5

Application to particular services, and implementation, cost and funding arrangements

Application to certain service providers

5.1 Proposed new subsection 187A(3) of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) sets out which services will be subject to data retention obligations, subject to the exclusions set out in proposed new section 187B. Obligations will apply to communications services provided by carriers, carriage service providers, internet service providers or prescribed service providers, provided that they have communications-related infrastructure in Australia.

5.2 However, obligations will not apply in relation to services provided by carriage service providers to:

- a person's 'immediate circle', within the meaning of section 23 of the Telecommunications Act; or
- only to places that are all in the 'same area', within the meaning of section 36 of that Act.

Application to 'offshore' and 'over-the-top' providers

5.3 Proposed new subsection 187A(3) provides that data retention obligations will apply to a service if:

(a) it is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both; and

(b) it is a service:

(i) operated by a carrier; or

(ii) operated by an internet service provider (within the meaning of Schedule 5 to the *Broadcasting Services Act 1992*); or

(iii) of a kind prescribed by the regulations; and

(c) the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services;

but [do] not apply to a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*).

Application to 'offshore' providers

5.4 The Explanatory Memorandum confirms that data retention obligations:

> will apply to a service if the person operating the service owns or operates infrastructure in Australia relating to any of its services, irrespective of whether the person owns or operates infrastructure in Australia relating to the particular service in question.[1]

5.5 Communications Alliance and the Australian Mobile Telecommunications Association submitted that the exclusion of offshore providers may place Australian service providers at a competitive disadvantage.[2]

5.6 The Internet Society of Australia noted that the exclusion of offshore providers will:

> [R]esult in significant 'gaps' in the data retained… and is therefore likely to undermine the efficacy of this legislation's stated purpose of providing the means to identify activities that represent a potential security risk.[3]

5.7 In its submission, the Attorney-General's Department acknowledged that data retention obligations would not apply to a number of service providers that have a significant presence in the Australian market, but that do not have infrastructure in this country. However, the Department noted that the potential impact of this 'gap' on agencies' investigative capabilities is mitigated by three factors:

---

1 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 43.

2 Communications Alliance and the Australian Mobile Telecommunications Association (AMTA), *Submission 1*, p. 17.

3 Internet Society of Australia, *Submission 122*, p. 9.

> Providers offering services from infrastructure based offshore may be subject to separate local legislation relating to their retention of data. Offshore based companies are able to assist Australian law enforcement, to the extent that the laws of their home countries permit them to do so. Additionally, as a party to the Council of Europe Cybercrime Convention, Australian law enforcement agencies are able to obtain expedited assistance from 43 countries to obtain telecommunications data held in those countries that is relevant to Australian investigations.[4]

5.8 Commissioner Andrew Colvin of the Australian Federal Police (AFP) has subsequently addressed the concerns expressed by some about the exclusion of offshore providers, and explained the role that data retention will play in reducing what is an existing, rather than a new issue for law enforcement and national security agencies:

> people need to leave a digital fingerprint, effectively, so even if you are using a Gmail account for instance, you're using an over the top provider that is an application provided by an overseas company that may be out of the reach of legislation, you still need to make a footprint somewhere where you connect to the internet. This is about that basic identifier of who it was that connected to the internet at that time.[5]

5.9 At a public hearing, the Internet Society acknowledged that:

> My impression is that it will be difficult for this government to actually regulate some body that is based overseas. However, you can incorporate regulation for an entity that is based in Australia.[6]

5.10 The Department also noted that attempting to impose extra-territorial data retention obligations would:

> give rise to significant jurisdictional and conflict-of-laws issues including where, for example:
>
> - providers are already subject to data retention laws in their own jurisdiction, leading to the provider being subject to inconsistent Australian and foreign obligations, and

4 Attorney-General's Department, *Submission 27.2*, p. 18.

5 Commissioner Andrew Colvin APM OAM, Australian Federal Police (AFP), *Transcript of the Prime Minister, the Hon. Tony Abbott MP, Joint Press Conference with the Hon. Michael Keenan MP, Minister for Justice and Mr Andrew Colvin APM OAM, Commissioner of the Australian Federal Police, AFP Headquarters, Melbourne*, 5 February 2015, p. 5.

6 Ms Holly Raiche, Chair of the Policy Committee, Internet Society of Australia, *Committee Hansard,* Canberra, 29 January 2015, p. 88.

- providers are subject to data minimisation obligations in their own jurisdiction, leading to the provider being subject to contradictory obligations to retain and delete telecommunications data.[7]

Definition of 'infrastructure'

5.11 The Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG) recommended that, to avoid data retention obligations being expanded to cover offshore providers of 'over-the-top' services beyond what Parliament intended, the term 'infrastructure in Australia' should be defined to mean 'physical hardware located within Australia that is critical to the deployment of communication carriage services offered to people in Australia.'[8] The Law Council of Australia,[9] Communications Alliance and the Australian Mobile Telecommunications Association also noted that the definition of 'infrastructure' is uncertain.[10]

5.12 The Attorney-General's Department confirmed, in its submission, that data retention obligations are intended to 'apply to providers that own or operate infrastructure, such as servers, routers and/or cables, within Australia that enables one or more of their communications services', and that the purpose of this requirement is to 'ensure that service providers cannot avoid their data retention obligations by off-shoring part of their infrastructure or outsourcing the provision of some services to overseas entities'.

Application to providers of 'over-the-top' services

5.13 The Australian Information Industry Association advised the Committee that a number of its members were uncertain about whether 'over-the-top' services, such as web-based email, VoIP or cloud service would be subject to data retention obligations.[11]

5.14 The Australian Privacy Commissioner also considered that the Bill's application to over-the-top services was unclear, raising potential challenges for his office as a regulator:

> We are just not clear whether they do fall in necessarily to the services that it is proposed be covered by the Bill. I think from a regulator's point of view, that is possibly a bit of a challenge

7 Attorney-General's Department, *Submission 27*, p. 24.

8 Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG), *Submission 34*, p. 8.

9 Law Council of Australia, *Submission 126*, p. 9.

10 Communications Alliance and the AMTA, *Submission 6*, p. 10.

11 Ms Suzanne Campbell, Chief Executive Officer, Australian Information Industry Association, *Committee Hansard*, Canberra, 29 January 2015, p. 31.

> because, if we are not clear about whether those services do fall in or not, it is hard to be sure whom or what services we are supposed to be regulating—if we are to take some of our more proactive regulatory roles that I have described or if in fact we are going to be, say, pursuing individual complaints about a matter.[12]

5.15 However, in evidence to the Senate Legal and Constitutional Affairs References Committee's current inquiry, Communications Alliance explained that:

> Our understanding is that, if it is an over-the-top application that is not provided by the service provider, the service provider is not required to retain those data. Whether or not those data have to be retained by anybody depends on whether they are an operator providing a communications service in Australia.[13]

Committee comment

5.16 The Committee supports the intended operation of proposed new paragraph 187A(3)(c). It is appropriate that data retention obligations apply in respect of services provided to Australian customers, even where infrastructure used by the service provider to deliver that service is not located in Australia.

5.17 The Committee also accepts that limiting the application of data retention obligations to companies that are within Australia's territorial jurisdiction is an appropriate measure, as it avoids subjecting multinational companies to competing and potentially irreconcilable legal obligations. The primary effect of this limitation is that data retention obligations will apply to 'over-the-top' services provided by service providers with infrastructure in Australia, but will not apply to 'over-the-top' services provided by wholly-offshore companies.

5.18 The Committee acknowledges that the exclusion of over-the-top services provided by wholly-offshore companies may have capability implications, to the extent that those companies do not retain relevant telecommunications data about their customers. However, the Committee notes the evidence it has received that data retention laws have been implemented or are under active consideration in most Western nations, and that Australian agencies are able to obtain relatively rapid assistance from law enforcement counterparts in these countries when seeking access

12 Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard,* Canberra, 29 January 2015, p. 53.

13 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard,* Canberra, 2 February 2015, p. 12.

to telecommunications data. Additionally, the Committee considers that any benefits to agencies' investigative capabilities or to competitive neutrality that might flow from extending data retention obligations to offshore providers must be weighed against the additional complexity that would result, particularly in light of the significant challenges in the enforcement of extraterritorial laws. The Committee notes that the United Kingdom Government has gone as far as to appoint a Special Envoy to attempt to resolve this complexity.[14]

5.19 The Committee notes that section 187A(3)(c) applies only to providers that have, in Australia, 'infrastructure that enables the provision of any of its *relevant services*' (emphasis added). The term 'relevant service' is defined in subsection 187A(1), and relates only to services that, among other things, are services 'for carrying communications, or for enabling communications to be carried'. Accordingly, the Bill as drafted applies only to companies that have, in Australia, infrastructure that enables the provision of communications services. It would not appear to apply to a broader class of infrastructure, such as buildings or marketing databases.

5.20 Nevertheless, the Committee notes evidence from industry that there remains some uncertainty about the intended meaning of the term 'infrastructure' as used in paragraph 187A(3)(c) of the Bill and considers this matter should be addressed in order to put the matter beyond doubt. This clarification would support the Bill's intent to exclude overseas providers of 'over-the-top' services from the proposed data retention obligations.

Recommendation 11

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to define the term 'infrastructure' in greater detail, for the purposes of paragraph 187A(3)(c).

Exclusion of services provided to an 'immediate circle' or 'single area'

5.21 Subsection 187B(1) of the Bill provides that data retention obligations do not apply to a service provider in relation to relevant services that are

14 Government of the United Kingdom, Cabinet Office and Home Office, 'Sir Nigel Sheinwald appointed Special Envoy on intelligence and law enforcement data sharing', *Press Release*, 19 September 2014, <https://www.gov.uk/government/news/sir-nigel-sheinwald-appointed-special-envoy-on-intelligence-and-law-enforcement-data-sharing> viewed 26 February 2015.

provider only to a person's 'immediate circle' (such as corporate or university intranets) or only within places that are in the 'same area' (such as a Wi-Fi hotspot in a café or library).

5.22 Several submissions expressed concern that the exclusion of data retention obligations from these services would undermine the effectiveness of the regime.[15] For example, the Internet Society of Australia argued that:

> It appears that anybody seeking to evade the provisions of the Bill could simply become a student somewhere and communicate within that educational institution without detection.[16]

5.23 The Chair of the Policy Committee for the Internet Society of Australia explained some of the complexity of attempting to regulate some of these services:

> In that situation [immediate circles], they are provided generally by a service provider under contract with a particular firm. So those are in one sense commercial agreements that you do not unpick … So in some cases we are dealing with definitions in the Telecommunications Act that mean some areas are not covered. If you read the Attorney-General's [Department's] submission, they are relaxed about some of that. They understand the difficulty in covering some of this.[17]

5.24 The Attorney-General's Department explained that telecommunications services provided within a single area had been excluded from the scope of the scheme based on an assessment that the utility of data relating to those services would be outweighed by the regulatory burden:

> That particular section is excluded because of an assessment that, while that data is useful, the compliance burden and impost upon the providers of those same-area services is a significant one, and the intention of the regime is to provide a targeted response around a range of data that is useful. Naturally, agencies have a range of tools at their disposal to access communications and identify the behaviours and communications of suspects, but there is a particular exclusion there which relates back to a particular compliance burden for the providers of those services.[18]

---

15 See, for example, Mr Brian Ridgway, *Submission No, 20*, p. 5.

16 Internet Society of Australia, *Submission 122*, p. 8.

17 Ms Raiche, *Committee Hansard,* Canberra, 29 January 2015, p. 86.

18 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 7.

5.25 Universities Australia, the peak body representing 39 Australian universities, welcomed the Government's decision to exclude universities from data retention obligations under the Bill, noting that there would be a 'significant administrative burden and cost for universities if they were required to collect and retain data that is currently not required for their internal purposes'.[19] The submission also expressed concern at the power of the Communications Access Co-ordinator to declare, pursuant to proposed new subsection 187B(2), that data retention obligations would apply to a particular service provided to an immediate circle or single area, such as a publicly-accessible Wi-Fi network operated by a university across a campus.[20] The University of Sydney and the Society of University Lawyers made submissions in similar terms.[21]

5.26 The Attorney-General's Department also confirmed that a range of data would continue to be retained in relation to such services, ensuring that critical lead information remains available for law enforcement and national security investigations:

> Without going into too great a detail about the operational practices of agencies, data may be accessible at a different point in the process. The fact that a particular coffee shop is not required to retain data in relation to who it provides its free Wi-Fi to does not preclude data from being accessed at a different point in the process, so the excludes are an illustration or a representation of the proportionality of the data retention measure in that it targets appropriate points in the process and provides data for key telecommunications services.[22]

5.27 The AFP expanded on the operational implications of this exclusion for law enforcement agencies:

> If I may, how it would work in an operation sense is that, if an internet café or a coffee shop has a service provided by Telstra, we would know that that internet café service accessed their system from between the internet café and Telstra at a given point in time, but we would not know which device within that café accessed their internal Wi-Fi router or modem to do it. It is similar to if it is a home; out of the six or seven or eight phones or devices inside, you do not know which one has accessed it. However, it is a gap in that sense, but it does not mean that we do not have other technologies or other abilities to exploit that situation. It is just

19 Universities Australia, *Submission 84*, p. 1.

20 Universities Australia, *Submission 84*, pp. 1-2.

21 University of Sydney, *Submission 93*, p. 1; Society of University Lawyers, *Submission 98*, p 1.

22 Ms Harmer, *Committee Hansard,* Canberra, 30 January 2015, p. 75.

> another investigative technique. For example, we would know that, if a person is in that area, they are using that particular Wi-Fi network, maybe, and then could use other techniques. So it is not the end of the world but, like anything else—I think the state police gave the evidence—it would be nice to have and it would be great for law enforcement. We have to do the proportionality test as well, though.[23]

5.28 The New South Wales Police Force advised the Committee that, from an operational perspective, the Bill as drafted 'will not go all the way, but we will be able to do other things, other investigative processes'.[24]

5.29 However, the Australian Intelligence Security Organisation (ASIO) advised the Committee that the exclusion of these services does carry an element of risk:

> [B}eing able to understand in national security matters the detail of the connectivity of an individual of interest – delivered through Wi-Fi services provided by carriers, businesses, local government and the community – will be critical. ASIO would argue against wide scale exemption of Wi-Fi network access providers from data retention obligations. At minimum, identifying details of the device, the Wi-Fi point of connection and the date-time stamp of the connection should be retained.[25]

5.30 Victoria Police raised similar issues from a law enforcement perspective:

> Without meaning to sound flippant, from a law enforcement point of view, I would have thought that that is self evident: that if we have got areas within our community that persons can go to and engage in communications where they are less likely to come under notice or be discovered, the persons in our community who wish to or choose to do that because they are undertaking criminal activity, or actions that they do not want to come to the attention to law enforcement, will naturally gravitate to those areas.[26]

---

23 Deputy Commissioner Michael Phelan APM, *Committee Hansard,* Canberra, 30 January 2015, p. 75.

24 Detective Superintendent Arthur Kopsias APM, Commander, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard,* Canberra, 30 January 2015, p. 56.

25 ASIO, *Submission 12.2*, p. 7.

26 Inspector Gavan Segrave, Intelligence and Covert Support Command, Victoria Police, *Committee Hansard,* Canberra, 30 January 2015, p. 57.

Declaration that obligations apply to particular services provided to an 'immediate circle' or 'same area'

5.31 Subsection 187B(2) permits the Communications Access Co-ordinator (CAC) to declare that data retention obligations apply to one or more services provided by a service provider that would otherwise be excluded under subsection 187B(1).

5.32 The Attorney-General's Department advised the Committee that:

> Based on the experience of law-enforcement and national security agencies the Bill presumes that those service providers should not be covered by data retention obligations. However, the CAC can declare data retention obligations on certain otherwise excluded service providers. The CAC can declare a service provided to a person's 'immediate circle' or to a 'same area' to have data retention obligations if the interests of national security and law enforcement agencies require that the service should. The Bill presumes that those particular types of services should not have data retention obligations, but that presumption can be rebutted.[27]

5.33 The Australian Privacy Commissioner noted that, while the CAC is required to take a range of considerations into account when declaring a service, the CAC is not required to take into account the impact of such a declaration on the privacy of individuals. Accordingly, the Commissioner recommended that, if the declaration-making power is retained, the CAC should be required to consider the 'objects of the Privacy Act' and consult with the Commissioner before making such a declaration.[28]

Committee comment

5.34 The Committee accepts that exclusions set out in proposed new section 187B are the result of a compromise to limit the privacy impact and regulatory impost of the proposed regime. The Committee notes that the exclusions do not worsen the current situation, and also accepts that national security and law enforcement agencies will retain a range of investigative capabilities that can be used where service providers do not retain detailed telecommunications data as a result of these exclusions.

5.35 However, the Committee notes its previous recommendation, as part of its *Report of the inquiry into potential reforms of Australia's national security legislation*, that the *Telecommunications (Interception and Access) Act 1979* 'be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including

27 Attorney-General's Department, *Submission 27.2*, p. 18.

28 Australian Privacy Commissioner, *Submission 92*, p. 26.

ancillary service providers) of telecommunications services accessed within Australia'.[29]

5.36 There was a strength of opinion from some Committee members that publicly-accessible Wi-Fi networks and services provided to a single area should be included in the scope of the Bill. This should be a matter for future review and, the Committee considers that the ongoing appropriateness of these exclusions should be reviewed in light of the investigative experience.

Recommendation 12

The Committee recommends that the Attorney-General's Department and national security and law enforcement agencies provide the Parliamentary Joint Committee on Intelligence and Security with detailed information about the impact of the exclusion of services provided to a single area pursuant to subparagraph 187B(1)(a)(ii) as part of the Committee's review of the regime, pursuant to section 187N of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

5.37 The ability of the CAC to declare that data retention obligations apply to a particular service provided to an 'immediate circle' or 'same area' allows for the limited expansion of the regime in circumstances where there is a particular law enforcement or security interest at stake. However, such an expansion will also have privacy implications. As such, it would be appropriate for the CAC to be required to consider the objects of the Privacy Act when making such a declaration. Consultation with the Privacy Commissioner in relation to the privacy impact may assist the CAC in his or her consideration in circumstances where there is uncertainty. The Committee also considers that oversight of the declaration-making power would be strengthened if the Committee were to be notified in each instance that a declaration is made.

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

Recommendation 13

The Committee recommends that proposed section 187B in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require the Communications Access Co-ordinator to consider the objects of the *Privacy Act 1988* when considering whether to make a declaration under proposed subsection 187B(2). If there is any uncertainty or a need for clarification, the Co-ordinator should consult with the Australian Privacy Commissioner on that issue before making such a declaration.

Further, the Co-ordinator should be required to notify the Parliamentary Joint Committee on Intelligence and Security of any declaration made under 187B(2) as soon as practicable after it is made.

Prescription of additional kinds of service providers in regulations

5.38 Subparagraph 187A(3)(b)(iii) establishes a regulation-making power, permitting additional kinds of service providers to be prescribed. However, this regulation-making power is subject to limits: data retention obligations will only apply to communications services provided by prescribed service providers that have communications-related infrastructure in Australia.

5.39 The Explanatory Memorandum states that a regulation-making power is required on the basis that:

> The telecommunications industry is highly innovative and increasingly converged. 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. As such, a regulation-making power is required to ensure the data retention regime is able to remain up-to-date with rapidly changes to communications technologies, business practices, and law enforcement and national security threat environments.[30]

5.40 In its *First Report for 2015*, the Scrutiny of Bills Committee stated that it 'considers that the range of communications service providers to which the data retention obligations will apply is a core element of the proposed scheme' and recommended that 'the types of service providers subject to

30 Data Retention Bill, *Explanatory Memorandum*, p. 43.

the data retention obligations should be set out in the primary legislation to allow full Parliamentary scrutiny'.[31]

5.41 The Law Council of Australia supported the Scrutiny of Bills Committee's recommendation.[32]

Committee comment

5.42 The Committee considers that expanding the scope of the proposed data retention scheme to apply to new classes of service providers would raise significant questions of policy that would be more appropriately considered by the Parliament. However, the Committee acknowledges that rapid changes in technology may require data retention obligations to be applied to a different range of service providers, potentially in response to emergency circumstances.

Recommendation 14

To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare additional classes of service providers under the following conditions:

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

Implementation plans, exemptions and variations

5.43 Divisions 2 and 3 in Schedule 1 to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) contain

31 Scrutiny of Bills Committee, *First Report of 2015*, p. 120.

32 Law Council of Australia, *Submission 126*, p. 9.

details of the proposed data retention implementation plans and exceptions from the mandatory data retention obligations.

5.44 This section focuses on Divisions 2 and 3 and provides an overview of the issues raised by submitters.

Implementation plans

5.45 Division 2 of the Bill introduces 'the development of data implementation plans.'[33] The Explanatory Memorandum states that the plans are intended to:

> allow the telecommunications industry to design a pathway to full compliance with their telecommunications data retention obligations within 18 months of the commencement of those obligations, while also allowing for interim measures that result in improved data retention practices.[34]

5.46 The Attorney-General's Department, in its submission, indicated that it had broadly modelled the implementation plan process after the *Broadcasting Services Act 1992* for the conversion to digital television.[35]

5.47 The Department added that the process aims to:

- allow service providers to develop and implement more cost-effective solutions to their data retention obligations, for example, by aligning the implementation of such solutions with a provider's internal business planning and investment cycles, or by modifying networks or services to allow data to be collected and retained more efficiently
- ensure that service providers achieve substantial compliance with their data retention obligations early in the implementation phase by encouraging interim data retention solutions, for example, by increasing storage capacity for existing databases to approach the two year retention period, or by prioritising the implementation of full data retention capability for some services or kinds of data
- facilitate engagement between industry and Government on the above issues
- provide regulatory certainty for industry during the implementation phase—once approved, a plan may only be varied if both the service provider and the CAC [Communications Access Co-ordinator] agree, and
- provide certainty for agencies that critical capability gaps will be mitigated in a timely fashion.[36]

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

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

35 Attorney-General's Department, *Submission 27*, p. 34.

5.48 Optus supported the introduction of data retention implementation plans, agreeing with the Attorney-General's Department that they provided certainty for industry:

> Optus supports the policy mechanism of data retention implementation plans as they can afford service providers the business certainty provided by a graduated and approved pathway to compliance.[37]

5.49 At its appearance at a public hearing, Optus added that while the implementation plan timetables were workable, it may take up to two years to fully implement the requirements due to logistical complexities:

> In terms of the scoping and the conceptualisation it is not a particularly difficult task because there is not a great variation. The real question lies with the logistics of the capacity to store consistent datasets across a very wide range of platforms for certain periods, particularly when data usage is growing and indeed when networks are, historically, in a very high state of transition.[38]

5.50 Optus commented in its submission that it would be beneficial to enhance the implementation plans:

> To afford service providers with greater business, planning and compliance certainty it would be beneficial if the effect of data retention implementation plans was also explicitly stated as being a mechanism to provide prima facie evidence of day 1 compliance with section 187A(1). That is, if a provider can demonstrate that it has successfully executed against its approved data retention implementation plan, the Bill should allow for the Communications Access Coordinator to deem that to be equivalent to compliance with section 187A(1) being achieved at the end of the implementation phase for this Part.[39]

5.51 Optus also recommended that the implementation plan could be 'expanded to play a central role in any compliance or interpretive dispute in the initial three year period of the data retention scheme'.[40]

5.52 Optus did, however, put forward the view that

---

36 Attorney-General's Department, *Submission 27*, p. 34.

37 Singtel-Optus (Optus), *Submission 86*, p. 11.

38 Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Optus, *Committee Hansard,* Canberra, 30 January 2015, p. 15.

39 Optus, *Submission 86*, p. 11.

40 Optus, *Submission 86*, p. 12.

> a service provider's ability to achieve compliance within these timeframes is subject to risk because of the dependency on timely and comprehensive decision-making on implementation plans and exemptions by the Communications Access Co-ordinator.[41]

5.53 Optus also questioned whether the CAC, enforcement agencies, and security authorities would have sufficient resources to consider and respond to the large number of data retention implementation plans in a timely manner, recommending that:

> section 187H (1) (b) (i) be amended such that the data retention implementation plans cease to be in force 18 months after the Communications Access Coordinator has completed assessment and approval of a service provider's implementation plan, or, for any amended component of a plan, 18 months from the time that each component of the implementation plan is finally agreed by the service provider and the Communications Access Coordinator.[42]

5.54 The Australian Privacy Commissioner supported the use of data retention plans, indicating that they helped provide certainty:

> I support the proposal to permit service providers to seek approval of a data retention implementation plan, as this will help to provide regulatory certainty about providers' obligations during the implementation phase of the proposed data retention scheme.[43]

5.55 The Commissioner called for the implementation plans to be enhanced 'to include further details of the type of information service providers should include in an implementation plan'.[44] The Commissioner suggested that the Explanatory Memorandum could be amended to include these additional details, stating:

> The implementation plan should also include details of the measures the service provider proposes to implement to ensure that information that will be collected and retained under the plan is protected from misuse, interference and loss and from unauthorised access, modification and disclosure. … [T]his will ensure that the appropriate security protections are in place before service providers are required to collect and store any additional

41 Optus, *Submission 86*, p. 12.

42 Optus, *Submission 86*, p. 13.

43 Office of the Australian Information Commissioner, *Submission 92*, p. 25.

44 Office of the Australian Information Commissioner, *Submission 92*, p. 25.

> information under the scheme (or an approved data retention implementation plan).[45]

5.56 The Commissioner also recommended that section 187F of the Bill be amended to require that the CAC 'take these security measures into account when deciding whether to approve an implementation plan'.[46]

5.57 In his submission, the Commissioner highlighted that the CAC must, under section 187G of the Bill, give a copy of the implementation plan to enforcement agencies and security authorities and invite them to provide comments on the plan. The Commissioner recommended that this section be amended to 'include a requirement for the CAC to give a copy of the implementation plan to the [Australian Privacy] Commissioner and invite the Commissioner to provide comments'.[47]

5.58 Electronics Frontiers Australia agreed with the Commissioner that the 'potential privacy impact for users' should be included for consideration as part of the implementation plan.[48]

5.59 Electronics Frontiers also put forward its concerns that there was a risk that the implementations plans would be used too broadly:

> There is therefore a significant risk that implementation plans will be used for everything. That is, all retention that takes place will be negotiated on a case-by-case basis between a government coordinator and a given service provider. The criteria for determining whether an implementation plan is acceptable are extremely broad—they go so far as s187F(2)(f): 'any other matter that the Coordinator considers relevant'.[49]

5.60 Dr John Selby, Professor Vijay Varadharajan and Dr Yvette Blount of Macquarie University held a similar view, recommending that security measures be taken into account when deciding whether to approve implementation plans:

> … the decision to approve a data retention plan should include analysis of whether a service provider has implemented a level of security sufficient to protect metadata sensitive to their most-at-

45 Office of the Australian Information Commissioner, *Submission 92*, p. 25.

46 Office of the Australian Information Commissioner, *Submission 92*, p. 25.

47 Office of the Australian Information Commissioner, *Submission 92*, p. 26.

48 Electronics Frontiers Australia, *Submission 97*, p. 5.

49 Electronics Frontiers Australia, *Submission 97*, p. 5.

> risk business customers (rather than the precautions necessary to protect the average risk exposure of their business customers).[50]

5.61 The Pirate Party Australia expressed its belief that the implementation plans could be more intrusive on privacy arguing that there was not sufficient justification for the data retention plans to be kept confidential.[51]

5.62 The Australian Information Industry Association questioned whether the proposed 18 month implementation plan period was sufficient 'given the infrastructure required to comply with the requirements'.[52]

5.63 At a public hearing, the Attorney-General's Department advised that during the course of the Data Retention Implementation Working Group's discussions, service providers expressed the view that the proposed draft dataset does provide service providers with sufficient information to prepare implementation plans.[53]

5.64 In its supplementary submission, the Department argued that the period for which implementation plans are in force should not be extended:

> Under the Bill a DRIP would cease to be in force 18 months following commencement of the obligation. The Department acknowledges the importance of certainty for industry participants subject to the obligations, and notes that the inclusion of both delayed commencement and a Data Retention Implementation Plan respond to and indeed exceed the period requested by industry to achieve compliance with the proposed obligation.
>
> However, the Department is also conscious of the potential for delay in implementing data retention obligations due to factors exclusively within the control of service providers. The 24 month period for service providers to reach full compliance meets the dual objectives of giving providers sufficient time to plan, develop and install their capabilities, while giving law enforcement and security agencies certainty that the implementation will be achieved within the extended implementation phase supported by the Bill.[54]

---

50 Dr John Selby, Professor Vijay Varadharajan and Dr Yvette Blount, Macquarie University, *Submission 114*, p. 5.

51 Pirate Party Australia, *Submission 124*, p. 11.

52 Australian Information Industry Association, *Submission 109*, p. 3.

53 Ms Harmer, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 24.

54 Attorney-General's Department, *Submission 27.2*, p. 14.

Committee Comment

5.65 The Committee notes the suggestions raised by submitters that the data implementation plans should include additional information on how data will be collected, retained and protected. The Committee also received a range of evidence about the security of retained data more broadly, which is discussed in Chapter 7.

5.66 The Committee is aware that service providers already have a number of obligations under the *Privacy Act 1998* and the Australian Privacy Principles, the *Telecommunications Act 1997*, the *Telecommunications (Consumer Protection and Service Standards) Act 1999*, and the Communications Alliance Telecommunications Consumer Protections Code, which all provide details on how an individual's private information is to be collected, retained and protected. However, the Committee considers that the security of retained data is a critical issue and the community must be able to have confidence in the security of stored data.

5.67 Accordingly, the Committee has made a number of recommendations to ensure the security of retained data at Chapter 7 of this report.

5.68 The Committee also notes the recommendation that the Australian Privacy Commissioner should be given an oversight role in assessing service providers' data retention implementation plans. The Committee is conscious of the administrative burden such a requirement could place on the implementation plan approval process, and does not consider it has received sufficient evidence on the matter to form a view.

Exemptions and variations

5.69 Under Division 3 of the Bill, the Communications Access Co-ordinator may exempt or vary the obligations imposed on a specified service provider.[55]

5.70 In its submission, the Attorney-General's Department stated that the proposed section 187K, which provides for the CAC to grant exemptions or variations, will:

> allow the CAC to exempt a specified service provider, or a specified class of service providers, from the data retention obligations, or to vary the provider's obligations. The proposed exemption process is modelled on the current exemption regime for 'interception capability', which is the existing requirement

55 Proposed section 187K of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

> under the [*Telecommunications (Interception and Access) Act 1979*] for providers to develop and implement technical capabilities that enable them to execute interception warrants.[56]

5.71 The Department added that:

> The exemption process would allow the data retention obligation to be tailored appropriately:
>
> - a service might be exempted entirely
> - an exemption could apply in respect of a particular type of data, or
> - an exemption could reduce the retention period for defined services and/or types of data.[57]

5.72 The Department highlighted that the CAC was required to consider a number of issues prior to granting an exemption, including:

- the interests of law enforcement and national security, for example data relating to a particular service may currently be of relatively lower relevance to investigations
- the cost to a service provider of complying with data retention obligations in relation to the relevant service, and if that cost would be disproportionately high, and
- the objects of the *Telecommunications Act 1997*, which includes matters such as the long-term interests of end-users of carriage services or of services provided by means of carriage services, the efficiency and international competitiveness of the Australian telecommunications industry, and the availability of accessible and affordable carriage services that enhance the welfare of Australians.[58]

5.73 Additionally, when making a decision on granting an exemption, the CAC may:

> also take into account the service provider's history of compliance, alternative data retention arrangements that the service provider has identified, and any other relevant issues. Exemptions may also be appropriate for trial services that are not being used or made available to the public, and where data retention capability is being developed but is not yet in place.[59]

5.74 The Law Council of Australia was of the view that the exemptions from data retention obligations were not clear:

---

56 Attorney-General's Department, *Submission 27*, p. 35.

57 Attorney-General's Department, *Submission 27*, p. 35.

58 Attorney-General's Department, *Submission 27*, p. 35.

59 Attorney-General's Department, *Submission 27*, p. 35.

> It is not clear why the proposed scheme draws certain distinctions in permitting exemptions from data retention obligations. The decision of the Communications Access Co-ordinator (CAC) may be expressed broadly and may specify service providers in any way, for example by reference to a class of service providers.[60]

5.75 The Council also sought to clarify the Australian Communications Media Authority's (ACMA) role in reviewing decisions by the CAC to grant an exemption or variation:

> It is also unclear whether the Australian Communications Media Authority (ACMA) will have the power to review a decision by the CAC to grant an exemption or variation. As currently drafted, it appears that ACMA only has the power to review implementation plans. It is unclear whether an exemption or variation will constitute part of a service provider's implementation plan or be a separate process not subject to ACMA review.[61]

5.76 The Council called for the Explanatory Memorandum to be amended 'to ensure ACMA is empowered to review the exemption and variation scheme'.[62]

5.77 In its submission, the Law Council also noted that the Explanatory Memorandum was silent on:

> why merits review by an independent body such as the Administrative Appeals Tribunal [AAT] is unavailable for decisions made by the ACMA in relation to implementation plans and CAC to grant an exemption or variation.[63]

5.78 The Council highlighted that 'a number of ACMA's other decisions which affect service providers are subject to AAT review'.[64] It argued that administrative decisions should be subject to merits review, stating:

> Unless there are valid reasons for its exclusion, an administrative decision not to exempt or vary a particular telecommunications service provider's telecommunications data retention obligations is likely to adversely affect the interests of that provider – for example, in terms of the implementation and maintenance costs of storing the data securely – and should therefore be subject to

60 Law Council of Australia, *Submission 126*, pp. 9-10.
61 Law Council of Australia, *Submission 126*, p. 10.
62 Law Council of Australia, *Submission 126*, p. 10.
63 Law Council of Australia, *Submission 126*, p. 10.
64 Law Council of Australia, *Submission 126*, p. 10.

> merits review. This is particularly pertinent given that judicial review under the *Administrative Decisions (Judicial Review) Act 1977* will not be available. No valid reason for exclusion of such decisions from merits review has been identified by the Government.[65]

5.79 The Council recommended that the Explanatory Memorandum be amended to:

- more clearly explain why the scheme proposes to apply to certain forms of media and not others
- provide for merits review for decisions made by the ACMA in relation to implementation plans and by the CAC to grant an exemption or variation or explain why merits review is not available
- make it clear that a service provider would be able to make a complaint to the Commonwealth Ombudsman in relation to a decision by ACMA or the CAC.[66]

5.80 At a public hearing, Optus expressed concerns about the capacity for a minister or CAC to provide exemptions for classes of service.[67] Optus called for a:

> … good definition of an exemption regime that could enable a discussion about that. I cannot see why it could not be in an instrument that can be subject to some external scrutiny …[68]

5.81 The Australian Information Industry Association put forward the view that the proposed section on exemptions in the Bill was ambiguous and could lead to 'potential scope creep'.[69]

5.82 The Communications Alliance and the Australian Mobile Telecommunications Association (AMTA), in their joint submission, expressed their belief that red tape could be limited by appropriate exemption provisions.[70]

5.83 The Communications Alliance and AMTA asked that consideration be given to exempting a number of services up-front, including:

- over the top services such as IPTV, on-demand movie services and Fetch TV,

65 Law Council of Australia, *Submission 126*, pp. 10-11.

66 Law Council of Australia, *Submission 126*, p. 11.

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

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

69 Australian Information Industry Association, *Submission 109*, p. 3.

70 Communications Alliance and the AMTA, *Submission 6*, p. 11.

- bespoke customer solutions, as typically offered to large corporate customers,
- services supplied where end user is not identifiable at the Carrier/CSP level (metrowave, virtual private local access network service, ethernet over copper, 10 GbE point-to-point, or internet (access) service),
- services used for machine to machine communications (extranet solution or machine to machine), and
- broadcast/content services (Satellite broadcast or on demand movie services).[71]

Committee Comment

5.84 The proposed sections 187G(4) and (5) 'provide for the role of the ACMA in relation to a proposed amendment of a service provider's implementation plan'.[72] These subsections will require the CAC to refer disputes over proposed implementation plan amendments to ACMA for determination.[73]

5.85 As noted in the Explanatory Memorandum:

> ACMA is the industry regulator for the telecommunications industry, and has substantial expertise relating to the technical and commercial operation of the industry. As such, the ACMA is the appropriate body to review any dispute over a request to amend a data retention implementation plan.[74]

5.86 The Committee therefore agrees with the Law Council of Australia that the ACMA should also have a role in reviewing any disputes over proposed implementation plan exemptions or variations.

Recommendation 15

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 and accompanying Explanatory Memorandum be amended to enable the Communications Access Co-ordinator to refer any disputes over proposed implementation plan exemptions or variations to the Australian Communications Media Authority for determination.

71 Communications Alliance and the AMTA, *Submission 6*, pp. 11, 24-25.
72 Data Retention Bill, *Explanatory Memorandum*, p. 53.
73 Data Retention Bill, *Explanatory Memorandum*, p. 53.
74 Data Retention Bill, *Explanatory Memorandum*, p. 53.

5.87 The Committee is not convinced of the merits of exempting certain services up-front and believes the Bill provides significant scope to apply for exemptions where appropriate.

5.88 The Committee notes that decisions made under the *Telecommunications (Interception and Access) Act 1979* are not subject to review by the AAT, and are exempt from review under the *Administrative Decisions (Judicial Review) Act 1977*. This is consistent with the long-standing practice in relation to decisions relating to national security.[75]

Cost of data retention

5.89 A number of submitters and witnesses raised concerns about the potential cost impacts of data retention.

5.90 The Australian Communications Consumer Action Network (ACCAN) highlighted the risk that, should service providers pass through any increased costs as a result of data retention to consumers, the impact would be felt disproportionately by those on the lowest incomes within society.

> We already see many consumers going without to pay their phone and internet bills, and so we are very concerned about the level of cost that may be associated with this system. … [W]e are very concerned that this will cause a distortion in the marketplace and make things very, very difficult for consumers.[76]

5.91 Telstra summarised the ways in which the proposed scheme would create costs for Telstra and other service providers, stating that the scheme would create:

> both capital costs and operational costs. The impact on our business comes not just from the new data we must collect but from the requirement to extract, index, store and retrieve upon request from the dataset, as well as security measures needed to impact the data.[77]

5.92 As part of its 2013 inquiry, this Committee received a number of estimates from the telecommunications industry about the potential cost of implementing a data retention scheme. For example:

---

75 *Administrative Decisions (Judicial Review) Act 1977*, Schedule 1, item (d).

76 Ms Narelle Clark, Deputy Chief Executive Officer, Australian Communications Consumer Action Network (ACCAN), *Committee Hansard,* Canberra, 29 January 2015, p. 80.

77 Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 7.

- The AMTA and Communications Alliance estimated that data retention could cost between $500m and $700m, across industry;[78] and
- iiNet estimated that data retention would cost approximately $400m, across industry.[79]

5.93 A number of submitters to this inquiry also drew the Committee's attention to the costs incurred in implementing data retention overseas. For example:

- The Pirate Party Australia drew the Committee's attention to the UK Government's assessment that retaining IP address allocation records, which are a central feature of the Government's proposed data set, will cost £26.6m over ten years to establish and operate.[80] This equates to approximately $0.10 per person, per year.[81]
- The Law Institute of Victoria cited data that Deutsche Telekom (Germany's largest telecommunications company with 39.1m mobile and 13.3m fixed broadband customers in 2008),[82] incurred capital expenses of €5.2m implementing data retention.[83] This equates to approximately $0.15 per customer.[84]

5.94 However, these cost estimates do not necessarily reflect the cost of the current proposed scheme. The Committee notes that the estimates provided by service providers in 2012 were prepared without the benefit of draft legislation or a proposed data set, and that many of the estimates were premised on providers of internet access services being required to retain web-browsing histories,[85] which would have involved the collection of a 'stupendous'[86] volume of data.

---

78 AMTA and Communications Alliance, *Submission 114* (PJCIS Inquiry into Potential Reforms of Australia's National Security Legislation), p. 14.

79 Mr Steve Dalby, Chief Regulatory Officer, iiNet Ltd, *Committee Hansard,* Sydney, 27 September 2012, p. 48.

80 Pirate Party Australia, *Submission 124*, p. 14, citing European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*; and Wilfried Gansterer and Michael Ilger, *Data Retention – The EU Directive 2006/24/EC from a Technological Perspective*, Wien: Verlag Medien und Recht, 2008.

81 Based on the population of the United Kingdom being 64.1m, and exchange rate of GBP 1.00 = AUD 1.98.

82 Deutsche Telekom, *Annual Report 2008*, pp. 52, 58.

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

84 Based on an exchange rate of EUR 1.00 = AUD 1.47.

85 See, for example: AMTA and Communications Alliance, *Submission 114*, p. 14; Mr Steve Dalby, iiNet Ltd, *Committee Hansard,* Sydney, 27 September 2012, p. 48 (PJCIS Inquiry into Potential Reforms of Australia's National Security Legislation).

86 Mr Steve Dalby, iiNet Ltd, *Committee Hansard,* Sydney, 27 September 2012, p. 48.

5.95 By comparison, the current proposal is to require the providers of internet access services to collect IP address allocation records, which iiNet advised at the time could be retained 'for a very long time at very little cost'.[87]

5.96 Optus stated in evidence that the cost of the proposed scheme would be would significantly lower than some of the previous estimates, and would potentially reduce further as discussions around exempting particular services progressed:

> [Y]ou will be aware of numbers that have been speculated about for similar regimes that have been proposed in the past, particularly in 2012-13. There were also some proposals in 2010. Some of those have been speculated about in the media. Our view is that, while the costs are substantial, what is proposed now, though, would be considerably below the upper end of what has been speculated about for previous proposed regimes. Indeed, as discussions proceed, if some of the refinements being discussed proceed further we can see the costs being reduced further.[88]

5.97 Similarly, the figures for overseas regimes necessarily reflect the regimes implemented in those jurisdictions, rather than the regime and data set proposed by this Bill.

5.98 In the context of the current inquiry, service providers were unwilling to publicly advise the Committee of their estimated cost impact due to the commercially sensitive nature of such figures.[89]

5.99 In September 2014, the Attorney-General's Department engaged PricewaterhouseCoopers, a consultancy, to model the cost of implementing mandatory data retention. In its supplementary submission, the Department confirmed that these consultations include 'a representative sample of the telecommunications industry' and that refinements of cost estimates are ongoing.[90]

5.100 Optus explained why, as a service provider, it was not in a position to provide a definitive cost estimate to PricewaterhouseCoopers. In particular, Optus noted that, while it had been able to provide 'ballpark

87 Mr John Lindsay, Chief Technology Officer, iiNet Ltd, *Committee Hansard,* Sydney, 27 September 2012, p. 50.

88 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 14.

89 See, for example: Mr Shaw, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 7; Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (Vodafone), *Committee Hansard,* Canberra, 29 January 2015, pp. 62, 64; Mr Epstein, Optus, *Committee Hansard,* Canberra, 30 January 2015, p. 14.

90 Attorney-General's Department, *Submission 27.2*, p. 5.

estimates' of the cost of implementing mandatory data retention,[91] it would not be able to definitively model its costs until the legislation is fully enacted and implemented, as 'settled law is ultimately the arbiter':

> For example, the deliberations of this committee might affect the requirements. When those sorts of things are more settled—that is the reality of this.[92]

5.101 Vodafone noted that it was continuing to engage with the Attorney-General's Department about technical options that Vodafone may be able to implement to reduce the volume of data it may need to collect and store. These options would reduce costs.[93]

5.102 Optus also noted that its final costings would depend on which services are granted exemptions under the legislation and that, while there is a 'pretty mature and, indeed longstanding understanding' within industry and Government about which services are relevant for national security and law enforcement purposes,[94] final decisions on these matters could not be made until the Bill receives Royal Assent.[95]

5.103 The Attorney-General's Department confirmed that there had been 'various iterations of PricewaterhouseCoopers' draft reporting', but advised that a draft or finalised version of the report document itself would likely not be able to be provided to the Committee due to Cabinet confidentiality.[96]

5.104 However, on 9 February 2015, the Attorney-General's Department provided the Committee with a two-hour confidential briefing on the preliminary findings of the PricewaterhouseCoopers report. The Committee also received an unclassified version of the Department's opening remarks for that briefing, which the Committee has accepted as a submission and made available on its website.[97] Based on this briefing, the Committee understands that the upfront capital costs of implementing data retention will be between approximately $188.8million and $319.1million.[98]

5.105 The Department also advised the Committee that:

91 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 14.

92 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 18.

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

94 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 19.

95 Mr Elsegood, *Committee Hansard,* Canberra, 30 January 2015, pp. 18-19.

96 Mr Chris Moraitis PSM, Secretary, Attorney-General's Department, *Committee Hansard,* Canberra, 30 January 2015, p. 71.

97 Attorney-General's Department, *Submission 27.4*.

98 Attorney-General's Department, *Submission 27.4*, p. 1.

> The retention period will have only a modest impact upon the costs. PwC have estimated that should the retention period increase by 12 months, the cost to industry would increase between $11.4 million and $20.9 million.
>
> Alternatively, reducing the retention period by 12 months would decrease the costs between 5 per cent and 6 per cent. This amounts to a decrease in costs of between $11.4 million and $16.6 million.[99]

Impact on small and medium-sized enterprises

5.106 Several submitters and witnesses raised concerns that the scheme could impose disproportionate costs for smaller service providers, who would have limited capacity to absorb any significant capital expenses. For example, Mr Chris Berg, Senior Fellow at the Institute of Public Affairs, argued that:

> This cost will have significant effects on the shape of the telecommunications industry. The cost of regulatory compliance is not evenly distributed among firms of all sizes. It will be relatively more expensive for low-budget telecommunications providers – who do not, and have no business desire to store masses of data currently – to implement the government's full data retention scheme. Regulations favour large incumbent firms over smaller ones.[100]

5.107 Similarly, ACCAN stated that:

> The information available suggests that the costs associated with the scheme are not marginal per user but are predominately fixed for each telecommunications provider. As such, it is likely that smaller providers – with fewer users – would have to pass on a disproportionately higher cost to their customers.[101]

5.108 ACCAN further argued that there was the potential for smaller providers to be priced out of the market as a result of increased costs – that is, data retention could have an anti-competitive impact, unless appropriate funding arrangements are put in place.[102]

5.109 On the other hand, Telstra argued that this view may be 'a little bit simplistic':

---

99 Attorney-General's Department, *Submission 27.4*, p. 1.

100 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 11.

101 ACCAN, *Submission 120*, p. 8.

102 ACCAN, *Submission 120*, p. 9.

> We think the complexity of systems, numbers of systems and the like mean that on a per-subscriber basis you could find that it will vary according to factors other than just the size of the ISP or carrier. If you are providing only a simple broadband service but you have a large number of customers, as opposed to a carrier that has multiple systems—mobile platforms, fixed platforms, IP platforms, the old PSTN—then you have a multitude of products across them. That complexity adds significantly to the cost of extracting and indexing and collecting that information. So, we would not agree with the proposition that says that the cost of implementation is directly linked to the size. We think complexity is a very important factor. [103]

5.110 Similarly, Optus argued that the cost impact, and therefore the reimbursement, would likely vary significantly between providers:

> You will have heard evidence already, and it is very apparent from some of the representations you will have heard from our industry group, the Comms Alliance, that there is a great deal of variation in capability, in capital capability and, indeed, in call. There are hundreds, I think over 600, service providers in Australia at the moment. Some of them are quite small outfits who may not have the capability themselves. A lot of these outfits are, of course, drawing wholesale services from some of us major providers. For some of our major wholesale customers, for example, if they have an interception capability plan, it is essentially our interception capability plan, which we are running for them on a wholesale basis. I cannot see why that sort of thing could not be accommodated in this regime when you are negotiating plans with individual providers, which might obviate the need for a standard set of expenditure or hardware or software requirements.
>
> So, accordingly, it is likely to vary. Some people may want to go down one path; others might want to go down another. What I can tell you is that, as occurs today, the vast bulk of the burden will fall to the three largest carriers, in particular the two largest carriers.[104]

103 Mr Shaw, *Committee Hansard,* Canberra, 29 January 2015, p. 12.

104 Mr Epstein, *Committee Hansard,* Canberra, 30 January 2015, p. 19.

Government funding for service providers

5.111 The major telecommunications companies acknowledged the importance of communications-related information to safeguarding national security and combating serious crime, and the commitment of industry to assist in this area.[105] For example, Telstra stated that:

> Protecting its citizens is one of the state's most fundamental roles. The use of telecommunications data is critical to modern policing and national security. It helps save the lives of Australians and solve serious crime. … One of the obligations that come with being a telecommunications carrier and internet service provider in Australia is the requirement to provide lawful assistance to the agencies. This is a profound responsibility for industry and one we take very seriously.[106]

5.112 However, service providers generally recommended that the cost of data retention should be funded by Government. For example, Optus argued that:

> If Government considers there is a net benefit to the community of imposing these obligations (in the national interest) then it should also be prepared to contribute to the costs and assist in a practical manner via capital funding to at the affected providers to make the expected benefit come about.[107]

5.113 ACCAN noted that, without Government funding, providers are likely to pass on some or all of any costs incurred as a result of data retention to consumers, with a potentially regressive impact for Australians on low incomes. ACCAN and argued that:

> Therefore, to ensure that costs passed on to consumers are minimised, ACCAN supports the view that government should bear the cost of the mandatory data retention scheme. Furthermore, in line with the public policy theory of user-pays, the federal government should cover the costs because the scheme is being implemented as a policy objective of the government rather than of the telecommunications industry. Government funding, while falling on taxpayers, would be less regressive than necessitating recovery from consumers.[108]

105 Communications Alliance and the AMTA, *Submission No. 6*, p. 2; Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 66; Mr Epstein, *Committee Hansard*

106 Mr Shaw, *Committee Hansard,* Canberra, 29 January 2014, p. 7.

107 Optus, *Submission 86*, p. 21.

108 ACCAN, *Submission 120*, p. 8.

5.114 ACCAN also drew the Committee's attention to a recommendation made by the Internet Society of Australia that industry costs could be funded in one of two ways:

- Relevant law enforcement and national security agencies could subsidise the telecommunications provider's capital implementation costs and pay the true cost of each access request they make; and
- A public subsidy could be made available to telecommunications providers and calculated and allocated in an effective manner.[109]

5.115 If Government does not cover the entire cost of data retention, ACCAN recommended that any funding arrangements should be made proportional to a provider's subscriber base, to minimise anti-competitive impact.[110]

5.116 The Government has undertaken to make a 'substantial contribution' to both the cost of implementation and the operation of the scheme.[111] Australian service providers are currently able to recover the costs of complying with data authorisations on a 'no profit, no loss' basis.[112]

5.117 In response to a question from the Committee, the Attorney-General's Department provided a summary of how other jurisdictions have funded the implementation of mandatory data retention:

> The European Commission's Evaluation Report on the Data Retention Directive, published in 2011, examined the funding models for data retention. The reimbursement of costs is categorised either as operational expenditure (e.g. operating costs related to operating the business, devices, components, equipment or facilities) or capital expenditure (e.g. cost of developing or providing infrastructure, overheads such as wages facilities' rent and utilities). The Evaluation reported that a majority of the countries (13 countries including Ireland, Greece, Portugal and Poland) pay neither operational nor capital costs. Six countries (Belgium, Denmark, Estonia, France, Lithuania and Netherlands)

109 ACCAN, *Submission 120*, p. 8, quoting Internet Society of Australia, 'Ten questions about metadata retention', 6 August 2014, <http://www.isoc-au.org.au/Media/ISOC-AU_Ten_questions_metadata_retention20140806.pdf> viewed 26 February 2015.

110 ACCAN, *Submission 120*, p. 9.

111 The Hon Malcolm Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12562.

112 *Telecommunications Act 1997*, section 314.

provide only operational costs. Only the UK and Finland pay both operational and capital costs.[113]

5.118 The New South Wales Police Force drew the Committee's attention to the 2005 *Report of the Review of the Regulation of Access to Communications* (the Blunn Review).[114] The Blunn Review recommended, among other things, that the capital expenses associated with the telecommunications interception and access regime should be allocated 'where they are best able to be managed'. That is, that service providers should bear the capital expenses associated with developing and incorporating capabilities into their networks, while agencies should bear the costs associated with each interception warrant or request for access to telecommunications data.[115]

Committee comment

5.119 The Committee also notes that services providers are currently entitled to recover their actual costs in complying with a data authorisation on a 'no profit, no loss' basis. The Bill does not propose to alter that arrangement.

5.120 In regards to a mandatory data retention regime, in its 2013 report this Committee recommended that these 'costs incurred by providers should be reimbursed by the Government'.[116]

5.121 In this course of this inquiry, the Committee has heard significant concerns about the potential cost-impact of mandatory data retention, particularly in relation to small and medium-sized ISPs, which may not have the financial wherewithal to fund any significant capital expenditure.

5.122 As noted above, the Committee received a confidential briefing on the costings from the Attorney-General's Department and the opening statement from that briefing has been accepted as a submission and published on the Committee's website.[117] Indicative costing estimates for industry's implementation of the data retention scheme, based on PricewaterhouseCoopers analysis, suggested that the upfront capital cost of the regime would be between $188.8 million and $319.1 million.

5.123 The Committee accepts that it may not be in the public interest for Government to fully fund the costs of implementing data retention in all cases. As the Blunn Review noted, there is a strong economic argument

113 Attorney-General's Department, *Submission 27.2*, p. 5.

114 Detective Superintendent Kopsias, *Committee Hansard,* Canberra, 30 January 2015, p. 56.

115 Mr Anthony Blunn AO, *Report of the Review of the Regulation of Access to Communications*, pp. 49-50.

116 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, p. 192.

117 Attorney-General's Department, *Submission 27.4*.

that costs should be borne by the party best able to mitigate those costs. Service providers are better placed to develop efficient solutions to their data retention obligations, for example through outsourcing, or innovative technical solutions. Without at least a degree of cost discipline, there is a genuine risk that some service providers may engage in the sort of 'gold plating' that has been experienced in other sectors.

5.124 Further, as a number of service providers have acknowledged, their services also enable and facilitate serious criminal activity and threats to national security. There is an argument that service providers should bear some of the cost of addressing these external harms.

5.125 The Committee notes that only two out of 21 countries identified in the European Commission's *Evaluation Report* have provided up-front funding for the capital costs of data retention.

5.126 Accordingly, the Committee welcomes the Australian Government's commitment to make a 'substantial contribution' to the costs of implementing and operating the scheme. The Committee expects that national security and law enforcement agencies will continue to contribute to the operational costs associated with accessing data under the scheme under the existing 'no profit, no loss' arrangements. In determining how to appropriately assist industry with capital costs associated with the mandatory data regime, the Committee considers that there are a number of factors which should characterise any funding model.

5.127 An appropriately developed funding model offers the opportunity for an approach that mitigates any potential anti-competitive impacts on small and medium-sized businesses, and reduces pass-through costs to consumers, while encouraging industry to implement their obligations in a cost-effective manner.

Recommendation 16

The Committee recommends that the Government make a substantial contribution to the upfront capital costs of service providers implementing their data retention obligations. When designing the funding arrangements to give effect to this recommendation, the Government should ensure that an appropriate balance is achieved that accounts for the significant variations between the services, business models, sizes and financial positions of different companies within the telecommunications industry. In particular, the Committee recommends that the Government ensure that the model for funding service providers:

- **provides sufficient support for smaller service providers, who may not have sufficient capital budgets or operating cash flow to implement data retention, and privacy and security controls, without up-front assistance;**
- **minimises any potential anti-competitive impacts or market distortions;**
- **accounts for the differentiated impact of data retention across different segments of the telecommunications industry;**
- **incentivises timely compliance with their data retention obligations;**
- **provides appropriate incentives for service providers to implement efficient solutions to data retention;**
- **does not result in service providers receiving windfall payments to operate and maintain existing, legacy systems; and**
- **takes into account companies that have recently invested in compliant data retention capabilities in anticipation of the Bill's passage.**