3

The data set

Introduction

3.1 Proposed new Division 1 of Part 5-1A of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill), entitled 'Obligation to keep information and documents', would establish a mandatory telecommunications data retention regime. The proposed regime would require carriers, carriage service providers and internet service providers to retain a defined set of telecommunications data for two years, ensuring that such data remained available for law enforcement and national security investigations.

3.2 The following three chapters discuss the main issues raised in evidence to the inquiry in relation to Schedule 1 to the Bill, and the Committee's comments and recommendations in regard to those issues.

3.3 The chapters do not comment comprehensively on all aspects of the proposed regime. Instead, the chapters focus on the issues that were of most concern to the Committee, informed by the evidence received from participants in this inquiry in written submissions and at hearings. These issues were:

(Chapter 3)

- whether the Government's proposed data set should be contained in primary legislation, as opposed to being made in regulations, and
- the scope of the Government's proposed data set.

(Chapter 4)

- the proposed two-year retention period, and
- whether service providers should be required to destroy telecommunications data retained in accordance with proposed new Division 1 of Part 5-1A at the end of the retention-period.

(Chapter 5)

- the range of service providers and services to which data retention obligations are proposed to apply,
- the implementation arrangements for the proposed data retention regime, and
- the cost of the proposed data retention scheme.

Should the data set be contained in primary legislation?

3.4 Paragraph 187A(1)(a) of the Bill provides that service providers must keep information of a kind prescribed in regulations. This regulation-making power is subject to a number of limitations, the most significant being subclause 187A(2), which provides that the information prescribed for the purposes of subclause 187A(1)(a) must relate to one or more of six matters, being:

- the subscriber, accounts, telecommunications devices and other relevant services of a relevant service,
- the source of a communication,
- the destination of a communication,
- the date, time and duration of a communication,
- the type of communication, and
- the location of the line, equipment or telecommunications device.

3.5 The Explanatory Memorandum states:

> A regulation-making power is required to ensure that the legislative framework gives service providers sufficient technical detail about their data retention obligations while remaining flexible enough to adapt to future changes in communication technology.[1]

3.6 The Attorney-General's Department gave further evidence at a public hearing explaining the rationale for the data set being set out in subordinate legislation, in particular drawing the Committee's attention to international precedent on the value of a more flexible approach to amending the data set:

> I think international experience suggests that potentially reshaping may be required at a future point. Our international colleagues

1 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 36.

> have reflected on their experience with the EU Data Retention Directive, which took a technologically specific approach to their data set and found that it was very quickly outdated. We have learnt from that in some respects by proposing to prescribe a more technologically neutral data set. But our discussions with industry consistently reinforce the fact that telecommunications technology evolves at a rapid pace. The kinds of services that are available now were not available 10 years ago or even five years ago. There have been radical changes in the technology and service offerings that are available to customers, who include people who use telecommunications services to engage in criminal acts and other activities. On the basis of advice from industry, we believe technological change is almost inevitable. Regulations would provide a vehicle for potentially making any refinements that were necessary in an expeditious way. That is an advantage of a regulation based approach. Amendment to legislation is naturally possible, but it takes longer.[2]

3.7 In its supplementary submission, the Department noted the risks to national security and law enforcement if there is a delay in updating the data set in response to technological change:

> Sophisticated criminals and persons engaged in activities prejudicial to security are frequently early adopters of communications technologies that they perceive will assist them to evade lawful investigations.[3]

3.8 The Department also noted that the level of detail contained in the data set is typically included in regulation rather than primary legislation.[4]

3.9 In a letter to the Committee, dated 21 January 2015, the Director-General of Security provided a historical example of the significant delay that can occur where amendments to primary legislation are required to address technological change:

> A serious counter-example to defining everything in primary legislation is the history of [International Mobile Equipment Identifier (IMEI)] interception in Australia which took 10 years to achieve because it required change to the legislation. There was a technical solution available within months and, if it was open to

2 Ms Anna Harmer, Acting First Assistant Secretary, National Security Law and Policy Division, *Committee Hansard,* Canberra, 30 January 2015, p. 76.

3 Attorney-General's Department, *Submission 27.2*, p. 7.

4 Ms Harmer, *Committee Hansard,* Canberra, 17 December 2014, p. 16.

> make a regulatory change, it could have been adapted for in faster time without this capability gap for interception agencies.[5]

3.10 The Senate Standing Committee on the Scrutiny of Bills (Scrutiny of Bills Committee) concluded that paragraph 187A(1)(a) 'delegates legislative power inappropriately', and has recommended that 'the types of data to be retained should be set out in the primary legislation to allow full Parliamentary scrutiny.'[6]

3.11 The Scrutiny of Bills Committee also recommended that, if the data set is not set out in primary legislation:

> the bill be amended to ensure that any regulation under paragraph 187A(1)(a) setting out the types of data to be retained under the scheme does not come into effect until the regulation has been positively approved by each House of the Parliament (see, for example, s 10B of the Health Insurance Act 1973). At a minimum, the committee considers that such regulations should not come into effect until after the disallowance period has expired (as recommended by the [Implementation Working Group (IWG)].[7]

3.12 The Committee received submissions and evidence from a number of organisations and individuals recommending that the data set be set out in the Bill, rather than in regulations.[8]

3.13 Professor George Williams agreed with the Attorney-General's Department's assessment that there is no practical impediment to including the data set in primary legislation, and argued that the government's proposal to include the data set in regulations is 'very inappropriate given that the definition itself is at the heart of whether the scheme should proceed'.[9]

3.14 The Victorian Commissioner for Privacy and Data Protection supported the Scrutiny of Bills Committee's recommendation, noting that:

> The public interest in maintaining an extremely flexible data retention scheme does not outweigh the public interest in ensuring:
>
> - adequate privacy and security protections are maintained

5 Australian Security Intelligence Organisation, *Submission 12.2*, pp. 6-7.

6 Senate Standing Committee for the Scrutiny of Bills, *First Report of 2015*, p. 118.

7 Senate Standing Committee for the Scrutiny of Bills, *First Report of 2015*, p. 118.

8 See, for example: Australian Human Rights Commission, *Submission 42*, p. 7; Mr Douglas Stetner, *Submission 32*, p. 1.

9 Professor George Williams AO, Anthony Mason Professor of Law and Foundation Director of the Gilbert + Tobin Centre for Public Law, University of New South Wales, *Committee Hansard,* Canberra, 30 January 2015, p. 10.

- a certain and transparent scheme that is subject to public scrutiny.[10]

3.15 The Australian Privacy Commissioner provided the Committee with a detailed analysis of the relevant issues and identified a range of potential options:

> The bill allows for regulations to be made that significantly affect the scope of the data retention scheme. In particular, the bill allows for regulations to be made relating to the services covered by the data retention scheme and the kinds of telecommunications data that service providers will be required to collect and retain. To ensure the greatest level of certainty, transparency and accountability possible, my preference would be for these matters to be included in the bill itself. However, I do note that in a period of rapidly changing technology this may not be achievable. In the event, then, that a decision is made to continue with the current model, with these matters being addressed in regulations, I consider that the bill should be amended to include a requirement for the undertaking of a privacy impact assessment, before any changes are made or new regulations are made, and that the Australian Privacy Commissioner be consulted in the making of any new regulations or changes to the existing regulations.[11]

3.16 In its submission, the Law Council of Australia acknowledged that the disallowance process for regulations, which includes scrutiny of legislative instruments by the Senate Standing Committee on Regulations and Ordinances, might provide a mechanism to address concerns about the data set being unduly expanded by a future Minister. However, the Council argued that the fact that regulations come into force from the date of registration, which may be 'weeks or months before a disallowance motion may be tabled or considered by the Parliament', posed an unacceptable concern.[12]

3.17 However, at a public hearing, the Council indicated that it had revised its position, having noted the Privacy Commissioner's recommendations about additional safeguards that could be put in place to provide for greater oversight, while allowing for the data set to be amended via delegated legislation. The Council also endorsed any such amendments being referred to this Committee for review:

---

10 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 9.

11 Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard,* Canberra, 29 January 2015, p. 47.

12 Law Council of Australia, *Submission 126*, p. 14.

> I think they are all excellent suggestions. We had suggested in our submission that it should be included and therefore locked in the legislation itself in the interests of certainty but we do hear other evidence which says that there is a need for some flexibility, ability to change over time, and if it is considered that to lock the dataset into legislation itself is excessive, then these are the alternative safeguard mechanisms that could be used.[13]

3.18 Professor Williams gave evidence to the Committee recommending a hybrid approach whereby the data set is set out in the Bill, with a carefully circumscribed regulation-making power to allow the data set to be updated over time, if necessary:

> I accept the government's design for a level of flexibility; that does seem appropriate to me. But, to be frank, we have moved beyond flexibility to actually not telling much at all of substance about exactly what data will be collected. All we have are some guidelines which are fairly loose given they are relating to criteria, and I think what you have ended up with is a shell of a scheme… So I think the balance here is to define as precisely as possible what the data set is while proving a power to the attorney to make appropriate modifications to that within limits so that there is a degree of flexibility over time.[14]

3.19 Professor Williams and Dr Keiran Hardy also noted a particular concern, being that the current drafting of clause 187A(1) may allow telecommunications data to be prescribed that 'relate to' one of the categories listed in clause 187A(2) in a 'tenuous way'.[15]

3.20 Telstra and Optus both confirmed that, as service providers, they were agnostic about whether the data set is contained in primary or subordinate legislation and that their view, as service providers, is that it is more important to ensure that the consultation and implementation arrangements around any change to the data set ensure that any changes are technically feasible, cost-effective, allow for sufficient 'lead-time' to implement, and provide long-term regulatory certainty.[16] Optus also

---

13 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard,* Canberra, 30 January 2015, p. 36.

14 Professor Williams, *Committee Hansard,* Canberra, 30 January 2015, p. 5.

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

16 See, for example, Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 11; Ms Jane van Beelen, Executive Director, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 13; Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Singtel-Optus (Optus), *Committee Hansard*, Canberra, 30 January 2015, p. 17.

considered the use of regulations to set out the detail of the data set to be 'appropriate', and stated that, in its view:

> The proposed safeguards in the Bill are the guidance provided by section 187A(2) on the 'kind of information' that may be prescribed, and that the regulations are to be a disallowable instrument, which provides for Parliamentary scrutiny. These 'structural' safeguards appear adequate.[17]

3.21 In its first report, the Data Retention Implementation Working Group (IWG) acknowledged that any change to the data set could impose costs on service providers, and recommended greater procedural safeguards around any changes to the data set prescribed in regulations:

> The IWG recommends that any proposed change to the regulations should not enter into force immediately, but rather come into effect only after Parliament has had an opportunity to review the proposed change and the disallowance period has expired.[18]

3.22 The IWG also noted that, pursuant to paragraph 187F(2)(c) of the Bill, 'any change to the data set would also trigger the ability for industry to re-apply for an 18 month implementation plan'.[19]

3.23 In its submission, Optus also argued that the Bill should be amended to preclude changes to the data set until after this Committee has conducted its review of the scheme pursuant to proposed new section 187N (discussed later in this report). In Optus' view, this would provide service providers with 'a reasonable expectation of stability', which would allow for 'planning and investment certainty, and allow time for efficient practices to be developed and refined'.[20]

3.24 The Attorney-General's Department addressed this issue in its supplementary submission:

> The Department acknowledges the importance of regulatory certainty for industry, and notes the Department's extensive consultations with industry to support the development of a clear data set capable of implementation within provider networks. The joint Government-Industry Implementation Working Group considered the issues of both certainty and affording industry an appropriate interval to adapt to any changes in the data set and

17 Optus, *Submission 86*, p. 7.

18 Data Retention Implementation Working Group (IWG), *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 10.

19 IWG, *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 11.

20 Optus, *Submission 86*, p. 7.

> recommended that any changes to the data set not commence until after the expiry of the disallowance period. The Department supports that IWG recommendation.
>
> The Department considers however that precluding amendment of the data set until the completion of a future review may prejudice national security and law enforcement interests. Industry participants have consistently advised that their services and technology evolve rapidly. In circumstances where new services offerings and technology are inevitable in a technology and market driven environment, it is important for the framework to be able to respond to those changes. Only in the event that services offerings and technology are not changing would it be appropriate to fix the data set – in circumstances where the telecommunications services are certain to change, the Government should not be precluded from responding.[21]

3.25 The Committee also received a number of submissions which stated that the decision to leave the data set to be prescribed in regulations meant that submitters either did not have sufficient certainty to comment on the detail of the data set, or were unaware that the data set had been publicly released.[22]

3.26 The Department had published a copy of the Government's proposed data set and accompanying explanatory material on 31 October 2014, which the Committee has had access to throughout the inquiry. The Department confirmed on a number of occasions that this document, included at Appendix A to this report, is, in fact, the Government's proposed data set to be put into effect by regulation when the Bill receives Royal Assent.[23]

3.27 The Department acknowledged that there are a number of possible alternative approaches to defining the data set that could be adopted:

> There are a number of different approaches, as the committee will be familiar with. All could be in legislation; all detail could be in regulations. Alternatively, what we have here is what might be described as a hybrid model, under which the key criteria or threshold issues are described in the legislation, with the detail being left to regulation. That provides a degree of flexibility in the event that changes are required, while still providing the

---

21 Attorney-General's Department, *Submission 27.2*, p. 11.

22 See, for example, Mr Bernard Keane, *Submission 37*, pp. 2-4.

23 Ms Harmer, *Committee Hansard,* Canberra, 17 December 2014, p. 13; Ms Harmer, Letter to the Committee Secretary, 17 January 2015, published alongside Attorney-General's Department, *Submission 27*; Ms Harmer, *Committee Hansard,* Canberra, 30 January 2015, p. 71.

opportunity for parliamentary consideration of regulations that are made under that act.[24]

Committee comment

3.28 The set of telecommunications data that service providers will be required to retain is central to the operation of the proposed data retention regime. It is critical that industry and the Australian public are assured that the data set proposed comprises that which is necessary and proportionate, and that safeguards are in place to monitor any future proposals to amend the data set.

3.29 As such, the Committee considers that the proposed data set should be set out in primary legislation.

3.30 The Committee notes that, while the proposed data set has been developed to be a technologically-neutral scheme, future technologies or changing telecommunications practices may require amendments to the data set in time to maintain the core purpose of the scheme. Currently the Committee does not see a situation where emergency changes to the data set may be required. However, given the dynamic environment of developing technologies, the Committee has considered the merits of including an emergency declaration power.

Recommendation 2

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to include the proposed data set in primary legislation.

24 Ms Harmer, *Committee Hansard,* Canberra, 17 December 2014, p. 16.

Recommendation 3

To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare items for inclusion in the data set under the following conditions:

- **The declaration ceases to have effect after 40 sitting days of either House,**
- **An amendment to include the data item in legislation should be brought before the Parliament before the expiry of the 40 sitting days, and**
- **The amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report.**

The data set as proposed and Industry Working Group recommendations

3.31 Section 187A of the Bill establishes the set of telecommunications data that service providers would be required to retain. As the Explanatory Memorandum notes, '[d]ata retention obligations will not apply to all telecommunications data',[25] but to a defined set of telecommunications data prescribed in regulations.

3.32 The regulation-making power, currently proposed in the Bill, is subject to a number of limits. Subsection 187A(2) provides that the prescribed data must relate to one of six categories, outlined above.

3.33 The Bill also contains six further limits, being that service providers are not required to:

- keep the contents or substance of any communication,[26]
- keep web-browsing records or other records about the destination of communications sent via an internet access service,[27]
- keep records about communications sent or received using third-party communications services,[28]

25 Data Retention Bill, *Explanatory Memorandum*, p. 38.

26 Paragraph 187A(4)(a).

27 Paragraph 187A(4)(b).

28 Paragraph 187A(4)(c).

- keep records of information the provider would otherwise be required to delete under a determination made under section 99 of the Telecommunications Act, such as the Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Carriage Services) Determination 2013,[29]
- generate and keep location records that are more detailed than or different to the location records used in relation to the relevant service,[30] or
- keep location records on a continuous basis.[31]

3.34 Telstra welcomed the Government's decision to include these limits as part of the proposed scheme:

> In terms of minimising the impact of the scheme on industry and our customers, we welcome the limits that the government has established for the scheme, such as focusing on metadata rather than the content of communications and limiting the agencies that can access the data. We believe these limits will help give the community a greater degree of comfort about the access to telecommunications data by the agencies.[32]

3.35 The Government has not released a copy of draft regulations currently proposed to be made under the Bill. However, the Attorney-General's Department has published a proposed data set. The Department confirmed in the inquiry that the difference between the proposed data set and draft regulations would be a question of form, rather than substance.[33]

3.36 While not requiring it, the Bill will not preclude service providers from keeping the contents or substance of a communication for other lawful purposes.[34] For example, a company providing an email service may keep the emails sent and received on its servers. However, the Explanatory Memorandum explains that agencies are not permitted to access the content of communications held by service providers under a data authorisation:

---

29 Paragraph 187A(4)(d).

30 Paragraph 187A(4)(e).

31 Subsection 187A(7). Service providers would only be required to keep location records at the start and end of a communication, such as a phone or VoIP call or an SMS message, or the start and end of a communications session, such as an entire internet access session that may last for several hours through to many months.

32 Mr Shaw, *Committee Hansard,* Canberra, 29 January 2015, p. 7.

33 Ms Anna Harmer, Acting First Assistant Secretary, National Security Law and Policy Division, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 13.

34 Data Retention Bill, *Explanatory Memorandum*, p. 44.

> Section 172 of the TIA Act currently prohibits ASIO or enforcement agencies from authorising the disclosure of the substance or content of a communication under a data authorisation made under Chapter 4 of the Act. Agencies may only access the substance or content of a communication under a warrant, or in limited other circumstances, such as in a life-threatening emergency. [35]

3.37 The Inspector-General of Intelligence and Security (IGIS) also noted that a range of other telecommunications data will not be subject to data retention obligations but will, nevertheless, remain accessible to agencies under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to the extent that service providers continue to retain it for their ordinary business purposes.[36]

3.38 On 16 December 2014, the Attorney-General provided the Committee with *Report 1 of the Data Retention Implementation Working Group*. The Implementation Working Group (IWG) is a joint government-industry group is chaired by the Secretary of the Attorney-General's Department and is comprised of CEO-level representatives from Government and industry, and has been tasked by Government to 'further refine the data set and report back to the Government and the PJCIS'.[37] The IWG established an Experts' Group, comprised of technical experts from across Government and industry to assist the IWG in this task.

3.39 The IWG recommended four further amendments to the data set and identified a number of areas in which additional explanatory material would be beneficial. A list of the IWG's recommendations is included at Appendix C to this report. The IWG also prepared a revised data set in its report, including additional explanatory material, reflecting its recommendations.

3.40 As noted in the introduction to this report, the Attorney-General's Department clarified that the IWG's recommendations 'are intended to assist the Committee's consideration of the proposed data set rather than provide a replacement'.[38]

---

35 Data Retention Bill, *Explanatory Memorandum*, p. 44.

36 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard,* Canberra, 29 January 2015, p. 39.

37 IWG, *Report 1 of the Data Retention Implementation Working Group*, December 2014, Attachment B, p. 1.

38 Ms Harmer, Letter to the Committee Secretary, 16 January 2015.

Committee Comment

3.41 The Committee acknowledges the contribution of the data retention Implementation Working Group to the inquiry. The Committee recognises that the IWG's recommendations are the result of expert level consultation and cooperation between key national security and law enforcement agencies, and industry stakeholders.

3.42 The Committee notes that the IWG's recommended changes to the data set and its explanatory material (set out in Appendix C) do not significantly change the kinds of data that are intended to be retained under the scheme. The recommendations would rather provide greater technical clarity to industry as to the precise nature of their data retention obligations. As such, the Committee supports the implementation of these recommendations and recommends their inclusion in the final data set.

Recommendation 4

The Committee recommends that the proposed data set published by the Attorney-General's Department on 31 October 2014 be amended to incorporate the recommendations of the Data Retention Implementation Working Group.

Is the proposed data set sufficiently clear?

3.43 A number of service providers assured the Committee that the level of detail provided in the Government's proposed data set, in conjunction with the information provided through the IWG process, was sufficient for them to design and implement a data retention system.[39]

3.44 Optus assured the Committee that it had:

> appreciated the ability to work with the Data Retention Implementation Working Group, convened by the Attorney-General's Department. Indeed, I think some of those discussions have helped to better inform both their understanding of some of the operational issues that arise and our own, in addition to informing the wider industry.[40]

3.45 Optus drew particular attention to the 'very large' technical-level working group, established by the IWG, which included a 'very representative

39 See, for example, Mr Shaw, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 7; Mr Epstein, Optus, *Committee Hansard,* Canberra, 30 January 2015, p. 17.

40 Mr Epstein, Optus, *Committee Hansard,* Canberra, 30 January 2015, p. 13.

sample' of the telecommunications industry.[41] Optus also addressed the concerns raised by a number of submitters and witnesses about the potential lack of certainty about what would be contained in the final data set, arising from the government's decision to prescribe the data set in regulations:

> Clearly, I think the point has been made by others that there is not an extant draft regulation that has been circulated, but in effect we have had fairly detailed discussions and they have gone directly to a consistent set of points, and you would assume that those consistent set of points would form the basis of regulations. And, yes, they are a bit better than in the broad workable; they appear quite workable.[42]

3.46 However, a number of submitters raised particular issues relating to the proposed data set.

Passwords and PINs

3.47 Optus recommended, in its submission, that item 1 of the data set be amended to place beyond doubt that the data retention regime will not require service providers to retain customer passwords.[43] In evidence, Mr Epstein confirmed that Optus' concern is that the data set 'does not directly exclude it, so there is always that risk' that it could be interpreted as requiring the retention of passwords.[44]

3.48 In its supplementary submission, the Attorney-General's Department advised the Committee that:

> the retention of passwords would be inconsistent with both the proposed data set and the categories of data that may be prescribed. Accordingly, the Department does not consider that further amendment or consideration is required. However, the Department notes that, for clarity, the explanatory material to the data set could include an appropriate explanatory note to put the matter beyond doubt.[45]

Data that is not readily available to service providers

3.49 Optus also recommended that the requirement for service providers to retain information that is not otherwise created in the operation of a

41 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 23.

42 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 17.

43 Optus, *Submission 86*, p. 19.

44 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 27.

45 Attorney-General's Department, *Submission 27.2*, p. 13.

relevant service, contained in proposed new subsection 187A(6), be amended to ensure that it does not impose an effectively impossible obligation in circumstances where a service provider does not have access to the relevant information.[46] In its submission, however, Optus acknowledged the potential value of this provision, noting that it:

> appears to be an anti-avoidance or loop-hole prevention clause, which removes any incentive to design or create services in a manner which does not generate the required data set. [47]

3.50 In its supplementary submission, the Attorney-General's Department advised the Committee that:

> Pursuant to proposed paragraph 187A(4)(d), the data retention obligations will apply to the services provided by access service providers. This does not include Over-The-Top services accessed by the user through the service provided. For example, an internet service provider does not have to keep information in relation to a third party VOIP or email usage, but must retain data in relation to an email service they provide. To that extent the data retention obligations are therefore directly connected to matters within a provider's control, being the services that they provide and support.[48]

3.51 The Explanatory Memorandum states that this provision is intended to apply in circumstances where the relevant information or documents 'are not created by the operation of the relevant service, or if they are created in only a transient fashion'.[49]

Committee Comment

3.52 Customer passwords, PINs and other like information are highly private and security sensitive information. The Committee accepts that the Bill is not intended to require the retention of such information, and notes that the Government's proposed data set is expressed as including name, address and other information for identification purposes, but considers that it would be appropriate to clarify this issue in the Explanatory Memorandum.

---

46 Mr Michael Elsegood, Manager, Regulatory Compliance and Safeguards, Optus, *Committee Hansard,* Canberra, 30 January 2015, p. 28.

47 Optus, *Submission 86*, p. 9.

48 Attorney-General's Department, *Submission 27.2*, p. 13.

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

Recommendation 5

The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that service providers are not required to collect and retain customer passwords, PINs or other like information.

3.53 The Committee considers that it has not been made clear that service providers are not required to collect and retain telecommunications data about devices that are not directly connected to their network (for example, devices connected to the network via a third-party router), or the details of communications passing over the top of an internet access network via a third-party communications application.

3.54 There would be value in clarifying that service providers are not required to retain information that is not otherwise created in the operation of a relevant service.

Recommendation 6

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that service providers are only required to retain telecommunications data to the extent that such information is, in fact, available to that service provider.

Is there a need to retain each element of the data set?

3.55 The Statement of Compatibility with Human Rights for the Bill contains a detailed description of the investigative value of each category of telecommunications data listed in subsection 187A(2).[50]

3.56 The Committee notes that, on 14 November 2014, the Parliamentary Joint Committee on Human Rights (PJCHR) released its preliminary report on the Bill, stating that:

> The statement of compatibility separately assesses why each category of data is necessary in pursuit of the scheme's stated objective; and the committee considers that the statement of compatibility has generally established why particular categories of data are considered necessary for law enforcement agencies.

50 Data Retention Bill, *Explanatory Memorandum*, pp. 13-16.

3.57 The Department's submission contains further information relating to the Government's proposed data set.[51] The submission states that:

> Privacy and proportionality considerations have been central to the development of the proposed categories of data that the data retention obligations will apply to. The data retention obligations have been strictly limited to data that is vital to law enforcement and national security investigations, and was developed based on advice from law enforcement and national security agencies and feedback from the telecommunications industry.[52]

3.58 Communications Alliance and the Australian Mobile Telecommunications Association (AMTA) emphasised the importance of balancing the cost to industry and taxpayers against improved law enforcement and national security outcomes:

> [A]gencies will naturally tend to 'ask for everything' because completeness lowers the risk of any small detail being missed. But when telecommunications users and taxpayers are liable for the cost of 'everything', some discipline should be applied to the scope and volume of agency requests.[53]

3.59 However, the IWG report notes that 'the data set has previously been the subject of, and benefited from, refinements and additional explanations arising from extensive previous consultations with industry',[54] and that 'some industry constituents not[ed] that the data retention obligations did not appear as onerous as they initially anticipated'.[55]

Detailed subscriber and account information—Items 1(b)-(f)

3.60 Item 1 of the Government's proposed data set would require service providers to retain a range of records that relate to subscribers of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service, being:

(a) any information that is one or both of the following:

(i) any name or address information;

(ii) any other information for identification purposes;

---

51 Attorney-General's Department, *Submission 27*, pp. 26-30.

52 Attorney-General's Department, *Submission 27*, pp. 25.

53 Communications Alliance and the Australian Mobile Telecommunications Association, *Submission 1*, p. 2.

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

55 IWG, *Report 1 of the Data Retention Implementation Working Group,* December 2014, p. 3.

relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service;

(b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device;

(c) any information that is one or both of the following:

(i) billing or payment information;

(ii) contact information;

relating to the relevant service, being information used by the service provider in relation to the relevant service;

(d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device;

(e) the status of the relevant service, or any related account, service or device;

(f) any information about metrics of the relevant service or a related account, service or device.

3.61 The Law Institute of Victoria posed the question:

> Why is it necessary, for example, for service providers to retain the features and service descripts of their account holders *(sic)* products and services? This data would seem to include information like a customer changing their monthly broadband quota, whether they have call waiting activated, whether their phone plan allows free international calls or free texts to numbers from the same provider.
>
> Beyond name, address and other contact details, how is all the very detailed subscriber information set out in category 1 of the draft data set relevant to law enforcement? Data such as billing information, status of the service and metrics of the service seems to have marginal relevance to the enforcement of serious crimes and protecting national security.[56]

3.62 The Law Institute of Victoria also raised particular concerns about the retention of IP address allocation records, arguing that:

56 Law Institute of Victoria, *Submission 117*, p. 10.

> An IP address does not identify a person. The LIV is concerned about the preservation of the presumption of innocence in the context of the use of source IP addresses.[57]

3.63 Similarly, FutureWise argued that billing information (item 1(c)(i)) and information about the status (item 1(e)) and metrics (item 1(f)) of a service, seem to be of 'marginal relevance to law enforcement'.[58]

3.64 The Committee notes that the EU Data Retention Directive did not require service providers to keep records of historic aggregate upload and download volumes.[59]

3.65 However, the Department's submission provides a detailed explanation of the utility of these kinds of information to law enforcement and national security investigations:

> The information listed under item 1(c) (billing, payment or contact information) serves a similar purpose [to the types of subscriber records listed under item 1(a)], and is of particular utility where an account is subscribed under a false identity. Billing and payment information is generally more difficult to falsify, and contact information can often provide agencies with further investigative leads to identify who has made a communication of interest.
>
> The information listed under item 1(d) (identifiers relating to the relevant service) includes information such as the phone number or IP address/port number combination allocated to a particular account, service or device at a particular point in time. This information is necessary to allow particular communications of interest to be attributed to a particular account, service or device. Importantly, from a technical perspective, item 1(d) is limited to identifiers used by the service provider—item 1(d) does not require service providers to generate and retain identifiers that are not natively used by their network or service.
>
> The information listed under items 1(b) (contractual information), (e) (status of the service), and (f) (information about the metrics of the service) is critical for a range of technical purposes. Most importantly, this information is vital to allow agencies to properly

57 Law Institute of Victoria, *Submission 117*, p. 10.

58 FutureWise, *Submission 128*, p. 19.

59 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, available online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> viewed 26 February 2015.

> provision and resource interception warrants.
> Telecommunications interception, particularly in relation to IP-based services, is highly complex and resource intensive. Inadequate resourcing and provisioning of interception systems can result in potentially incuplatory or exculpatory intercept material being lost, compromising the evidential chain and the overall investigation. The information… allows agencies to make an informed, risk-based estimate of how many resources need to be allocated to a particular interception warrant (for example, based on th[e] historic usage of the service or services, whether any of those services are no longer active, and the maximum data allowance for each service).[60]

3.66 The Australian Federal Police explained the utility of historic, aggregate upload and download volume information from its perspective:

> First of all, working out whether or not the line is active is most important of all—whether there is any volume passing over it or not and the amount of volume are important. Torrenting is certainly not something that we have been looking at, but certainly the amount of volume also determines, when we want to put an internet intercept off, how much capability we will have to dedicate to it. For planning purposes as well that is extremely important to us. Like anything else, we have to know how many lines to put off, our monitoring capability, our monitoring capacity and so on. That is one component of it, but the most important is to know in the first place whether or not the line is active and if any volume passes between an account at all.[61]

3.67 The Acting Director-General of Security also provided further information from ASIO's perspective:

> To add to that, everything that the deputy commissioner has said is relevant from ASIO's perspective. Also—and I am happy to talk further about this in a closed hearing—in terms of looking at facilitation, networks who might be central, that sort of download information can be quite important in investigations.[62]

3.68 The IWG has recommended that item 1(f) of the data set, which relates to 'metrics of the relevant service or a related account, service or device', be removed from the data set, on the basis that 'data of this kind is often not

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

61 Deputy Commissioner Michael Phelan APM, Australian Federal Police, *Committee Hansard,* Canberra, 17 December 2014, p. 14.

62 Ms Kerri Hartland, Acting Director-General of Security, Australian Security Intelligence Organisation (ASIO), *Committee Hansard,* Canberra, 17 December 2014, p. 14.

available and often only created because of numerous short-term marketing-based variations to allowances', making the data 'difficult to collect and aggregate for storage on an ongoing basis'.[63] For example, service providers may release short-term promotional allowances, such as 'unlimited download weekends' or 'unlimited MMS messages for New Year's Eve'.

3.69 The IWG has acknowledged that:

> The availability of this information is useful and desirable for agencies and that, where the information is currently retained for business purposes, agencies would continue to be assisted by the availability of such information to the extent it is otherwise retained.[64]

3.70 However, the IWG has also recommended that item 5(c) be amended to clarify that service providers would continue to be required to keep records of the historical upload and download volumes.

3.71 As indicated earlier in this chapter, the Committee has recommended that the Government accept the IWG's recommended amendments to the data set.

Location information—Item 6

3.72 The Committee received a number of submissions calling, in particular, for location information to not be retained as part of any data retention regime.

3.73 For example, Blueprint for Free Speech noted that '[l]ocation data is especially sensitive' and argued that:

> It is not appropriate for private companies nor government to routinely track and store this sort of information without a citizen's permission simply because they are able. Nor is it right for government to access it without proper oversight from a judge authorising a warrant. Tracking all Australian citizens in this manner is a fundamental change in the relationship between the citizen and the state in this country.[65]

3.74 Electronic Frontiers Australia also expressed concerns at the privacy sensitivity of location records:

> It is a concerning development that equipment locations are included in the draft data set. A mobile phone user is likely to

63 IWG, *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 7.

64 IWG, *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 7.

65 Blueprint for Free Speech, *Submission 54*, p. 6.

> have their location retained multiple times per day. Even though this is limited to approximate positions such as which cell tower is in use, this is sufficient to reveal all of a person's travels for the two year retention period to suburb granularity. The significance of this sensitive information is presumably why it is included in the draft data set at all.[66]

3.75 The Australian Privacy Commissioner, in his submission, noted that even the limited location data that the Bill proposes to require service providers to retain could, in some instances, provide detail 'at a level approaching the equivalent effect of real-time location tracking'.[67]

3.76 A number of other submitters also noted the particular privacy sensitivity of location information.[68]

3.77 The Explanatory Memorandum notes that location-based information is used for a number of investigative purposes, including to demonstrate that a person was likely present at the scene of a crime, exclude suspects from further investigation where they were likely not at the scene of a crime, and to identify the historic movements and locations of missing persons:

> Location-based data is valuable for identifying the location of a device at the time of a communication, providing both evidence linking the presence of a device to an event, or alternative providing indications that may exclude a person from further inquiry. This data may also be instructive in determining the location of a person who is reporting an emergency, or help with precursory steps towards identifying the locality of a missing person who has used a telecommunications device. Without this information being retained by service providers, agencies' abilities to investigate crimes, emergencies and missing person matters are substantially limited.[69]

3.78 The Attorney-General's Department further emphasised that location records can provide important contextual information about related records:

> [L]ocation information can provide important contextual information about communications that is often important for both inculpatory and exculpatory purposes. For example, where a

66 Electronic Frontiers Australia, *Submission 97*, p. 21.

67 Office of the Australian Information Commissioner, *Submission 92*, Appendix B, p. 1.

68 See, for example: Telstra, *Submission 112*, p. 2; Internet Society of Australia, *Submission 122*, p. 6.

69 Data Retention Bill, *Explanatory Memorandum*, pp. 15-16.

> 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.[70]

3.79 In its submission, the Department agreed that location information is 'among the most sensitive elements of the dataset' and noted that:

> [T]he nature and volume of location information that service providers will be required to keep has been strictly limited to ensure that service providers are not required to keep continuous records about the location of a device, or anything approaching that level of detail.[71]

3.80 Consistent with the Department's statement, the Bill and the Government's proposed data set contain a number of limitations on the nature and volume of location information that service providers would be required to retain. Paragraph 187A(4)(e) of the Bill provides that service providers are only required to retain location information of the kind 'used by the service provider in relation to the relevant service to which the device is connected.' The Explanatory Memorandum elaborates on this provision:

> Paragraph 187A(4)(e) will provide that a service provider is not required to keep information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected. This could include, for example, a record of which cell tower, base station or other network access point a device was connected to.[72]

3.81 Additionally, paragraph 187A(4)(c) limits the extent to which service providers are required to retain information about 'over the top' data services. As the Explanatory Memorandum notes:

> The purpose of this provision is to ensure that the provider of an underlying service, such as an internet access service, is not required to keep information about communications that are passing 'over the top' of the underlying service and that are being carried by means of another relevant service, such as a VoIP service, operated by another provider.[73]

---

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

71 Attorney-General's Department, *Submission 27*, p. 29.

72 Data Retention Bill, *Explanatory Memorandum*, p. 45.

73 Data Retention Bill, *Explanatory Memorandum*, p. 45.

3.82 The Government's proposed data set, in combination with subsection 187A(7) of the Bill, ensures that service providers are required to keep location records at, and only at:

- the time at which a device connects to and disconnects from the network, and
- the beginning and end of an actual communication, such as a phone call or SMS, or a communications session, such as an internet access session which may last between several hours and many months, depending on the underlying technology.[74]

3.83 As the Explanatory Memorandum notes:

> Subsection 187A(7) provides that for the purposes of certain information or documents required to be kept under paragraphs 187A(2)(b), (c), (d) and (f), two or more communications that together constitute a single communications session are taken to be a single communication.
>
> The purpose of subsection 187A(7) is to ensure that providers are not required to record the source, destination, time, date and duration of a communication or the location of a device throughout a communications session.
>
> For example, a smartphone connected to a mobile data network may have multiple applications running in the background, each of which may routinely communicate with remote servers, such as to seek and obtain updates. As such, the smartphone may send and receive a near-continuous stream of communications. However, these communications may together constitute a single communications session. Absent this provision, providers could, for example, be required to record the location of the device on a near-continuous basis. The effect of the provision is that providers will only be required to record prescribed location information for the overall communication rather than its constituent components.[75]

3.84 In evidence, Telstra confirmed that it currently retains call-related cell tower records—the type of location data that the Government proposes to prescribe for the purposes of the data retention scheme—for at least six years.[76] The Committee also received confidential submissions from

74 Proposed data set, item 6; Data Retention Bill, s. 187A(7).

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

76 Mr Mike Burgess, Chief Information Security Officer and Mrs Kate Hughes, Chief Risk Officer, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 18.

Vodafone and Optus setting out their current retention practices for location records.

3.85 Blueprint for Free Speech questioned whether service providers would only be required to retain 'limited records such as which, how and when a device connects to a cell phone tower', or whether providers would actually be required to retain highly-specific location data, such as GPS information:

> [M]ost people have GPS enabled smartphones which, when used with other services on a smart phone *(sic)* that connect to the internet or use data is some manner, make the location of the device (and therefore the user) known. So, it may be the case that when tracking the location of a call that the most accurate location is to the nearest cell tower, however all communication that used data (which is paired with the GPS functions on a mobile phone) will enable pinpoint accuracy of the user's location. [77]

3.86 The New South Wales Police Force provided the Committee with evidence about the granularity of the type of location data that would be accessed by police:

> With cell site location that we would normally get with metadata, we would talk about an area, for example if I am in Canberra I might be in Deakin or I might be somewhere—it does not specify. There is not the amount of specificity to say that I am in a particular place. We are talking about more gross data.[78]

3.87 Ms Hartland explained to the Committee how the location records covered by the proposed data retention obligations fit within the broader framework of ASIO's surveillance powers:

> The bill will not require providers to retain all the location information—the regular connections mobiles make to cell towers, for example. What the bill does require is for providers to retain the location information when communications occur. For example, what cell tower did the mobile connect to when they made a call? This does not amount to tracking as some people have suggested. If ASIO has a requirement to monitor individuals, other capabilities can be deployed—for example, tracking devices under warrant.
>
> The cell tower locations that will be required to be retained by the data retention bill will only ever provide agencies with the vicinity

77 Blueprint for Free Speech, *Submission 54*, p. 6.

78 Assistant Commissioner Malcolm Lanyon, Commander, Special Services Group, New South Wales Police Force, *Committee Hansard,* Canberra, 30 January 2015, p. 48.

> of the mobile phone. This information provides useful intelligence, including when correlated with other intelligence over time, and there are some operational examples of that in our classified submission.[79]

Should service providers be required to retain more detailed location records?

3.88 Proposed new section 187A requires service providers to retain location records relating to distinct communications events. However it does not require service providers to keep more frequent records about the location of a device based on its persistent, background connection to the network, known as Home and Visitor Location Records (HLR and VLR, respectively). Victoria Police argued against this exclusion:

> There is one area Victoria Police would like to put on the record. It is in our written submission—that is, VLR, visitor location register data. The intent of the bill, as I understand it, is explicitly around data that arises out of communications, which VLR does not. VLR is effectively the handshake, as it is anecdotally referred to, between the phone and the tower as the phone passes the tower, even when there is no actual communication occurring. That has what I would suggest are fairly obvious benefits for law enforcement and within the Victorian jurisdiction we have had one recent very high profile homicide which caused high degrees of community concern and in which VLR was instrumental in resolving, certainly in the time frames that we were able to do. Victoria Police would like it to be put on the record that our view is that VLR should also be part of the datasets that are considered in this legislation.[80]

3.89 The NSW Police Force supported this recommendation.[81]

3.90 The Committee also received a classified briefing relating to the utility of HLR and VLR data to investigations.

Committee comment

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

---

79 Ms Hartland, *Committee Hansard,* Canberra, 17 December 2014, p. 5.

80 Inspector Gavan Segrave, Intelligence and Covert Support Command, Victoria Police, *Committee Hansard,* Canberra, 30 January 2015, p. 63.

81 Detective Superintendent Arthur Kopsias, *Committee Hansard,* Canberra, 30 January 2015, p. 63.

3.92 The Committee acknowledges that location records are a sensitive category of telecommunications data included in the proposed data set. The Bill and proposed data set significantly curtail the detail and frequency of the location records that service providers would be required to retain.

3.93 However, information showing a person's approximate location at the time they made a communication can be vital to demonstrate associations and relationships between suspects, and to exclude people from suspicion. The Committee accepts that the retention of this data is necessary and proportionate for national security and law enforcement investigations.

Types of data excluded from the data set

3.94 Proposed new subsection 187(4) of the Bill excludes five types of telecommunications data from the scope of data retention obligations:

- information that is the contents or substance of a communication,
- web-browsing histories,
- information relating to communications carried by third-party over-the-top service providers,
- information that service providers are required to destroy pursuant to determinations made under section 99 of the Telecommunications Act, and
- detailed location records.

3.95 The Committee did not receive any submissions expressing concern about the proposed exclusion of information that service providers are required to destroy under the Telecommunications Act. The Committee has addressed the issue of the retention of location records above. The remaining exclusions are discussed in the following pages.

Contents or substance of a communication

3.96 Paragraph 187A(4)(a) of the Bill provides that service providers are not required to retain information that is the content or substance of a communication. This provision gives effect to this Committee's 2013 recommendation that 'any mandatory data retention regime should apply only to meta-data and exclude content'.[82] The Committee also notes that section 172 of the TIA Act provides that data authorisations made under Chapter 4 of the TIA Act cannot authorise the disclosure of the content or substance of a communication.

82 PJCIS, *Report of the inquiry into potential reforms of Australia's national security legislation*, Canberra, May 2013, p. 192.

Defining 'contents or substance' of a communication

3.97 The Parliamentary Joint Committee on Human Rights (PJCHR) noted that 'what constitutes the "content" of a communication (and would therefore be excluded from collection) is undefined in the bill',[83] and has expressed concern that this 'could see data retained that does include aspects of content'.[84]

3.98 The Senate Standing Committee for the Scrutiny of Bills also noted the absence of a definition of 'content' and noted that 'as long as the bill does not contain a clear definition of 'content' there is a real risk that personal rights and liberties will be unduly dependent on insufficiently defined administrative powers.'[85]

3.99 The Australian Human Rights Commission and the Law Council of Australia supported these recommendations.[86]

3.100 In its submission, the Attorney-General's Department acknowledged the PJCHR's recommendation and endorsed the importance of ensuring that data retention obligations do not inadvertently apply to the content of communications. However, the Department cautioned that:

> the PJCHR's recommendation would actually have the contrary effect as an exhaustive definition would not keep pace with technological change, leading to an increasingly wide range of information that may not be excluded from data retention obligations. The technologically-neutral approach taken to defining the content or substance of a communication under the TIA Act is consistent with the approach taken by the *Privacy Act 1988* and Part 13 of the Telecommunications Act, and is consistent with the 2008 views of the [Australian Law Reform Commission] about the desirability of technological neutrality in this field.[87]

3.101 As part of its 2008 report, *For your information: Australian privacy law and practice*, the Australian Law Reform Commission (ALRC) considered the question of whether 'telecommunications data' should be defined, and recommended against an exhaustive definition:

> The ALRC does not recommend amending the Telecommunications (Interception and Access) Act to define

83 Parliamentary Joint Committee on Human Rights (PJCHR), *Fifteenth Report of the 44th Parliament*, p. 14.

84 PJCHR, *Fifteenth Report of the 44th Parliament*, p. 14.

85 Senate Standing Committee for the Scrutiny of Bills, *First Report of 2015*, p. 122.

86 Australian Human Rights Commission, *Submission 42*, pp. 7-8; Law Council of Australia, *Submission 126*, p. 12.

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

> 'telecommunications data'. The exclusion of a definition enables the legislation to remain technology neutral so that it can be applied to new developments in technology without the need for amendment.[88]

3.102 The Department elaborated on this issue in its supplementary submission, arguing that:

> The challenges of maintaining technological neutrality in the context of the meaning of telecommunications data are equally applicable to defining content. The broad meaning of 'content or substance' of a communication in the TIA Act is capable of being interpreted in light of rapid changes in communications technology in a way that an exhaustive, static definition would not.
>
> Any new types of information that emerge as a result of rapid technological change would fall outside the defined list. They would then be excluded from the meaning of content, and the protections that apply to content.
>
> The TIA Act includes provisions which, when read in conjunction with a broad definition of content, create a strong incentive for the telecommunications industry and agencies to take a robust approach to protecting and accessing the content of communications. In particular:
>
> - apart from limited exceptions, it is a criminal offence for a service provider to disclose the content or substance of a communication without lawful authority
> - it is a criminal offence for officials of law enforcement and national security agencies to use or disclose unlawfully accessed stored communications except in strictly limited circumstances
> - there is no discretion for a court to admit unlawfully accessed stored communications, which includes information that has been wrongfully retained as data, and
> - any person who believes that the content or substance of their communications has been unlawfully accessed under a data authorisation can challenge that access and, if successful, seek remedies under Part 3-7 of the TIA Act.[89]

3.103 From a technical perspective, Ms Brenda Aynsley, President of the Australian Computer Society, advised the Committee that, 'I have been

88 Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice*, Report No. 108 (2008), p. 2485.

89 Attorney-General's Department, *Submission 27.2*, pp. 6-7.

party to the discussions on defining content since the seventies. I do not have a problem with the accepted definition in use today'.[90]

Can content be reliably separated from telecommunications data?

3.104 A number of submissions questioned whether service providers would, from a technical perspective, be able to appropriately separate content from telecommunications data.[91]

3.105 Mr Peter Froelich of Telstra, appearing in his capacity as a member representative of Communications Alliance and the AMTA, provided detailed evidence about the technical challenges associated with separating the content or substance of a communication from the telecommunications data associated with its transmission, for different types of communications. In summary, for some types of telecommunications data, such as email, service providers would be required to conduct some 'post processing' to separate the telecommunications data to be retained from the content that is not to be retained. He noted that:

> the technology is not overly challenging from an engineering function… but the concepts of unpicking it and putting it aside are certainly a little bit more challenging than perhaps meeting the standard TIA Act interception obligations.[92]

3.106 For other types of communications, such as SMS messages, Mr Froelich indicated that separating the content from the telecommunications data would not be complex:

> I think text messages are not particularly onerous in that there is a to and a from field and a billing function for those. We discreetly bill for those and the actual text line does not exist in the billing function. That one I do not think is particularly onerous for us.[93]

Web-browsing histories

3.107 Paragraph 187A(4)(b) of the Bill provides that service providers are not required to keep, or cause to be kept:

> information that:

---

90 Ms Brenda Aynsley, President, Australian Computer Society, *Committee Hansard,* Canberra, 29 January 2015, p. 84.

91 See, for example, Mr David Vaile and Mr Paolo Remati, *Submission 194*, pp. 7-8; Law Council of Australia, *Submission 126*, p. 13.

92 Mr Peter Froelich, General Manager, Special Networks Engineering, Telstra, *Committee Hansard,* Canberra, 17 December 2014, p. 41.

93 Mr Froelich, *Committee Hansard,* Canberra, 17 December 2014, p. 41.

(i) states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider; and

(ii) was obtained by the service provider only as a result of providing the service.

3.108 A note in the Bill states that 'this paragraph puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history', giving effect to this Committee's 2013 recommendation that 'internet browsing data should be explicitly excluded'.[94]

3.109 However, the language of the Bill establishes a broader exemption that covers more than merely 'web-browsing' data. As the Explanatory Memorandum makes clear:

> This provision will go further than the PJCIS Report recommended by ensuring that service providers are not required to keep records of the uniform resource locators (URLs), internet protocol (IP) addresses, port numbers and other internet identifiers with which a person has communicated via an internet access service provided by the service provider.[95]

3.110 The IWG report provides greater detail on this exclusion:

> The proposed data set must be read in the context of the Bill, which limits the scope and application of the data retention obligations and through that the extent to which data elements identified in the data set must be retained.
>
> …
>
> Subparagraph 187A(4)(b)(i) ensures that internet access service providers are not required to keep destination information associated with web browsing history *and other communication protocols* for those services.
>
> The data retention obligations relating to an internet access communication session are limited to the relevant provider retaining the time, date and location of a subscriber when the service was accessed, and the time, date and location of that subscriber when the service was disconnected, as well as all internet protocol (IP) addresses and, where applicable, port

94 PJCIS, *Report of the inquiry into potential reforms of Australia's national security legislation*, Canberra, May 2013, p. 192.

95 Data Retention Bill, *Explanatory Memorandum*, p. 44.

> numbers allocated to the subscriber during the session (and the associated dates and times).[96]

3.111 Subsection 187A(7) of the Bill is also relevant when considering the data retention obligations applicable to internet access services. As noted above in the context of location information, this provision provides that two or more communications that together constitute a single communications session are taken to be a single communication.

3.112 The Explanatory Memorandum states:

> The purpose of subsection 187A(7) is to ensure that providers are not required to record the source, destination, time, date and duration of a communication or the location of a device throughout a communications session.[97]

3.113 The Explanatory Memorandum then goes on to give a detailed example of how data retention obligations do, and do not, apply to smartphones running multiple background applications. The IWG report further explains that the effect of s 187A(7) is that 'data retention obligations do not require packet-level retention'.[98]

3.114 The Attorney-General's Department's submission explains the underlying purpose of the exclusion:

> This exception is intended to ensure that providers of internet access services are not required to engage in session logging, which may otherwise fall within the scope of the destination of a communication.
>
> However, the general obligation to retain destination information will continue to apply to other services, such as email, messaging or VoIP services that are analogous to 'traditional' communications services. Providers of those and other services will be required to retain the destination identifiers for communications sent using their services. [99]

Impact on national security and law enforcement investigations

3.115 Victoria Police, advised the Committee that the exclusion of web-browsing histories represents a significant, but justified exclusion from the scope of the proposed data set:

> From a Victoria Police point of view, if we were to look at this solely from a law enforcement perspective without considering all

96 IWG, *Report 1 of the Data Retention Implementation Working Group,* December 2014, pp. 3-4.

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

98 IWG, *Report 1 of the Data Retention Implementation Working Group,* December 2014, p. 4.

99 Attorney-General's Department, *Submission 27*, p. 28.

> the surrounding issues which obviously this committee and the community need to consider, the answer would probably be, 'Yes, we need that. That is fantastic.' But, like all other stakeholders in these proceedings, we need to bring a degree of pragmatism to these discussions. … We understand the need to try to find a balance. I think the view of the Victoria Police would be that, although that is something that would be very nice to have and very beneficial, it raises a level of concern in the community around the bill and the proposed regime generally, we are prepared so say we can live with the proposed arrangements and do the best we can under that regime.[100]

3.116 The New South Wales Police Force and South Australia Police expressed similar views.[101]

Concerns about the drafting of this exclusion

3.117 Optus noted that, while it understood the policy intent of the Bill is to exclude any requirement for the analysis or retention of internet packet address details, '[t]he draft legislation may not sufficiently exclude this for incoming communications to a customer.'[102] Optus confirmed that the current draft data set does not require the retention of web-browsing information, but noted that:

> It appears open for the Regulations to require collection of the origin IP address by the service provider supplying the internet access service to the destination customer. If this occurred, it could enable the browsing history of the customer to be reconstructed by examination of where web browsing packets came from.[103]

3.118 Professor George Williams of the University of New South Wales gave similar evidence.[104]

3.119 Optus recommended that section 187A(4)(b) of the Bill could be amended to place beyond doubt that the regulations could not be used to require the retention of web-browsing history.[105]

---

100 Inspector Segrave, *Committee Hansard,* Canberra, 30 January 2015, pp. 55-56.

101 Assistant Commissioners Malcolm Lanyon, Commander, Special Services Group, New South Wales Police Force and Paul Dickson, Crime Service, South Australia Police, *Committee Hansard,* Canberra, 30 January 2015, pp. 55-56.

102 Optus, *Submission 86*, p. 8.

103 Optus, *Submission 86*, p. 8.

104 Professor Williams, *Committee Hansard,* Canberra, 30 January 2015, p. 4.

105 Optus, *Submission 86*, p. 8.

3.120 The Attorney-General's Department disagreed, arguing that Optus' interpretation of the provision is 'plainly not supported by the language of the Bill':

> This reading is inconsistent with the wording of sub clause 187A(4). The exception excludes information that:
>
> - a provider has only because of its provision of an internet access service, and
> - states addresses to which information was sent on the internet.
>
> As such, any information that records a person's browsing history meets this test and is therefore excluded regardless of whether it is incoming (received) or outgoing (sent) – an incoming packet still states the address to which a communication was sent, because it responds to an instruction (the outgoing IP packet).[106]

3.121 The Department also noted that the amendments to the provision recommended by Optus could result in unintended consequences:

> Moreover, the Department is concerned that Optus' particular proposal could be read as excluding both web browsing history and the identifiers (IP addresses) that a provider assigns to its own customers. The Bill's clear intent is that providers be required to retain the IP address assigned to their own customers under the data retention regime. The amendment proposed by Optus would be inconsistent with that objective.[107]

Definition of the term 'session'

3.122 The Explanatory Memorandum provides some guidance about how the term 'session' is to be interpreted, indicating that it is intended to apply flexibly to different networks and services, based on their unique configurations:

> Whether a series of communications constitutes a single communications session is a question of technical fact and will depend upon the objective operation of the provider's network or service. This question should not be determined from the user's perspective, as the provider subject to data retention obligations will generally be unable to assess a user's intentions in this regard, and in many cases, users are unlikely to be aware of when their device is communicating, such as when applications installed on a smartphone or computer are automatically seeking and receiving updates.[108]

106 Attorney-General's Department, *Submission 27.2*, pp. 12-13.

107 Attorney-General's Department, *Submission 27.2*, p. 13.

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

3.123 However, Optus' submission also noted some potential uncertainty about the intended meaning of this term,[109] and in evidence noted that:

> It is an easy problem to identify but it is something that will require a lot of discussion around what a session actually is.[110]

3.124 The Data Retention Implementation Working Group's report also recommends that Government provide additional explanatory material for the term 'session', which, as noted above, is used within proposed new subsection 187A(7) of the Bill to limit the volume and type of information that service providers are required to retain.[111]

3.125 In its supplementary submission, however, the Attorney-General's Department disagreed that the current approach is ambiguous, explaining that:

> In relation to the term 'session', paragraph 187A(7) of the Bill provides that two or more communications that together constitute a single communications session are taken to be a single communication. With internet access sessions, this means that service providers will only be required to keep location records at the start and end of a session, which can last from a few minutes to several days or even weeks. For phone calls, each call will be a separate communication that will have separate data retention requirements.
>
> In regards to location information, the location records will be limited to the location of a device at the start and end of a communication (such as a phone call or Short Message Service (SMS) message). For services provided to a fixed location, such as an ADSL service, this requirement can be met through the retention of the subscriber's service address.[112]

Should service providers be precluded from retaining web-browsing information?

3.126 The Australian Privacy Foundation argued that proposed new paragraph 187A(4)(b) does not go far enough, as it does not prohibit the retention of web-browsing information:

> The problem with this is that it simply says that this information does not have to be retained, but it does not prevent the retention of this information, and it does not prevent access to this information under Chapter 4 of the TIA Act. Now, we believe that

109 Optus, *Submission 86*, p. 9.

110 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 25.

111 IWG, *Report 1 of the Data Retention Implementation Working Group*, December 2014, p. 8.

112 Attorney-General's Department, *Submission 27.2*, p. 12.

> to say that the bill is privacy protective, because there is no obligation to retain this data, does not deal with the fact that the data may well be retained.[113]

3.127 However, in recent evidence to the Senate Legal and Constitutional Affairs References Committee in September 2014, Mr Matthew Lobb, General Manager Industry Strategy and Public Policy at Vodafone Hutchison Australia, confirmed that Vodafone, and likely other major service providers, was currently developing and implementing the capability to collect and retain at least some web-browsing history for commercial purposes, unrelated to the proposed data retention scheme:

> **CHAIR:** I want to draw three distinctions here. You can tell us where Vodafone sits now, and where you think your business is heading. One distinction that you could capture is that this customer downloaded X gigabytes of data in a period of time and that that customer was responsible for that much data transfer. That is very minimal.
>
> The second or middle tier is where you would be able to tell the host IP but not necessarily pages within a particular address space. The third tier is being able to track exactly what kind of content, click by click. Where is Vodafone now, and where is it heading?
>
> **Mr Lobb:** We are at the cusp of the second capability. We have been developing that capability. Because it is such a large amount of information that would need to be stored and accessed it is a challenge, but that is something that we have been developing.
>
> **CHAIR:** We are hearing from Telstra a little bit later in the day. I am presuming that this is not something that Vodafone is embarking upon, where you are out on some kind of limb.
>
> **Mr Lobb:** No.
>
> **CHAIR:** This is where the industry is heading?
>
> **Mr Lobb:** That is right. I am not sure where other companies are at, but I would expect that the capability is something that is evolving across the industry.[114]

Data about communications passing 'over the top' of internet access services

3.128 The Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG) expressed concern that service providers may be

113 Dr David Lindsay, Vice-Chair, Australian Privacy Foundation, *Committee Hansard,* Canberra, 30 January 2015, p. 78.

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

required to use deep packet inspection to extract telecommunications data about third-party over-the-top services passing over their network:

> It is unclear… the extent to which the proposed data retention regime is intended to apply to information about communications using 'over the top' (OTT) services. For example, it appears from the categories of information that may be required to be retained that there is scope for the Minister to direct ISPs to collect data about all third party OTT services carried on their networks.[115]

3.129 However, proposed new paragraph 187A(4)(c) provides that service providers are not required to keep:

> information to the extent that it relates to a communication carried by means of another relevant service operated:
>
> (i) by another service provider; and
>
> (ii) using the relevant service;
>
> or a document to the extent that the document contains such information.

3.130 The Explanatory Memorandum states:

> The purpose of this provision is to ensure that the provider of an underlying service, such as an internet access service, is not required to keep information about communications that are passing 'over the top' of the underlying service and that are being carried by means of another relevant service, such as VoIP service, operated by another provider.[116]

3.131 Similarly, the IWG report states that:

> The obligation to retain data about a service only applies to the operator of that service. Providers are not required to retain data about the services offered by other providers. … Put another way, the data retention obligations do not require a service provider to inspect another service provider's packets to determine what service may be running over the top.[117]

3.132 The Department, in its submission, further explained that:

> proposed paragraph 187A(4)(c) makes clear that service providers are only required to keep records about the services they themselves provide and operate. They are not required to keep records about communications sent or received using third-party

115 Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG), *Submission 34*, p. 7.

116 Data Retention Bill, *Explanatory Memorandum*, p. 45.

117 IWG, *Report 1 of the Data Retention Implementation Working Group,* December 2014, p. 3.

> communications services running 'over-the-top' of their network or service. This means that an internet access service provider, though not required to retain web-browsing information, would have to retain destination information for webmail services, for example, but only if it provided that webmail service itself. That particular provider would not be required to retain destination information for services its customer used, but it did not provide.[118]

Committee comment

3.133 The Committee accepts the evidence provided by industry representatives that content can be reliably separated from data for the purpose of data retention. The Committee notes that, currently, service providers are required by law to separate content from data when complying with historic and prospective data authorisations made under Chapter 4 of the TIA Act. The Committee also notes the offence provisions under both Part 13 of the *Telecommunications Act 1997,* and Chapters 2 and 3 of the TIA Act for the unauthorised access to or disclosure of the content of a communication.

3.134 The Committee notes that the Bill does not in any way provide for agencies to access any content or substance of a communication, except under a warrant.

3.135 The Committee accepts the evidence of the Attorney-General's Department that the Bill, as drafted, is intended to exclude any obligation for providers of internet access services to retain web-browsing history, or any other destination information relating to third-party protocols passing over their service, and that this exclusion applies equally to incoming and outgoing traffic. However, ensuring that web-browsing histories are not required to be retained is important to ensuring the proportionality of any data retention regime. This issue should be further clarified in the Explanatory Memorandum.

118 Attorney-General's Department, *Submission 27*, p. 28.

Recommendation 7

The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that service providers are not required to keep web-browsing histories or other destination information, for either incoming or outgoing traffic.

3.136 The Committee acknowledges that in some instances service providers may have legitimate commercial reasons to choose to retain web-browsing history, including allowing service providers to provide cheaper internet access services that are partially funded by advertising revenue based on a person's web-browsing history. The collection of web-browsing information in that context would continue to be regulated by the Privacy Act and Part 13 of the Telecommunications Act.

3.137 In regards to the definition of 'sessions', the Committee notes that individual networks and services manage 'sessions' in very different ways. The approach proposed in subsection 187A(7) is intended to allow service providers to adopt retention practices consistent with their existing session-management practices. However, the Committee is concerned that the proposed approach may be overly broad and may contribute to industry uncertainty.

3.138 The Committee sees value in the Explanatory Memorandum clarifying how 'sessions' are to be defined.

Recommendation 8

The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to provide greater clarity in defining 'sessions' in proposed new subsection 187A(7) of the Bill.

3.139 Finally, in regards to the proposed data set, the Committee accepts evidence that the Bill does not require service providers to keep records about communications sent or received using third-party communications services running 'over-the-top' of their network or service. Service providers are only required to keep records about the services they themselves provide and operate.