevant information that was not currently retained. The Explanatory Memorandum states that:

> Subsection 187A(6) will clarify that if the information or documents that service providers are required to keep under subsection 187A(1) are not created by the operation of the relevant service, or if they are only created in a transient fashion, then the service provider is required to use other means to create this information or document.
>
> Mandatory data retention is the creation of a consistent minimum standard across the telecommunications industry for what data is to be collected and how long it is to be retained. Subsection 187A(6) will ensure that all service providers must meet this minimum standard, whether or not that data is currently being collected or retained by the relevant service provider.[39]

4.33 Optus also noted that there are likely to be a small number of cases in which the retention of certain categories of telecommunications data for particular services would be more difficult, and recommended amending the Bill to allow the regulations to prescribe a shorter retention period for 'specific or "special case" data or service types' would enhance the flexibility of the overall data retention arrangements.[40]

4.34 In its supplementary submission, the Attorney-General's Department has advised that :

> The Department has sought to estimate the cost of implementing the proposed data retention obligation, including seeking to assess the variation in capital costs of implementation if data were to be retained for 12, 24 and 36 months respectively. Extending the data retention period for industry participants will increase the capital costs of implementation; however a preliminary assessment indicates that the costs impacts are modest, and are substantially less than the percentage change in the retention period.[41]

---

38 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 11.

39 Data Retention Bill, *Explanatory Memorandum*, p. 46.

40 Optus, *Submission 86*, p. 10.

41 Attorney-General's Department, *Submission 27.2*, pp. 4-5.

4.35 The Committee also received a confidential briefing on the preliminary findings of the PricewaterhouseCoopers report on the costs of implementing data retention.

4.36 The Committee has considered the implications of a two-year retention period across a range of different data types below.

Law enforcement and security interests

4.37 Law enforcement and national security agencies supported a two-year retention period. A number of law enforcement agencies and ASIO noted that, from an investigative perspective, a retention period of greater than two years would be beneficial. However, there was recognition within the law enforcement and national security communities that mandatory data retention obligations should be used only to establish a minimum, legally-binding standard for record-keeping.

4.38 The Director-General of Security confirmed that ASIO supports a two-year retention period,[42] but emphasised that due to ASIO's unique investigative requirements, particularly in relation to counter-espionage investigations, this two-year period was the 'minimum' viable retention period from his perspective.[43] ASIO's submission stated:

> A two year retention period is a compromise from ASIO's perspective – we would prefer a longer retention period due to the long-term nature of some security threats, the sophistication of foreign intelligence actors, and that intelligence lead information can surface many months or years after an event has occurred. For example, leads to individuals who have recruited spies or facilitated individuals to terrorist training camps require ASIO to examine historical connections to understand those they may have influenced to engage in activities prejudicial to Australia's security.[44]

4.39 ASIO and the Attorney-General's Department advised the Committee that the proposed two year retention period is the result of 'extensive' engagement between the Attorney-General's Department, and law enforcement and national security agencies. In the course of these consultations, ASIO had advocated for a retention period of up to five years, however the Department concluded that the shorter, two-year retention period would be proportionate to the legitimate ends of

42 Mr Duncan Lewis AO DSC CSC, Director-General of Security, ASIO, *Committee Hansard,* Canberra, 30 January 2015, p. 64.

43 Mr Lewis, *Committee Hansard,* Canberra, 30 January 2015, p. 66.

44 ASIO, *Submission 12.1*, p. 9.

safeguarding national security and public safety, and the enforcement of the criminal law.[45]

4.40 ASIO addressed the Australian Privacy Commissioner's comments in relation to the potential distinction between the number of authorisations made for access to telecommunications data more than two years old, and the relative gravity of the subject matter of the investigations to which those authorisations relate:

> A point that was made by one of the previous witnesses here was that the data we pull from deeper into the time period is quite often the most important because it will be some critical piece of a major inquiry. I would also—and this is a particular and peculiar requirement for ASIO—reinforce the point that counterintelligence investigations have a very long sine wave.[46]

4.41 The Australian Federal Police (AFP) emphasised that, while the majority of criminal investigations relate to relatively recent conduct, complex and serious investigations often require access to telecommunications data from a considerable time ago:

> The nature of criminal investigations means that the bulk of matters subject to investigation relate to relatively recent conduct. However, where those investigations relate to historical events, the investigation will likely be more complex, relate to more serious conduct, or both. While the volume of requests for telecommunications data beyond 12 months old is likely to be lower than for more recent data, the relative value of that data is likely to be more significant.
>
> An example of historical events that may be the subject of investigation are international child protection operations, where information on Australian IP addresses are identified. This process may take a significant amount of time, meaning that data could be more than a year old before it becomes available to Australian authorities. Delays in the provision of information may relate to:
>
> - Lack of control over prioritisation or legal processes in foreign partner agencies;
> - Administrative processes associated with international cooperative
> - arrangements;
> - Establishment of coordinated international operational activity;
> - Technical difficulties in analysis of source data.[47]

45 *Committee Hansard,* Canberra, 30 January 2015, p. 68.

46 Mr Lewis, *Committee Hansard,* Canberra, 30 January 2015, p. 66.

47 AFP, *Submission 7*, p. 3.

4.42 The AFP stressed that the value of telecommunications data does not diminish with age, and that in many cases its value will increase as other sources of evidence are lost:

> [T]here is no clear correlation between the age of the information and its intrinsic value. Depending on the type of investigation, telecommunications data could be as important five years after an event as it is in the immediate aftermath. Moreover, in complex cases the value of older data may increase, particularly where physical evidence has eroded or (as is the case [in] cyber investigations) it is non-existent, making telecommunications data the key piece of information and evidence available.[48]

4.43 Deputy Commissioner Michael Phelan noted that agencies are often not in a position to even begin investigations for some time after a crime has been committed, due to delays in criminal activity being brought to their attention:

> You are actually beholden to when the originating information comes to you not from when the offence occurred. So an offence occurred last year, three years ago, two years ago, 10 years ago but you can only start the investigation when you know about it. That has sometimes been lost on some of our commentators, that they think the offence occurred and straightaway we have access to the information. That is not true.[49]

4.44 The Australian Commission for Law Enforcement Integrity (ACLEI) explained the particular importance of older data to anti-corruption investigations:

> The sophistication of corrupt networks (and organised criminals generally) develops over time. If left undisturbed, it is likely that they will become competent at counter-surveillance and increase their ability to defeat law enforcement efforts.
>
> …
>
> The means and frequency of contact with each individual varies over time, making it difficult to know how wide a corrupt network is, or how deep the compromise may be. Older data can be more useful, since it increases the chances of hidden relationships being discovered.[50]

---

48 AFP, *Submission 7.1*, p. 5.

49 Deputy Commissioner Michael Phelan APM, Australian Federal Police, *Committee Hansard,* Canberra, 30 January 2015, p. 75.

50 Australian Commission for Law Enforcement Integrity, *Submission 48*, p. 5.

4.45 ACLEI also provided the Committee with a detailed case study analysing the role that 18-month old telecommunications data played in Operation Heritage/Marca. The investigation, which began in 2011, uncovered a drug importation ring involving corrupt Customs and Department of Agriculture officials that had been operating since at least 2007. Initial investigations considered a particular associate as being benign. However, subsequent analysis of telecommunications data up to 18 months old demonstrated that this associate did, in fact, have corrupt connections, had been involved in criminal conduct, and was in fact a central figure in the conspiracy. The associate had, however, become more cautious over time and had adopted more sophisticated tradecraft that enabled him to avoid other forms of detection, including in the initial stages of Operation Heritage/Marca.[51]

4.46 From the perspective of a state police force, the New South Wales Police Force (NSW Police) argued that a longer retention period would be preferable:

> Whilst two years may be appropriate for the majority of offences investigated by the Commonwealth, such as national security, drug and online sexual offences, states are also responsible for investigating a range of criminal offences, including murders, sexual assaults and robberies, which are often historical or take years to investigate prior to a suspect being identified.
>
> …
>
> The need for data retention for extended periods is even more important at the moment, as DNA, trace evidence and other forensic science becomes more sophisticated and it is possible to test against older crime exhibits, resulting in the identification of suspects years after offences being committed.[52]

4.47 NSW Police provided the Committee with a detailed account of the types of matters currently under investigation dating back more than five years:

> [T]o perhaps clarify that this is not just rhetoric, we have some records on our books at the moment that justify data in excess of five years. Whilst they are minimal, as Mr Lanyon has alluded to—minimal in terms of the volume of requests that are handled up-front in the first six to 12 months—we have nearly 1,000 cases involving most-serious fraud, unsolved homicides, historical

51 Australian Commission for Law Enforcement Integrity, *Submission 48*, pp. 7-8.

52 Assistant Commissioner Mal Lanyon APM, Commander, Special Services Group, New South Wales Police Force, *Committee Hansard,* Canberra, 30 January 2015, p. 43.

> sexual assaults, and a lot of clear-up armed robberies. They are fairly complex crimes in that batch.[53]

4.48 Victoria Police similarly advised the Committee that:

> If we are looking at an investigation that may be afoot three, four, five or six years after a communication, almost invariably it is going to be an investigation of great significance. Law enforcement is not going to take on an incident that occurred that long ago, unless it is a homicide, a sex crime, a crime of significant personal violence, a counterterrorism inquiry or something of that nature.
>
> The other point I would make, and I think it has already been borne out in other evidence before you, is that the reality is that the bulk of these types of inquiries are made when this data is relatively new. Minimal inquiries are made father out. But again, they are ones that pertain to investigations that are probably of greater import.[54]

4.49 NSW Police also highlighted to the Committee that law enforcement agencies are not only required to access telecommunications data as part of criminal investigations, but are also required to access such information at the request of prosecutors and defendants in the course of proceedings, which can occur months or even years after the investigation itself concludes:

> [W]hen a court proceeding comes up, whether it is a trial, a hearing or a committal, somewhere down the track, whether it is two, three, four or five years, we get requests from the DPP and from the defence in terms of alibis, in terms of checking out a particular witness's statement, a particular location or a particular subscriber. So we get after the fact type requests for metadata.[55]

4.50 South Australia Police further argued that the importance of telecommunications data aged more than two years' old is likely to increase into the future, rather than decrease:

> If we got to two years, from an investigative perspective that is a retrograde step, especially when you are dealing with more and more historical offences, be they murders or historical sex offences, which do require that information. All of us around the table here

---

53 Detective Superintendent Arthur Kopsias APM, Commander, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard,* Canberra, 30 January 2015, p. 52.

54 Inspector Gavan Segrave, Intelligence and Covert Support Command, Victoria Police, *Committee Hansard,* Canberra, 30 January 2015, p. 51.

55 Detective Superintendent Kopsias, *Committee Hansard,* Canberra, 30 January 2015, p. 52.

> would understand that the reliance on and use of electronic devices such as those we are talking about is not going to go away. It is increasing. So we will become more and more reliant on this sort of technology in the future.
>
> From a law enforcement perspective and, I would imagine, also from a security perspective, the longer the data is kept the better because there will be investigations where we would ordinarily have sought information that goes back beyond two years. This is about trying to create a minimum standard that is level across the industry. As the department has already said, there are internet providers now who routinely hold this information for up to seven years and perhaps longer, depending on the way their systems are configured. From a policing perspective, that would be beneficial to us. But this is about creating a minimum standard. … Two years is a time frame that law enforcement and security agencies have accepted. That is appropriate in the circumstances, but I can see instances where we will still claw back further than two years if the data is held. If data is not held under this regime then it is not available to us.[56]

4.51 NSW Police expressed concern that the proposed two year retention period would not prevent service providers from reducing their current retention practices to a two-year minimum, which would significantly reduce the period of time for which certain types of telecommunications data are retained:

> The reason that New South Wales has asked for that period of two years, particularly with call charge records and reverse call charge records and subscriber checks to be longer than that period is that there is nothing to stop a service provider keeping for commercial purposes what are only billing records, after two years.[57]

4.52 On 4 December 2014, the Committee wrote to the heads of the ACC, AFP, ASIO and State and Territory police forces to request information about their agencies' access to and use of both stored communications and telecommunications data. In particular, the Committee sought information about the age breakdown of historical telecommunications data for which access was sought in each of the past five years.

---

56 Assistant Commissioner Paul Dickson, Crime Service, South Australia Police, *Committee Hansard,* Canberra, 30 January 2015, p. 52.

57 Assistant Commissioner Lanyon, *Committee Hansard,* Canberra, 30 January 2015, p. 51.

4.53 Some were unable to provide the Committee with information about the age breakdown of historical telecommunications data for which access was sought. For example, the Western Australia Police stated that:

> the systems used do not permit interrogation to identify the age of the data requested. Each request would have to be manually checked to identify the date range, and WA Police is unable to allocate resources required to provide the information without affecting core policing services.[58]

4.54 South Australia Police was able to provide the Committee with an age breakdown for the historic telecommunications data for which access was sought. Between 1 July 2010 and 31 June 2014:

- data less than three months old was sought in between 36.9 per cent and 38.9 per cent of authorisations,
- data between three months old and 12 months old was sought in between 0.1 per cent and 1.2 per cent of authorisations, and
- data more than 12 months old was sought in between 61 per cent and 62.1 per cent of authorisations.[59]

4.55 Queensland Police advised that, while its record keeping systems were not designed to specifically record the requested information, it had attempted to manually analyse the available information for the 2013 and 2014 calendar years:

> Although the data showed a strong tendency towards recent information this is attributable to the fact [that] most offences are reported soon after occurring and investigations that use a high volume of telecommunications information, such as drug matters, are focused on current real time events.
>
> The sample set did show at least 10% of authorisations were for information over 12 months old; however the sample set is considered to be too small to provide a reliable indication of the true requirement for and value of information more than 12 months old. Anecdotally, it is offences such as cold case homicide, historical sex offences and other serious offences where new suspects are identified that require older telecommunications data.[60]

4.56 In public evidence, Ms Kerri Hartland, Acting Director-General of Security, explained that:

---

58 Western Australia Police, *Submission 11*, p. 2.

59 South Australia Police, *Submission 9*, pp. 2-3.

60 Queensland Police, *Submission 19*, pp. 2-3.

> Around 10 per cent of the requests are for periods of 12 months or more, leading into periods of up to two years and beyond. Those cases relate to—10 per cent may seem small number—our most serious and complex cases. Typically, these relate to activities of hostile foreign nationals or nations engaged in spying and influence operations against Australia.[61]

4.57 The Committee also received a classified submission from ASIO containing the number of data authorisations made by ASIO over the past five years, as well as a breakdown of the age of data requested. The information contained in that classified submission is consistent with Ms Hartland's evidence. It is also consistent with the previous evidence of the former Director-General of Security, Mr David Irvine, to the Senate Legal and Constitutional Affairs References Committee that the number of authorisations made by ASIO for access to telecommunications data each year is 'proportionate… with other individual agencies.'[62]

4.58 The New South Wales Ministry for Police and Emergency Services provided the Committee with a confidential submission containing detailed statistics on its use of telecommunications data.[63] NSW Police also provided some information on its use of telecommunications data in at a public hearing:

> Of the 122,000 requests for telecommunications data New South Wales submitted in the previous year, 4,358 of those requests related to a period greater than two years for retention. Whilst as a percentage this may not appear large, it represents a significant number of offences which may be solved with the access to the information after two years. It is worth pointing out that, of those requests for greater than two years' data, the most common offence was murder, followed by sexual assault and then robbery.[64]

4.59 Communications Alliance and the AMTA confirmed that the majority of requests received by service providers from agencies 'relate to data that is 6 months old or younger'.[65]

4.60 The Committee also received supplementary submissions from Telstra, Optus and Vodafone setting out the age-breakdown of requests for

---

61 Ms Kerri Hartland, Acting Director of Security, ASIO, *Committee Hansard,* Canberra, 17 December 2014, p. 5.

62 Mr David Irvine AO, *Committee Hansard,* Canberra, 21 July 2014, p. 10.

63 New South Wales Ministry for Police and Emergency Services, *Submission 199*.

64 Assistant Commissioner Lanyon, *Committee Hansard,* Canberra, 30 January 2015, p. 43.

65 Communications Alliance and AMTA, *Submission 6*, p. 8.

telecommunications data each service provider had received. Telstra's submission showed that, in the 2014 calendar year:

- 79% of requests related to data less than six months old,
- 11% of requests related to data more than 12 months old, and
- 4% of requests related to data more than 24 months old.[66]

4.61 Vodafone's and Optus' submissions contained a higher level of detail and were provided to the Committee on a confidential basis.

4.62 However, at a public hearing Vodafone noted that its experience in relation to telephony data is that approximately three quarters of all requests relate to data less than six months old, while approximately 15 per cent of requests relate to data more than 12 months old.[67] The figures contained in Vodafone's confidential submission are consistent with this evidence, [68] and the figures provided by Optus were broadly consistent with those provided by Telstra and Vodafone.[69]

4.63 A number of witnesses, from both Government and industry, cautioned that the age breakdowns for access to historic telecommunications data are limited by industry's current retention practices and so reflect the age of data that agencies are able to access, rather than the age of data that may be of benefit to law enforcement and national security investigations.[70]

4.64 Optus also noted that the statistical information available about the age breakdown of requests may be misleading due to a number of factors that would tend to understate the importance of access to older telecommunications data to investigations, and in particular for investigations into suspects using particular counter-surveillance techniques:

> The one thing I would say is to exercise some caution in drawing immediate conclusions about where the volume of requests lies in terms of the age of the information, because I think you always have to apply a matrix about the seriousness of the request and the preservation regimes which might operate in tandem.
>
> …
>
> There is one other thing that perhaps I would say. This is particularly Optus specific, and it is not necessarily drawn out in

66 Telstra, *Submission 112.2*, p. 2.

67 Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (Vodafone), *Committee Hansard,* Canberra, 29 January 2015, p. 60.

68 Vodafone, *Submission 130.2*.

69 Optus, *Submission 86.2*.

70 See, for example, Queensland Police, *Submission 19*, p. 3; Mr Elsegood, Optus, *Committee Hansard,* Canberra, 17 December 2014, p. 34.

> the table that we have provided to the committee in confidence, but it is worth noting. We have a large, prepaid mobile base of customers and, indeed, are suppliers to resellers, who also do that. And there a number of reasons why people might prefer prepaid phones. The turnover of prepaid accounts can sometimes be greater. That does tend to explain a little bit why there is disproportionate interest in that particular cohort of customers. I think that does influence some of the timing and the age of the data that has been looked at to date.[71]

Retention periods for particular data types

4.65 While the above discussion focused on the overall retention period, the Committee also received more granular evidence on the necessity and proportionality of retaining particular types of telecommunications data.

4.66 The following pages discuss this evidence with regard to five semi-distinct classes of information:

- subscriber or account-holder records,
- IP address allocation records;
- telecommunications data relating to telephony services, other than location records,
- telecommunications data relating to internet-based communications services, such as email, VoIP and messaging applications, and
- location records.

Subscriber records

4.67 ASIO's unclassified assessment of industry retention practices indicated that there is some considerable variation in the periods for which service providers retain the range of subscriber records that are covered by item 1 of the Government's proposed data set, however, this variability relates primarily to subscriber records for internet-based services.[72]

4.68 Communications Alliance described subscriber records as being 'more static' than usage information, and advised that providers 'keep most of that sort of information for two years or so'.[73] As noted earlier, Communications Alliance also drew the Committee's attention to the requirements under the Telecommunications Consumer Protection Code

71 Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Optus, *Committee Hansard,* Canberra, 30 January 2015, pp. 20-21.

72 ASIO, *Submission 12.2*, p. 5.

73 Mr Elsegood, *Committee Hansard,* Canberra, 17 December 2014, p. 37.

to retain 'billing information', which includes many subscriber records, for at least six years.[74]

4.69 Similarly, Vodafone advised the Committee that it had 'always held the traditional telephony metadata—billing records, account holders—for certainly longer than two years'.[75]

IP address allocation records

4.70 Vodafone argued that IP address allocation records should be retained for no more than six months. Vodafone based this argument on the relative privacy sensitivity of this information, evidence about access rates from European jurisdictions, and the relative utility of historic IP address allocation records. In relation to the privacy sensitivity of this category of telecommunications data, Vodafone expressed the view, informed by customer feedback, that IP address allocation records are more sensitive than other categories of telecommunications data, and should therefore be retained for no more than six months:

> Traditional metadata is generally account information and phone numbers, and often that information is in the *White Pages* and so on. The feedback we are getting from consumers is that that kind of information is less sensitive than IP identifier information.[76]

4.71 However, Vodafone also explained that an IP address allocation record 'is essentially analogous to a telephone phone number, where a customer, when they access the internet, gets assigned an IP identifier so that they can carry out access to the internet'.[77]

4.72 The Committee also notes Vodafone's previous evidence to the Senate Legal and Constitutional Affairs References Committee, referred to above, that it intends to implement capability to collect these records for its own business purposes.[78]

4.73 The Attorney-General's Department's submission took an opposing view to Vodafone, arguing that:

> For internet access services, the types of telecommunications data that service providers would be required to retain (subscriber records and IP address allocation records) are less privacy

74 Mr Stanton, *Committee Hansard,* Canberra, 17 December 2014, p. 39.

75 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 62.

76 Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia, *Committee Hansard,* Canberra, 29 January 2015, p. 60.

77 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 60.

78 Mr Lobb, *Committee Hansard,* Senate Legal and Constitutional Affairs References Committee, Canberra, 26 September 2014, p. 20.

> sensitive than the records they would be required to retain for 'traditional' telephony services (including call-charge and limited location records).[79]

4.74 Vodafone also highlighted the European Commission's *Evaluation Report*, which concluded that the majority of law enforcement requests for access to telecommunications data are for data less than six months old. However, Vodafone confirmed that it had only very limited experience with law enforcement requests for IP address allocation records.[80]

4.75 Vodafone further advanced the argument that law enforcement agencies would be relatively less interested in IP address allocation records aged more than six months old, compared to traditional telephony records aged more than six months old:

> Certainly our view is that IP identifier metadata would be of most use more immediately than telephony metadata. That is because it is ever-changing. I think it is going to be potentially useful in regard to IP telephony. I think there are other ways of overseeing that. But when you are talking about an 'under surveillance' website, an agency will be looking at a dodgy website, and IP identifier accesses that website and the agency wants to find out who that person is, it is unlikely that that will be in two years hence. It is much more likely to be an immediate offence.[81]

4.76 In evidence, Optus advised the Committee that it did retain IP address allocation records, albeit with some variability between different services.[82]

4.77 The Committee received confidential evidence from ASIO, Optus and other service providers on this issue about their current retention practices for IP address allocation records.[83] This evidence showed a great deal of variability between service providers, and even between services provided by the same provider, ranging from negligible through to well in excess of two years.

4.78 In its submission, the Attorney-General's Department noted that agencies are actually significantly more likely to need access to IP-based telecommunications data aged more than 12 months old compared to other types of telecommunications data, due to the more complex nature of cybercrime investigations. Additionally, the Committee notes that the

79 Attorney-General's Department, *Submission 27*, p. 32.

80 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, pp. 68-69.

81 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 64.

82 Mr Elsegood, *Committee Hansard,* Canberra, 30 January 2015, p. 21.

83 Optus, *Submission 86.1*; ASIO, *Submission 12.2*, Appendix B.

inherently global nature of internet-based communications means that the assistance of foreign law enforcement agencies is a more common requirement in investigations where such communications are involved. The Department stated:

> certain types of law enforcement investigations frequently involve longer investigatory periods and therefore require a disproportionate level of access to older telecommunications data. These types of investigations include, but are not limited to:
>
> …
>
> - cyber-crimes and other crimes where access to IP-based telecommunications data is required, due to the greater complexity of these investigations
>
> …
>
> - transnational investigations, which involve significant challenges for agencies attempting to coordinate investigations across multiple jurisdictions, frequently resulting in delays while preliminary information is obtained from foreign agencies.[84]

4.79 The Department also drew the Committee's attention to the findings of the European Commission in its *Evaluation Report*, and in particular that, for a range of operational reasons, law enforcement agencies were seven times more likely to require access to IP-based telecommunications data aged more than six months old, compared to telecommunications data relating to mobile telephone services aged more than six months old.[85]

4.80 The Committee also received a supplementary confidential submission from Optus which confirmed that the age-profile of requests for IP-based data is significantly older than for other data types, despite the significant variation in retention practices between Optus services.[86]

4.81 The Uniting Church Justice and International Mission Unit drew the Committee's attention to the Australian Institute of Criminology's findings in a 2009 research paper on the grooming of children online for future sexual exploitation, which highlights the critical importance of access to IP address allocation records for the investigation of this particularly pernicious crime:

> The modern criminal, using the same devices as today's teenagers, communications with Voice over Internet Protocol, video instant messaging, cellular camera phone, and text messaging in

84 Attorney-General's Department, *Submission 27*, p. 31.

85 European Commission, *Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, p. 22, referred to in Attorney-General's Department, *Submission 27*, p. 31.

86 Optus, *Submission 86.2*.

> computer slang that is foreign to most police officers and parents. The trail to uncover this valuable investigation resource often starts with a forensic examination, but this trail quickly grows cold as Internet Service Providers overwrite logs and data retention periods expire. All police agencies are facing the same challenge when dealing with computer forensics. Police managers must find a way to examine an increasing number of digital devices, each containing an immense volume of data, in a timely manner and with limited resources.[87]

4.82 The case study of Operation Drakensberg, provided by the AFP, exemplifies the above points. In November 2013, the UK police referred 552 IP addresses suspected of accessing child exploitation material on a UK-based website that was compromised for a short period of time in late 2011 to the AFP for further investigation. The AFP received more than 5 500 referrals for online child exploitation matters from international law enforcement agencies for in 2014,[88]and confirmed to the Committee during a private briefing that the two-year delay in the referral in Operations Drakensberg was the result of ordinary and proper investigative procedures conducted in the UK, and is not uncommon for such international referrals.

4.83 Bravehearts noted that '[f]or child sex offenders advances in on-line technologies are continuing to provide increased opportunities; including for grooming victims, accessing child exploitation material and networking',[89] and supported a two-year retention period 'as a critical tool for supporting the investigation of child sexual exploitation matters'.[90]

Telecommunications data relating to telephony services

4.84 Communications Alliance and the AMTA confirmed that, for telephony services, the Government's proposed data set and two-year retention period would not significantly alter existing industry practice:

> Industry notes that an appropriately defined data set relating to the standard telephone service and a requirement to retain such

87 Kim-Kwang Raymond Choo, *Online child grooming: a literature review of the misuse of social networking sites for growing children for sexual offences*, Australian Institute of Criminology Research and Public Policy Series 103, 2009, p. 82, quoted in Uniting Church in Australia, Justice and International Mission Unit, Synod of Victoria and Tasmania, *Submission 76*, p. 5.

88 AFP, *Submission 7.2*, p. 2.

89 Bravehearts, *Submission 33*, p. 2.

90 Bravehearts, *Submission 33*, p. 4.

> for a period of two years, as requested by agencies and proposed by Government, would be close to current industry practice.[91]

4.85 In evidence to the Committee, Communications Alliance further confirmed that the proposed data retention scheme for the Public Switched Telephone Network (PSTN) (which includes fixed, mobile and satellite telephony networks) 'has zero impact. You have the data anyway'.[92]

4.86 Vodafone also confirmed that it would continue to hold telecommunications data for its telephony services for in excess of two years, irrespective of any new data retention obligations imposed by this Bill.[93]

4.87 NSW Police argued for the retention period for subscriber and telephony data to be extended to six years, to match the existing industry standard set out in the Telecommunications Consumer Protection Code:

> My concern is that, regarding some of the data which I feel is least intrusive, if I can put it that way, and would be of concern, we have the potential to have it for a lesser period of time than we currently do. My submission to the Committee was that we could consider expanding that period or keeping that persion as it was for that data, which would be an extension of what the Bill is currently proposing.[94]

Telecommunications data related to internet-based services

4.88 Communications Alliance and the AMTA submitted that:

> Industry is… far from convinced that a two year retention period for IP-related data is either necessary, justifiable, cost-effective, or in the public interest.[95]

4.89 Communications Alliance gave further evidence on these issues:

> There are storage, maintenance and other costs associated with IP data, which is typically growing at a much faster rate than telephony data; the longer you need to store it the more it is going to cost. Also, there is a general recognition in many of those [EU] jurisdictions that it is the younger data, overwhelmingly, that is

91 Communications Alliance and the AMTA, *Submission 6*, p. 7.

92 Mr Peter Froelich, Industry Member, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

93 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 64.

94 Assistant Commissioner Lanyon, *Committee Hansard,* Canberra, 30 January 2015, p. 58.

95 Communications Alliance and the AMTA, *Submission 6*, p. 7.

> useful to the pursuit of serious crime and national-security issues.[96]

4.90 However, Communications Alliance and the AMTA also noted that there is a diversity of views within the telecommunications industry about whether a uniform retention period would result in a simpler and cheaper system:

> That said, there is some debate among our members as to whether the potential greater simplicity of having a uniform retention period for all services is outweighed by the expense of and complexities of building to a longer than necessary retention period for non-telephone data.[97]

4.91 Accordingly, Communications Alliance and the AMTA recommended that the Bill be amended to require service providers to retain data for a period 'in the order of 6 months' in conjunction with a provision that 'make[s] it clear that such data can be retained for up to two years without exposing the CSP to a potential breach of the Privacy Act'.[98]

4.92 The Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG), which represents the Australian digital industry and therefore has interests relating primarily to internet-based services, supported Communications Alliance's position,[99] and suggested that the two-year retention period goes 'well beyond what international experience suggests is necessary for effective law enforcement'.[100]

4.93 Communications Alliance argued that the cost to industry of retaining telecommunications data relating to internet-based services is likely to increase exponentially, rather than linearly, beyond a two-year retention period:

> I guess the costs are not strictly incremental but more exponential. In terms of the way that data growth is in the industry at the moment, as you start to blow out the time period from two years to three years, four years, five years or whatever you propose, the volume of data usage on an internet-type service is growing at a factor of 10 times. So you will have those exponential growths on

96 Mr Stanton, *Committee Hansard,* Canberra, 17 December 2014, p. 38.

97 Communications Alliance and the AMTA, *Submission 6*, p. 7.

98 Communications Alliance and the AMTA, *Submission 6*, p. 8.

99 Australian Interactive Media Industry Association (AIMIA) Digital Policy Group, *Submission 34*, p. 3.

100 AIMIA Digital Policy Group, *Submission 34*, p. 3.

> top of the basic incremental growth of the length of time you want to store the data.[101]

4.94 However, Telstra disagreed with the proposition that the retention period would have either a 'significant' or 'exponential' impact on the capital or operational cost of any data retention scheme:

> The costs will change if the prescribed period changes. We have costed to two years. If that were to change, then our costings would change. Will we get substantially different costs? Probably not, because a lot of the capital cost is setting up the systems to extract this data.
>
> …
>
> I am not sure that we necessarily agree on the use of the word 'significant'. It certainly has an impact on cost, because the more data there is then the greater the task to continue to maintain that database, make it accessible and then to interrogate when required. With changes it becomes more complex. So there is a relationship between the retention period and the cost of the scheme. I am not sure that we would go as far as saying it is significant, but it is certainly a factor.[102]

4.95 Mr Chris Berg, Senior Fellow at the Institute for Public affairs, argued that there is a fundamental distinction between the types of telecommunications data associated with traditional telephony services, such as voice calls or SMS, and the internet-based communications covered by the proposed data set, such as VoIP and email:

> [I]nternet activity and telephone activity are not parallels. They operate under substantially different technological paradigms, and they have vastly different social profiles. Where telephone conversations are an adjunct to our lives, internet access is central to it – an enormous amount of interaction with the world is done through the internet. What we do on the internet is part of our private domain to a degree that telephone conversations are not. We live our lives online – to a great degree our work, private lives, our leisure, and our personal and professional relationships are mediated by digital technologies.[103]

4.96 Telstra's submission argued in favour of a single fixed retention period across all technologies and data types. In part, Telstra's position was based

---

101 Mr Froelich, *Committee Hansard,* Canberra, 17 December 2014, p. 35.

102 Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard,* Canberra, 29 January 2015, pp. 14, 20.

103 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, pp. 4-5.

on the size and complexity of Telstra's own network and service offerings.[104] Telstra also argued strongly that a single retention period would prevent criminals from migrating to alternative services to evade lawful surveillance, and would promote competitive neutrality in a rapidly evolving technological environment:

> [O]bligations should be technologically agnostic to the greatest extent possible. For example, one set of retention obligations should not apply to traditional technologies, such as PSTN or mobile voice and SMS services, while different obligations apply to competing technologies, such as Voice over IP or instant messaging. Not only would asymmetric regulatory obligations put providers of the traditional services at a competitive disadvantage, it would create a perverse incentive from criminals to circumvent scrutiny by the agencies by using the alternative services.[105]

4.97 The Committee notes the findings of the European Commission's Evaluation Report on the Data Retention Directive, that 'internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations',[106] and that EU law enforcement agencies are significantly *more* likely to access internet-related data that is aged more than 12 months compared to other types of telecommunications data.[107]

4.98 The Attorney-General's Department argued that internet-based communications services are similar in functionality, from a user's perspective, to traditional telephony services, and so should be required to retain analogous records.[108]

4.99 The Data Retention Implementation Working Group (IWG) noted that the data set adopts a technologically-neutral approach, and that 'some European nations encountered challenges with the EU Data Retention Directive's technically specific approach, which has inhibited its application to new technologies.'[109] The Attorney-General's Department similarly highlighted the importance of a technologically neutral approach and the importance of drawing on international experience.[110] The

104 Telstra, *Submission 112*, p. 3.

105 Telstra, *Submission 112*, p. 3.

106 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 2011, p. 22.

107 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 2011, p. 22.

108 Attorney-General's Department, *Submission 27*, p. 32.

109 Data Retention Implementation Working Group (IWG), *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 5.

110 Attorney-General's Department, *Submission 27*, p. 25.

Department cited the Netherlands Government's review of its data retention laws, which concluded that:

> It is not quite clear on the basis of which arguments the retention periods for telephone and internet traffic data vary. It is possible that arguments pertaining to privacy issues (in part) underlie this distinction. However, the nature of the internet data stored, effectively doesn't pose a greater infringement on individual privacy when compared to the nature of telephony data.
>
> …
>
> The retention period of six months for internet data is considered unanimously to be too short by the criminal investigations professionals and experts. This is particularly so for complex cases where such data can be useful.[111]

4.100 The IWG industry members noted that 'significant technological change is likely to occur within the Australian telecommunications industry, with potential for significant technological evolution even in the short term.'[112]

Location records

4.101 The Committee received a range of evidence about the privacy sensitivity and utility of location records, which has been discussed above.

4.102 Communications Alliance provided evidence to the Senate Legal and Constitutional Affairs References Committee that location data 'is typically not kept for long periods of time today but would need to be'.[113] The confidential submissions received from service providers indicated that retention practices for location records vary considerably, both between providers and between individual services offered by the same provider, with records not being kept for some services, and being kept for well in excess of two years for others.

4.103 The Attorney-General's Department acknowledged that, 'Arguably, location records are less intimately linked to the remainder of the data set', but that the contextual information that could be provided to other telecommunications data by knowing the location from which a communication was made was particularly important, including to exculpate individuals from suspicion:

---

111 Netherlands Government, *The Dutch Implementation of the Data Retention Directive*, p. 139. The Netherlands Government had implemented laws requiring telephony data to be retained for 12 months, and internet-related data to be retained for six months.

112 IWG, *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 5.

113 Mr Stanton, *Committee Hansard,* Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 9.

> For example, where a suspect makes a phone call immediately after the time a crime was committed, that phone call may appear suspicious. However, location records showing the phone call was made several suburbs from the scene of the crime would tend to remove that person from suspicion.[114]

International comparisons

4.104 The Department provided the Committee with a summary of past and present retention practices across 35 Western countries.[115] Communications Alliance and the AMTA also provided the Committee with a summary of past and present retention practices across 25 Western countries.[116]

4.105 There were a limited number of inconsistencies between the two summaries. In summary, 26 countries previously required or currently require a uniform retention period for both 'traditional' telephony data and internet-based data. Of those countries:

- South Africa specified a 3-year retention period,
- Poland specified a 2-year retention period,
- Latvia specified an eighteen-month retention period,
- twelve specified a twelve-month retention period,[117] and
- eleven specified a 6-month retention period, [118] although the Swiss Government has introduced new laws into its Parliament to increase its retention period to 12 months.

4.106 The remaining nine countries specified different retention periods for different types of telecommunications data:

- two specified a two-year period for fixed and mobile telephony data, and a one-year period for internet access, email and telephony data,[119]
- the United States specified an 18-month period for telephony data, and does not require the retention of internet-based data,

114 Attorney-General's Department, *Submission 27*, pp. 32-33.

115 Attorney-General's Department, *Submission 27*, pp. 38–40.

116 Communications Alliance

117 Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Greece, Spain, France, Portugal, Finland and the United Kingdom.

118 Austria, Cyprus, Germany, Iceland, Liechtenstein, Lithuania, Luxembourg, Romania, Sweden and Switzerland.

119 Ireland and Italy.

- Slovenia specified a 14-month period for fixed and mobile telephony data, and an eight-month period for internet access, email and telephony data,
- Brazil specified a 12-month period for IP connection logs, such as IP address allocation records, a 6-month period for IP access logs, such as web-browsing history, and does not require the retention of telephony data,
- Hungary specified a 12-month period for all telecommunications data, except for unsuccessful call attempts, which are retained for six months,
- two specified a 12-month period for fixed and mobile telephony data, and a six-month period for internet access, email and telephony data,[120] and
- Malta specified a 12-month period for fixed, mobile and internet telephony data, and a six-month period for internet access and email data.

4.107 In summary, 19 out of 34 countries have passed laws requiring the retention of internet-related data for at least 12 months,[121] and six out of 33 countries have implemented different retention periods for telephony and internet-related data.[122]

4.108 The Australian Human Rights Commission argued that the retention periods selected by other countries are 'relevant evidence' for this Committee, but are 'not determinative'.[123]

4.109 The Attorney-General's Department similarly indicated that the proposed data retention regime had drawn on international experience, rather than being identical to regimes in place in Europe.[124]

4.110 As noted above, the Department and Vodafone each drew the Committee's attention to the European Commission's *Evaluation Report*, which discussed the experience of EU nations under the former Data Retention Directive. The Report acknowledges that access to telecommunications data more than six months old is 'less frequent', but argues that access to older data can be 'crucial':

> Firstly, internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations. Analysis

120 The Netherlands and Slovakia.

121 The United States does not require the retention of internet-based data and so has not been counted.

122 The United States does not require the retention of internet-based data, and Brazil does not require the retention of telephony data. As such, these countries have not been counted.

123 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

124 Attorney-General's Department, *Submission 27*, p. 25.

> of fixed network and mobile telephony data often generates potential leads which result in further requests for older data. For example, if during an investigation a name has been found on the basis of fixed network or mobile telephony data, investigators may want to identify the Internet Protocol (IP) address this person has been using and may want to identify with whom that person has been in contact over a given period of time using this IP address. In such a scenario, investigators are likely to request data allowing the tracing also of communications with other IP addresses and the identity of the persons who have used those IP addresses.
>
> Secondly, investigations of particularly serious crimes, a series of crimes, organised crime and terrorist incidents tend to rely on older retained data reflecting the length of time taken to plan these offences, to identify patterns of criminal behaviour and relations between accomplices to a crime and to establish criminal intent. Activities connected with complex financial crimes are often only detected after several months. Thirdly, and exceptionally, Member States have requested traffic data held in another Member State, which can usually only release these data with judicial authorisation in response to a letter rogatory issued by a judge in the requesting Member State. This type of mutual legal assistance can be a lengthy process, which explains why some of the requested data was in these cases over six months old.[125]

4.111 The European Commission also identified that, while the majority of requests for access to telecommunications data in the EU were made within a few months or even weeks of the communication taking place, there were four types of criminal investigation for which older data tended to be required, being:

- terrorism and organised crime,
- serious sexual offences,
- substantiating previous intent to commit illegal activities, and
- large cross-border cases.[126]

4.112 The Commission further noted that, the adoption of flat-rate, unlimited use contracts and services had, prior to the introduction of mandatory data retention obligations, significantly impacted the availability of telecommunications data for investigative purposes. The Commission cited the examples of Germany, where the proportion of users with such

125 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 2011, p. 22.

126 European Commission, *Evidence for necessity of data retention in the EU*, 2013, pp. 4-5.

plans 'rose from 18% in 2005 to 87% in 2009' and noted that it had received advice from both data protection authorities and service providers that data about such services was of 'minimal business value and are only stored in a retrievable form because of mandatory data retention.'[127]

4.113 The Committee notes that major providers have begun offering such unlimited use plans in Australia, but not at the rates observed in Germany.

4.114 As noted above, the Committee's attention was also drawn to the Netherlands Government's review of its data retention laws. The review concluded *inter alia* that a six month retention regime was 'considered unanimously to be too short by the criminal investigations professionals and experts. This is particularly so for complex cases where such data can be useful.'[128] The review also noted that a 12 month retention period was adequate for the majority of cases, but that 'there are cases where for longer term investigations it is insufficient.'[129]

Committee comment

4.115 The length of time for which telecommunications data is retained has direct implications for both the necessity and the proportionality of the scheme.

4.116 Evidence received from ASIO, law enforcement agencies and service providers consistently showed that between 10 and 15 per cent of data authorisations made by Australian agencies are for data which is in excess of one year old. However, these requests disproportionately relate to investigations into serious and complex criminal activity, serious matters of national security (particularly counter-espionage investigations), and other complex cases. Despite constituting only a minority of all access requests, the public interest in the effective resolution of these matters is particularly strong.

4.117 The Committee notes that agencies consider a two year retention period to be a compromise and the minimum amount of time that would be acceptable from a national security and law enforcement perspective.

4.118 The Committee also notes that current retention practices are not uniform across the industry. Some service providers will be required to begin collecting telecommunications data that they do not currently hold for their business purposes. Other providers that do currently collect and retain the data will need to retain it for longer periods. In many cases,

127 European Commission, *Evidence for necessity of data retention in the EU*, 2013, p. 5.

128 Netherlands Government, *The Dutch Implementation of the Data Retention Directive*, p. 139.

129 Netherlands Government, *The Dutch Implementation of the Data Retention Directive*, p. 89.

however, service providers currently collect and retain telecommunications data covered by the proposed data set for well in excess of two years.

4.119 On the basis of the evidence provided, the Committee considers that a two-year retention period is necessary and proportionate. This two-year period would run from the time a particular communication is made, in the case of communications-related data, or from the time an account is closed, in the case of account-holder data.

4.120 The Committee acknowledges that a two-year retention period would place Australia at the upper end of retention periods adopted in other jurisdictions. Of the 35 Western countries identified as having implemented mandatory data retention obligations, only Italy, Ireland, Poland and South Africa require service providers to retain some or all telecommunications data for two years or more. However, the Committee accepts the unequivocal evidence of the national security and law enforcement agencies, which is supported by the international evidence, that a retention period of up to two years is necessary and proportionate for a range of investigations into particularly serious types of criminal and security-relevant activity.

4.121 The Committee received a confidential briefing on the costings from the Attorney-General's Department, which is discussed in greater detail later in this report. The analysis presented to the Committee as part of that briefing showed that reducing the retention period to 12 months would decrease the cost of the scheme by only five to six per cent.[130] Further, varied retention periods for different elements of the data set would risk undermining the efficacy of the scheme as a whole.

4.122 The Committee notes that longer retention periods may aid particular investigations. However, the effective conduct of serious national security and criminal investigations must be balanced against the degree to which a two-year retention period could interfere with the privacy, freedom of expression and other rights of ordinary Australians. For many service providers, a two-year retention period will not represent a substantial change to existing retention practices.

4.123 The Committee notes that the proposed two-year retention period would not impact the ability of service providers to retain telecommunications data for longer than two years for their legitimate business purposes.

130 Attorney-General's Department, *Submission 27.4*, p. 2.

Recommendation 9

The Committee recommends that the two-year retention period specified in section 187C of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be maintained.

4.124 The Committee notes that as a consequence of its earlier recommendation that the data set be contained in primary legislation, there may be some consequential amendments required to section 187C of the Bill that will need to be addressed. These may include consequential amendments to specify the appropriate retention period for different kinds of subscriber data that are covered by proposed new paragraph 187A(2)(a).

Should providers be required to destroy data at the end of the retention period?

4.125 Subsection 187C(3) of the Bill provides that service providers are not precluded from retaining telecommunications data covered by their data retention obligations for longer than two years. The Explanatory Memorandum notes that:

> This means, for example, that service providers will not be prevented by new section 187C from retaining telecommunications data for longer than two years for their own lawful business purposes.
>
> However, the Australian Privacy Principles (APPs), as set out in Schedule 1 of the *Privacy Act 1988* (the Privacy Act), will still apply to service providers and their dealings with the telecommunications data that is personal information and that is required to be retained under the new Part 5-1A of the TIA Act. For example, APP 11.2 requires entities to take reasonable steps to destroy personal information or to ensure that the information is de-identified where the entity no longer needs the information for a reason set out in the APPs. Where the required retention period for telecommunications data under the new Part 5-1A of the TIA Act expires, entities may be required to destroy or de-identify such information if it constitutes personal information.[131]

4.126 The Victorian Commissioner for Privacy and Data Protection noted that the Bill does not require the destruction of telecommunications data at the

131 Data Retention Bill, *Explanatory Memorandum*, p. 49.

end of the retention period.[132] This issue was also highlighted by the EU Court of Justice in its decision.[133]

4.127 In its submission, Electronic Frontiers Australia argued that s. 187C(3) of the Bill, which provides that service providers are not precluded from retaining data for longer than the prescribed period, should be removed from the Bill, and that service providers should instead be prohibited from retaining any telecommunications data for longer than two years.[134] However, in evidence to the Committee, Mr Lawrence conceded that 'it may not be of significant harm for [s. 187C(3)] to remain there', after it was pointed out that carriers routinely retain data for longer periods for their business purposes, and that the *Privacy Act 1988* continues to prohibit service providers from retaining data for any longer than required for those business purposes.[135]

Committee comment

4.128 The Committee understands that proposed new subsection 187C(3) is intended to operate as an avoidance of doubt provision. It is not intended to override the existing requirement under APP 11.2 that service providers destroy or de-identify information when it is no longer required for a legitimate purpose.

4.129 The Committee received a range of public and classified evidence from service providers, which is outlined in greater detail above, showing that service providers currently retain a wide range of telecommunications data for longer than the proposed two-year retention period, for their own business purposes and in compliance with other regulatory obligations, such as the Telecommunications Consumer Protection Code. The Committee considers that it is entirely appropriate for service providers to continue retaining such telecommunications data for longer than two years where they have a legitimate business purpose to do so, or in accordance with another regulatory obligation.

4.130 However, the proposed new data retention obligations will require service providers to retain some types of telecommunications data for longer than they otherwise would for their business purposes, or even to begin collecting and retaining particular types of telecommunications data for the first time. In these situations, the Committee is concerned that service providers should not retain such telecommunications data for longer than

132 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 11.

133 *Digital Rights Ireland v Ireland* and *Kärntner Landesregierung* (joined cases C-293/12 and C-594/12), [67].

134 Electronic Frontiers Australia, *Submission 97*, pp. 4-5.

135 Mr Lawrence, *Committee Hansard,* Canberra, 29 January 2015, p. 28.

the proposed two-year retention period without a legitimate business or regulatory purpose.

Recommendation 10

The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 clarify the requirements for service providers with regard to the retention, de-identification or destruction of data once the two year retention period has expired