Submission to the Parliamentary Joint Committee on Intelligence and Security

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

January 2015

Contents

Section 1. Executive summary

1.1 Optus welcomes the opportunity to provide this submission to the Committee's inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* ("the Bill").

1.2 Optus considers that it is ultimately a matter for Government to balance the fundamental principles at stake in the proposed data retention regime, that is, the extension of the power of the state over the individual and the associated tension with privacy principles and civil liberties and the utility of the information and guaranteed access to law enforcement and national security agencies.

1.3 Policy in this area is the prerogative of Government and Optus will not attempt to conclude the appropriate balance or present a view on the merits of the policy, but will observe a number of relevant facts pertinent to this balance and present comment and analysis based on a commercial and practical compliance perspective on the Bill.

1.4 In this context, Optus' key priority is for the Bill and data retention regime to establish:

(a) a **practical and stable legislative and policy framework**, which allows for business and compliance certainty for service providers;

(b) arrangements for **a capital contribution from Government** to service providers to assist meet implementation costs;

(c) a set of arrangements which are consistent with the **privacy objectives of our customers** and which do not undermine the confidence and position of trust service providers hold in the supply of communications services to their customers.

1.5 Optus considers the proposed data set is basically workable, with a critical proviso that appropriate level of detail and interpretive guidance being made available in the Regulations which are proposed to buttress the provisions in the Bill which prescribe the kind of information which must be retained.

1.6 While Optus appreciates the opportunity it has had to work with the Data Retention Implementation Working Group convened by the Attorney-General's Department which has been focussing in some detail on the data set, the fact remains that draft regulations have not been made available and this omission does restrict service provider's ability to arrive at definitive views on both the workability and cost of the proposals.

1.7 Optus makes a number of recommendations to the Committee throughout this submission. The recommendations focus on key issues arising from Optus review of the Bill and associated arrangements.

1.8 With regards to the framework established by the Bill for the data set, Optus has recommended at paragraph 3.6 that a draft of the regulations be made available to both service providers and the Committee to assist and inform further deliberations on the Bill. Further, at paragraphs 3.8 and 3.80, Optus has recommended that the data set be kept fixed (unchanged) until at least after the scheduled review of the operation of this part of the legislation by the Committee.

1.9 With regards to the detail of the data set, Optus recommends clarification is required for the definition of "session" (paragraph 3.26), to the retention obligation applying to incoming IP

'packets' (paragraph 3.8), whether the "data volume usage parameter" is within scope (paragraph 4.6), whether the retention of customer passwords and duplication of some records is required (paragraph 4.9), matters within a provider's control (paragraph 4.11), and limitations on the availability of location information (paragraph 4.13).

1.10 Optus also recommends at paragraph 3.33 that the flexibility of the arrangements would be enhanced if there was an ability for alternate (or shorter) retention periods to be determined in special cases, for example, data elements that generate a very high volume of storage requirements and may be of lesser utility to agencies.

1.11 Optus considers the implementation timeframes set out in the Bill as generally reasonable, but notes that 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. See also the comment below at paragraph 1.13 and recommendation at paragraph 3.55.

1.12 Optus acknowledges the utility of the proposed Data Retention Implementation Plan concept, both to enable a measure of business certainty for providers and transparency to government about progress towards compliance. In practice, the success of the concept of Data Retention Implementation Plans will be reliant on timely and efficient decision-making by the Communications Access Co-ordinator.

1.13 Optus recommends at paragraph 3.50 that the process for approval and variation of Data Retention Implementation Plans be time bound at each step, and at paragraph 3.55 that the eighteen month implementation period should commence for a provider once the Communications Access Co-ordinator approves its Implementation Plan.

1.14 To enhance the investment and compliance certainty afforded by an approved Data Retention Implementation Plan, Optus recommends at paragraph 3.45 that in the event of a dispute about compliance, that the Communications Access Co-ordinator can investigate and deem a provider to have met its obligations if it has executed successfully against its approved Plan and can produce data consistent with the Plan.

1.15 A successful exemptions regime is a critical factor in the workability of the obligations. Optus recommends at paragraph 3.71 that the Communications Access Co-ordinator be given incentive to positively exercise powers to initiate consideration of exemptions at his or her own volition, especially early in the regime. The use of "own volition" considerations in conjunction with "class exemptions" may avoid the exemption process being clogged up with individual service exemption applications from each provider about similar matters. This would create potential of time delay, resourcing issues for the Co-ordinator and compliance jeopardy for service providers.

1.16 Optus also recommends at paragraph 3.74 a way of limiting the compliance risk for providers if they proceed with an exemption on the basis of a "non-decision" by the Communications Access Co-ordinator.

1.17 With regards to the transparency measures, Optus has also highlighted that the Bill will result in dual reporting arrangements and recommends at paragraph 3.84 that consideration be given to consolidating reporting obligations into one agency and Minister.

1.18 The data retention obligations will impose a substantial net cost, scheduling and resource impact on Optus, a provider that already makes a substantial 'social licence' contribution through its current levels of assistance to Government and agencies.

1.19 The proposed obligations will require Optus to put in place a set of arrangements to collect, store and retrieve data that it does not currently have in place today (or only partially exist

today) and bear an additional administrative and compliance burden, for example, to develop Data Retention Implementation Plans, reporting arrangements and exemption requests. The business and security risk faced by Optus also will be affected by the obligations proposed by the Bill.

1.20 In practical terms, Optus will need to initiate a significant scoping and compliance program which will operate for at least two years. It will have to identify and schedule its activities and resourcing amongst other critical commercial activity, business plans and customer contracted commitments. Optus already has major IT and network renewal programs in flight and scheduled for implementation over the next three years.

1.21 Optus recommends at paragraph 5.13 that in the context of this Bill, the Committee reiterate its earlier finding that Government should make a substantial contribution to costs incurred by providers in implementing data retention obligations.

1.22 Optus stands ready to elaborate on matters raised in this submission if invited to participate in the Committee's hearings.

End.

Section 2. Background

2.1 The SingTel Optus Pty Ltd group companies in Australia (hereafter called "Optus") serve over 10 million customers per day with a broad range of communications services, including mobile, national, local and international telephony, voice over IP, fixed and mobile broadband, internet access services and subscription television (including IPTV).

2.2 To deliver these services, Optus owns and operates fixed, mobile and long haul transmission and access networks and the largest domestic fleet of satellites. These provide a set of advanced technology platforms for the delivery of services. Optus has invested over one billion dollars in each of the last seven years to improve and upgrade its networks and services.

2.3 Optus also has an extensive wholesale business, providing services to hundreds of other carriage service providers. The Optus group companies also include other significant brands such as Virgin Mobile. In short, Optus is a provider of significant and critical national communications infrastructure and services to the Australian community and takes this responsibility seriously.

2.4 Optus has also invested in required interception and delivery capability on its platforms and services and operates a specialist team, its Law Enforcement Liaison Unit, which responds to warrants for lawful interception, authorised requests for call related data and other requests for assistance from law enforcement and national security agencies. The costs of this team and the infrastructure and capability to support it are substantial.

2.5 It is ultimately a matter for Government to balance the fundamental principles at stake in the proposed data retention regime, that is, the extension of the power of the state over the individual and the associated tension with privacy principles and civil liberties and the utility of the information and guaranteed access to law enforcement and national security agencies.

2.6 Optus will not attempt to conclude the appropriate balance or present a view on the merits of the policy, but will observe a number of relevant facts pertinent to this balance and present a commercial and practical compliance perspective on the proposals.

2.7 In this context, Optus' key priority is for the Bill and the data retention regime to establish:

(a) a **practical and stable legislative and policy framework**, which allows for business and compliance certainty for service providers;

(b) arrangements for **a capital contribution from Government** to service providers to assist meet the implementation costs of the data retention obligations in the Bill;

(c) a set of arrangements which are consistent with the **privacy objectives of our customers** and which do not undermine the confidence and position of trust service providers hold in the supply of communications services to their customers.

2.8 Optus' experience as a 'carrier practitioner' and carriage service provider which provides extensive assistance to the many Australian law enforcement and national security agencies under the various existing legislative provisions informs the following comments on the Committee's terms of reference and the Bill.

Section 3. Detailed comments on the Bill

Schedule 1 – Data Retention

Part 1 - Main amendments: Proposed new Part 5-1A – Data Retention

Division 1: Obligation to keep information and document

3.1 The proposed **Section 187A(1)** sets out a high level obligation to retain information, relying on existing definitions of service provider, service and communication. It adopts the device of providing for regulations to specify in more detail the information which must be kept.

3.2 Optus considers the use of regulations to spell out more detail of the intended data set is appropriate. The initial regulations and any subsequent proposal to alter them should also be subject to suitable safeguards to minimise the chance of unintended scope creep which could have the effect of imposing of substantial costs or complexity on the regulated entities.

3.3 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.

3.4 Attention should be given to the drafting of the regulations so that scope creep cannot easily come from changing "interpretations" over time. Industry scrutiny and input into of the drafting of regulations can assist with this objective.

3.5 Optus appreciates the opportunity it has had to work with the Data Retention Implementation Working Group convened by the Attorney-General's Department. The working group process has assisted refine and increase understanding of the draft data set supplied by the Attorney-General's Department. Nevertheless, Optus has not yet seen draft regulations and considers these a critical component necessary to evaluate the overall package, including estimating costs.

3.6 **Optus recommends that a draft of the regulation describing the data set definitions be made available as soon as possible, to assist the Committee and the Parliament's consideration of the Bill, and further consideration of cost and implementation issues by the industry.**

3.7 A reasonable expectation of stability of the data set for the transitional period and at least until after a specified policy evaluation point, would give service providers planning and investment certainty, and allow time for efficient practices to be developed and refined.

3.8 **Optus recommends that the data set defined in the regulations be fixed until after the proposed review of the operation of this Part proposed for the Committee in section 187N. That is, the regulations, or enabling legislation should require stability in the initial data set pending the scheduled review by the Committee.**

3.9 As mentioned above, the proposed **Section 187A(2)** provides guidance on the matters to which the data set to be prescribed in regulations must relate. Optus considers this a useful technique to define in the primary legislation the scope of the regulations, and provide legislators and the public with this guidance on the potential scope of the detailed obligations able to be included in regulations.

3.10 The proposed **Section 187A(3)** provides a scoping statement on the nature of services to which the obligation to keep information applies. In the main, it leverages off existing definitions and is reasonably clear in its application. It does however, provide at Section 187(3)(b)(iii) for services to be prescribed by regulation.

3.11 **Optus recommends that a draft of any proposed regulation describing further service types to which the information retention obligation will apply be made available as soon as possible, to assist the Committee and the Parliament's consideration of the Bill, and further consideration of cost and implementation issues by the industry**.

3.12 The proposed **Section 187A(4)** provides useful clarification that providers are not required to keep information that is the content of a service. Some clarification is required in relation to incoming internet communications.

Incoming Internet communications

3.13 Optus' understanding is that the policy intent is to exclude from the data retention regime the contents of communications and any means to determine the content of communications. That is, to exclude the possibility of the reconstruction of communications content from analysis of internet packet address details. The draft legislation may not sufficiently exclude this for incoming communications to a customer.

3.14 The Bill excludes via section 187A (4) (i) the internet packet address for packets sent from a telecommunications device, using an internet access service provided by the service provider. The Bill and the draft data set recognise that communications is inherently a two way process and require the collection and retention of both the source and destination of a communication (section 187A (2) (b) and (c)). In broad terms, the draft legislation requires this data to be collected by both the service provider where the communications are originated and by the service provider where the communications are received.

3.15 The draft data set states, in relation to the source of a communication:

> *Any identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.*

3.16 This aligns with the policy intent, as the requirement is related to the "relevant service" However, 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.

3.17 Optus suggests that legislation could be clarified with text following section 187A (4) (b) similar to:

> "*Information that:*
>
> *(i) states an address from which a communication was sent on the internet where that communication is received by the service provider from a source other than the subscriber, and*
>
> *(ii) was obtained by the service provider only as a result of providing the internet access service.*
>
> *Note: this paragraph puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history that could be inferred from information about the sources of incoming communications."*

3.18 **Optus recommends that to give more certain effect to the policy intent that service providers are not required to keep information about a subscribers' web browsing history, section 187A(4)(b) should be amended, along the lines set out in paragraph 3.17 above, to specifically exclude the collection of origin IP packet address details by the service provider providing the internet access service to the receiving customer.**

3.19 Subsection 187A (4) (d) is important to ensure that conflicting obligations are not established and consistency with the terms of access to the Government's Data Verification Service is maintained.

3.20 The proposed **Section 187(5)** clarifies that an unsuccessful or un-tariffed communication event is captured by the obligation to keep information by deeming them to be "the sending of a communication by means of the service". Optus has no comment on the drafting of this section.

3.21 The proposed **Section 187(6)** sets out an obligation on service providers to use other means to create the required information if the operation of the service does not create it. This 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.

3.22 This clause is also tantamount to a data creation obligation which in certain circumstances may have significant cost, complexity, competition and compliance implications. Optus does not seek to overplay this point, but is possible to envision instances where service providers may want to take to market a service construct which does not readily generate the required data set. This concern can be accommodated if the exemption provisions are able to make allowance for such circumstances, which appears to be the case given the decision-making factors at 187K(7)(d).

3.23 The proposed **Section 187A(7)**: The term "session" is a key concept in the legislation that will determine the instances where a service provider must collect specific service usage details. It will also be a key determinant of the volume of service usage data that will need to be stored.

3.24 There still appears to be a divergence of views about the application of the concept of "session". As an example, ASIO's verbal evidence to the Committee in the public hearing on 17 December 2014 indicated an expectation that mobile location information would be available at the start of every mobile call. However, discussion at the Data Retention Implementation Working Group suggested that mobile location information would only need to be collected and retained at the start and end of a "session". This alternative interpretation is that a mobile "session" might involve several mobile calls as "session" is a concept that accumulates individual communications as per proposed section 187A(7).

3.25 Optus draws attention to the recommendation number 8 of the Data Retention Implementation Working Group's report which has proposes that the Government include additional explanatory material illustrating the application of a "communications session'.

3.26 **Optus recommends that the Committee finds that the application and interpretation of the term "session" used in section 187A(7) needs to be clarified to avoid ambiguity, and that this could be addressed in the Regulations and associated explanatory material.**

3.27 The proposed **Section 187B** provides for an exception consistent with concepts of private networks derived from the definitions in the *Telecommunications Act 1997* of 'immediate circle' and 'distinct place'. It also provides the Communications Access Co-ordinator with power to declare that data retention obligations may apply to specific services operated by a service provider. Optus considers that services supplied by carriage service providers that are

the internal building blocks of private networks should be exempted (see comments below on Division 3 – Exemptions).

3.28 The proposed **Section 187C** sets out the rules for the period for keeping information.

3.29 The proposed **Section 187C(1)(a)** sets out a two year window for which particular information (customer or account information as described in 187A(2)(a)) must be kept after an account is closed. In effect, it is possible that this specific data from a closed account may be aged nearly four years by the time its mandatory retention period expires. While it has potential to create some additional record keeping complexity depending on the compliance approach adopted, Optus does not consider this will create any significant retention burden as most of this type of information is already kept by Optus for longer than these periods for other legal reasons.

3.30 The proposed **Section 187C(1)(b)** sets out the general requirement to keep other information for a two-year period after its creation. The justification for selecting the retention period of two years has not been visible to Optus, but this is a workable time period for most data types.

3.31 The policy question for Government is whether the extra cost and privacy intrusion of keeping the entire data set for two years is outweighed by the utility for national security and law enforcement agencies of having this information available. Optus notes the current construct of the Bill does not contain a mechanism for this time period to be varied. Optus also notes that a small quantity of data set elements, mainly those related to service usage, are likely to create a high volume of data and be the key drivers of the overall IT storage costs for data retention. Close attention to the cost/benefit of those high volume data set elements is warranted in any consideration of data retention periods.

3.32 Optus considers the flexibility of the package of arrangements would be significantly enhanced if there was scope provided in the Bill for the regulations to proscribe a lesser time period for specific or "special case" data or service types. Absent this, any consideration of a lesser retention period can only be achieved on a service-by-service, provider-by-provider basis using the exemption process.

3.33 Optus recommends that Committee investigate the merits of the Bill being amended to afford flexibility for the regulations to proscribe an alternative shorter period (than the two-year period specified in Section 187C(1)(b)) for keeping information for certain services or in relation to certain service related matters specified in 187A(2).

3.34 The proposed **Section 187C(2)** sets out scope for the regulation to vary the operation of the time period rules that apply to certain customer account information via section 187C(1)(a), within the two year limit described at 187C(1)(c). Optus has no comment on this aspect.

3.35 The proposed **Section 187C(3)** provides a useful clarification that the time period for keeping information set out in the Bill does not seek to prevent service providers keeping for a longer period if their business model or other legal requirements make this necessary.

Division 2: Data retention implementation plans

3.36 The proposed **Section 187D** provides the opportunity for services providers to devise a data retention implementation plan, which provides relief from, and becomes an approved pathway towards compliance with the obligation to keep information for certain services as set out in section 187A(1). Such Plans will also afford the Communications Access Co-ordinator, and through it, the interests of law enforcement and national security agencies, visibility of each service providers planned implementation.

3.37 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. This assurance could be further enhanced.

3.38 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 Co-ordinator to deem that to be equivalent to compliance with section 187A(1) being achieved at the end of the implementation phase for this Part.

3.39 This step is considered to be an important one to give service providers business and planning certainty and also ensure the implementation plans afford the Communications Access Co-ordinator and through him or her, the law enforcement and national security agencies, transparency on the specific detail of the information items expected to be available at the end of the implementation phase for each service and each provider.

3.40 It would also recognise that despite best efforts of all parties to settle the detail of the data set in the Bill and regulations, these definitions must still be interpreted in practice and translated into the actual "data fields" resident in the providers IT and network systems. The implementation plans are the place where service providers can get to this level of detail for each service and have the approach and effective data set approved.

3.41 It would be an unfortunate and undesirable policy outcome if a provider which had successfully executed against an approved plan could then be subject to compliance risk or jeopardy at day 1 by virtue of another party seeking to impose an alternate interpretation of the obligations imposed by section 187A(1) to that which was implicit in the providers approved plan. The plans are intended to provide a measure of certainty to all parties, and focus should be on developing approving and executing on the plans and minimising the chance of post implementation disputes about interpretation and capability.

3.42 Optus recommends that the Bill be amended to provide clarity that the effect of a provider successfully executing against an approved data retention implementation plan would be that it is deemed to be compliant with section 187A(1) at the end of the implementation phase set out in section 187H(2). This would be an important protection for providers and also for the Government, in the event that public funds are contributed to assist meet the cost of the provider meeting the obligations.

3.43 In practical terms, a mechanism to achieve this outcome would be that in the event that a provider is subject to challenge on its compliance with section 187A(1) in the three year period up until the review of the scheme under section 187N, the Communications Access Co-ordinator could investigate and make findings. That is, if the Communications Access Co-ordinator found that the supplier had successfully implemented its approved data retention implementation plan and could produce data according to the description in the plan, then it could issue an opinion or evidentiary certificate that is prima facie evidence of compliance with section 187A(1) or related matters.

3.44 This power for the Communications Access Co-ordinator would dovetail in with the other powers it has to approve data retention implementation plans and consider exemption requests. These roles afford the Communications Access Co-ordinator relevant knowledge and expertise to undertake such investigations and to form such opinions if required.

3.45 Optus recommends that:

a) the effect of a data retention implementation plan be expanded to play a central role in any compliance or interpretive dispute in the initial three year period of the data retention scheme; and

b) the Communications Access Co-ordinator be afforded a role to investigate and issue an opinion or certificate which would be considered prima facie evidence of the compliance by the service provider with section 187A(1) in the event that it finds that a provider has successfully implemented an approved data retention implementation plan as demonstrated by its ability to produce data consistent with that plan on request from authorised agencies.

3.46 The proposed **Section 187E** sets out the process for service providers to apply for approval of data retention implementation plans. Optus has no comment on this section.

3.47 The proposed **Section 187F** sets out the process for the Communications Access Co-ordinator to consider and approve data retention implementation plans. Given the central nature of these plans to transparency over capability, initial compliance and the tight overall compliance timeframes faced by service providers, it is important that the procedures for approving plans are not subject to process steps that can lead to inordinate or unintended delay. The 'fail-safe' mechanism for an initial deemed approval at section 187F(3) is helpful in this regard, but does not necessarily provide for long term certainty – see also paragraphs 3.54 and 3.73.

3.48 The proposed **Section 187G** sets out the consultation process the Communications Access Co-ordinator must undertake in relation to the data retention implementation plan applications that it receives. There is potential for a number of interested parties to be consulted and inject views that may lead to requests for variation of a Plan.

3.49 Apart from a 30 day time limit on service providers responding to a request for amendment of the original plan, the balance of the process relating to requests for Plan variation do not appear to be time bound. For example, there does not appear to be a time limit on a consideration by the ACMA under sections 187G(4) and (5).

3.50 Optus recommends that the Committee make a finding that the process for approval and variation for data retention implementation plans be tightened as far as practical and to impose time limits on each decision-making and review step.

3.51 The proposed **Section 187H** sets out when data retention implementation plans are in force. It also has the effect, in conjunction with the Commencement provisions (in section 2 of the Bill) of providing a window of six months plus eighteen months after the Act receives Royal Ascent for service providers to meet the requirements of this Part.

3.52 This time period appears workable, subject to the risk to service providers implementation schedules which is created by the necessary dependence on matters outside their control such as the time it will take to achieve approved of data retention implementation plans and exemption requests.

3.53 Optus considers the implementation timeframes implicit in the Bill as reasonable, but notes that 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.

3.54 Optus notes that in practice, the Communications Access Coordinator will be required to evaluate and make decisions about a very large number of data retention implementation plans at the commencement date of the Legislation as well as make decisions about associated Exemption requests. Consultation with Agencies is also required as part of the decision making process (section 187G). Optus questions whether the Communications Access Coordinator and the Agencies will have sufficient resources to consider and respond to all of these implementation plans and exemption requests in a timely manner. Any delays in response from the Communications Access Coordinator should not subtract from the 18 month time period allowed for the development of compliant network and IT systems.

3.55 **Optus recommends 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 the each component of the implementation plan is finally agreed by the service provider and the Communications Access Coordinator.**

Division 3: Exemptions

3.56 The proposed **section 187K** provides that the Communications Access Co-ordinator may exempt a service provider from the mandatory data retention obligations, or vary the obligations that a service provider is subject to.

3.57 The Explanatory Memorandum (paragraph 106) clarifies that:

> *"The CAC may grant this exemption or variation on his or her own volition or on application by a service provider."*

3.58 While section 187K(7) sets out a number of factors to be taken into account in actually making the decision whether to grant an exemption (or variation), the current Bill does not provide any guidance on the circumstances in which the Communications Access Co-ordinator should initiate such a consideration on his or her own volition. Section 187(8) allows the Communications Access Co-ordinator to take into account other relevant matters, but once again, this appears to relate to factors to be taken into account in the decision-making of whether to grant an exemption (or variation), not the question of whether a decision-making process is initiated in the first instance.

3.59 The Communications Access Co-ordinator is in a position to ease the introductory phase of the data retention legislation and, in particular, the implementation task faced by service providers in preparing data retention implementation plans and retention arrangements, if it provides timely guidance to industry on exempt categories. This would be of particular assistance in relation to potential "class" rulings under section 187K(1), where the prospect of a number of individual applications for exemptions could be avoided with a timely self-initiated exemption by the Communications Access Co-ordinator.

3.60 An example of a class ruling has been provided in a document produced by the Attorney-General's Department in December 2014, "*Industry FAQs on the Government's proposed data retention obligations*". In similar terms to the Explanatory Memorandum (paragraph 111), it says on page 11:

> "Exemptions may also reference a class of service providers, for example the CAC may specify that any service provider that provides Internet Protocol television (IPTV) services is not required to retain any data in relation to its IPTV service. Similarly an exemption or variation may be expressed to apply to a class of obligations."

3.61 Optus considers that the value of the Communications Access Co-ordinator's power to initiate exemption considerations will be maximised if the Co-ordinator is positively encouraged to use this power as early as possible in the regime in relation to issues that are suited to "class exemptions". The early and timely use of such powers has the potential to reduce business risk, implementation costs and administrative effort for service providers in preparing individual exemption requests and data retention implementation plans and decision–making efficiency for the Co-ordinator by potentially reducing the number of individual exemption requests that have to be dealt with in the critical early days of the new regime.

3.62 In addition, and to the extent that the Communications Access Co-ordinator is required to, or decides to consult with the ACMA and law enforcement and national security agencies on matters relating to exemptions, the early and self-initiated use of class exemption powers will reduce the administrative burden on all parties.

3.63 The joint Government-industry Data Retention Implementation Working Group noted further potential candidates for exemptions including:

(i) Internet radio

(ii) Music steaming

(iii) Dark fibre

(iv) Telehealth services

Optus suggests additional candidates for exemptions:

(v) Specialised services used as building blocks within enterprise and government private networks

(vi) functions outsourced by operators of enterprise and government private networks

3.64 With reference to the examples above, it would clearly be more efficient if the Communications Access Co-ordinator made a class exemption ruling very close to the start of the implementation phase, rather than wait and react to (say) six exemption requests from individual IPTV service providers, as well as the potential for six data retention implementation plans which also deal with the matters of an exemption request being anticipated or lodged for these services.

3.65 The exemption process is expected to be an important process for:

- Providing short term relief to CSPs where immediate compliance to the data retention obligations is not technically, practically or financially viable.
- Exclusion of certain services, where the track record of Agency requests indicates a level of interest at zero or close to zero.
- Exclusion of certain data elements for certain services where compliance to the data retention obligations is not technically, practically or financially viable.

3.66 For mainstream services supplied to mass markets, Optus expects that the exemption process would be used infrequently and any exemptions granted be subject to strict conditions.

3.67 Optus may consider utilising the exemption process for:

- specialised communications services supplied to enterprise and government customers as building blocks for internal communications carried on a private network.

- the supply of services outsourced by enterprise and government customers that, if supplied by the customer, would not be subject to the data retention regime.

3.68 As an example, a large, complex enterprise may establish a private network to link multiple sites for fixed telephone and data communications within the enterprise. Optus may supply point to point communications links between the sites, such that any service or usage data the Optus might collect would only have meaning within the context of the enterprise private network, and would only be visible within the enterprise private network. Further, the day to day management of items such as data storage, routers and voice switches may be outsourced to Optus and internal enterprise data may be acquired in that process. Optus will be competing for the supply of those services with non-carriage service provider entities that will not be subject to the data retention obligations.

3.69 Inclusion of the above types of services in the data retention regime would drive costs higher, with little or no benefit expected to the investigations of Law Enforcement and National Security Agencies.

3.70 Business certainty, cost and administrative burden can be reduced by the effective and efficient functioning of the exemption decision-making power at the earliest possible time in the regime, and the chances of this occurring can be enhanced by creating incentive for the Communications Access Co-ordinator to act early of his or her own volition.

3.71 Optus recommends that the effectiveness of Division 3 can be improved if guidance is added for the Communications Access Co-ordinator to positively exercise powers to initiate of his or her own volition the consideration of exemptions or variations to obligations in situations that may reduce the 'financial and administrative burdens on participants in the Australian telecommunications industry'. This threshold is consistent with the Regulatory Policy at section 4 of the *Telecommunications Act 1997.*

Exemption Decision Process

3.72 Carriage service providers require certainty about the administration of the exemption decision process, as it will be critical during the initial implementation phase for service providers to achieve a measure of certainty over their regulatory compliance obligations (which vary whether exemptions are granted or not) and to enable business decisions to be made for capital projects.

3.73 To some extent, the legislation creates an incentive for the Communications Access Coordinator to respond within a reasonable time frame (60 days) or an exemption application is deemed to be approved (section 187M(5)(b)). However, the effect of s 187M(6) is to effectively undermine any business certainty that might arise from a non-decision under section 187M(5)(b), as the Communications Access Coordinator can override any deemed approval at any time – a day, a year or ten years after the expiry of the 60 day period. If a service provider proceeds on the basis of section 187M (5) (b), including committing to network and IT infrastructure investments, the Communications Access Coordinator can, without further consultation, make the service in question non-compliant to the data retention obligations at any time.

3.74 Optus recommends that if a service provider proceeds on the basis of a "non-decision" by the Communications Access co-ordinator under section 187M(5)(b), there should be two-

year delay before any subsequent decision by the CAC takes effect – similar to the six months staged date of effect and 18 months implementation phase.

Division 4: Miscellaneous

3.75 The proposed **Section 187L** creates confidentiality provisions for exemption requests and requests for approval of data retention implementation plans. The sensitivity and general desirability for the nature of such decisions to be protected and only made available to those that need to know is reasonable. Optus supports these protections.

3.76 The proposed **section 187M** sets out that the key data retention obligations (section 187A(1) and section 187D(a)) are civil penalty provisions for the purposes of the *Telecommunications Act 1997*. In effect, this means that the enforcement options available for the data retention regime include remedial directions, formal warnings and pecuniary penalties.

3.77 Optus supports the approach of leveraging an enforcement regime that has graduated enforcement options. In the event that a breach occurs such a regime enables consideration to be given to the range of circumstances and events that may give cause to a breach, and for suitable remedial options to be available which can be calibrated to the seriousness of the situation. See also Optus' comments about deemed compliance at paragraph 3.43 and recommendation at paragraph 3.45.

3.78 The proposed **section 187N** provides for the review of the new Part 5-1A as soon as practical after the third anniversary of the end of the implementation phase for data retention obligations. Optus supports the inclusion in the Bill of a review of the operation of this Part by the Committee, and considers the review can be best calibrated if it can focus on a stable data set for the initial period.

3.79 Optus also believes service providers should be afforded a reasonable expectation of stability of the data set for the transitional period and at least until after the specified policy evaluation point set out at section 187N. This would provide planning and investment certainty, and allow time for efficient practices to be developed and refined. This point is raised above along with other comments about section 185A(1).

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

3.81 The proposed section **187P** provides for the Minister to prepare a written report on the operation of this Part and include it in the annual report required under subsection 186(2) about the operation of data authorisation provisions.

3.82 One of the "Other amendments" proposed at Part 2, clause 3, proposes a change to **Subsection 105(5A)** which would require the ACMA to report each financial year on both the operation of Part 14 (National Interest Matters) and the costs of compliance with the data retention requirements of Part 5-1A.

3.83 These two sections (the proposed new 187P and the new 105(5A)) highlight that the current Bill envisages both the Attorney-General's Department, via the Attorney-General and the ACMA, via the Minister for Communications report to Parliament annually on closely related aspects of the data retention obligations. It would be a preferable situation if the transparency measures proposed for this part be consolidated into one report by one agency and not spread across two portfolios.

3.84 Optus recommends that the Committee consider the merit of recommending to the Government that the public accountability, transparency and reporting measures relating to the data retention regime proposed by section 187P and 186 of the *Telecommunications (Interception and Access) Act 1979* and section 105(5A) of the *Telecommunications Act 1997* be consolidated into one reporting obligation by one agency and one Minister.

Part 2 - Other amendments

3.85 Optus has no comment on the proposed amendments apart from the matter mentioned directly above regarding the proposed addition to section 105(5A).

Part 3 - Application provisions

3.86 Optus has no comment on items 7 and 8 and supports the practical and facilitative nature of items 9, 10 and 11.

Schedule 2 – Restricting access to stored communications and telecommunications data

Part 1 - Main amendments

3.87 **Items 1-4:** The proposed amendments in this Part seek to establish the set of agencies which can access stored communications and telecommunications data as well as describe a method for the Minister to add or subtract additional agencies to the baseline set of core agencies listed in the proposed section 110A.

3.88 Optus acknowledges it is the Government's and Parliament's prerogative to designate the authorised agencies for accessing retained data and balancing the various public interest elements that entails. Staff resourcing within the providers is limited so it is best devoted to servicing requests from the key state and Federal agencies identified by government. From a provider's perspective there are some minor efficiency benefits from only having to deal with the smallest set of known and relatively sophisticated users, but this is not a major policy consideration.

Part 2 - Other amendments

3.89 **Items 5-47:** Optus has no comments on these items.

Part 3 - Application provisions

3.90 **Items 48-51:** Optus considers these items to be reasonable and required transitional provisions but has no other comment.

Schedule 3 – Oversight by Commonwealth Ombudsman

3.91 **Part 1 – Amendments and Part 2 - Application provisions:** Optus notes that Schedule 3 sets out new arrangements for an oversight regime by the Commonwealth Ombudsman. Optus notes the public policy interest in ensuring an appropriate level of oversight of the access to telecommunications data but has no comments to make on the specific elements proposed or the drafting of the Bill.

Section 4. Detailed comments on the draft data Set

4.1 Optus seeks the specification of a clear and unambiguous data set via the Bill and the associated Regulations. This is needed to provide an adequate level of certainty:

(i) so that service providers can adequately assess compliance; and

(ii) design and implement networks and IT systems to retain and retrieve the required data.

4.2 The draft data set circulated by the Attorney General's Department (as per Attachment A of The Report of the Implementation Working Group) in the main provides specific requirements linked to the prescribed information types in section 187A (2) and excluding the information types specified in section 187A (4).

Data volume usage

4.3 A point raised via the Data Retention Implementation Working Group by industry representatives related to data service allowances/metrics at item 1(f) of the proposed data set. Optus supports the deletion of this aspect as proposed in the Data Retention Implementation Working Group's report. The underlying logic of this deletion does not appear to have been carried through consistently in the Working Group's findings, however, as the report also proposes the addition of 'data volume usage' to item 5(c) of the data set.

4.4 Optus' view is that the addition of "data volume usage" to item 5(c) of the data set raises concern because it may not be an item related to the allowable kinds of information set out for this element in section 187A (2) (e), "the type of a communication, or a type of relevant service used in connection with a communication." Nor is usage a "feature" of a service, as suggested in the draft data set. The type of service and related features are static components of service supply, and would be specified, for example, in standard agreements or other customer contracts.

4.5 The proposed 'Data volume usage' parameter which the Data Retention Implementation Working Group's report suggests be added to item 5 (c) is more properly considered as a measurement of the content or usage of communications and therefore it does not appear to fall within any of the allowable categories specified in section 187A (2), and section 187A(2)(e) in particular.

4.6 Optus recommends that the Committee finds that further consideration is required of the proposed inclusion of the 'Data Volume Usage' parameter in item 5 (c) of the draft data set to determine whether it is consistent with the allowable kinds of information prescribed for the regulations as set out in section 187A(2) of the Bill.

Subscriber Information

4.7 There is a risk of replication of records associated with item 1 (b) of the proposed data set in relation to related services and accounts. If the data retention regime covers both service X and Y supplied to the same customer, there is no additional value in requiring the details of Y to be included with those of X and the details of X with Y. Rather than the requirement to retain "any information", there should be the simpler requirement to simply retain the fact that the association exists.

4.8 The use of the words "any information" in data set parameter 1(a) and (b) appear to include a requirement to retain the details of any customer passwords used for service access, for example, the password to an email account. Optus' view is that release of a customer password could have the effect of allowing interception of a service outside of the lawful framework and should not be permitted. It follows that customer passwords should not be included in a data retention regime.

4.9 Optus recommends that the Committee find that further consideration is required of parameter 1 of the draft data set to remove potential replication of records and to make it clear that the data retention regime does not require retention of customer passwords.

Connection to Internet Access Services

4.10 It may not be apparent to an internet access service provider that an individual user or a particular device has connected or disconnected from an internet access service. Many home users connect to the internet using a variety of devices via a wifi or other modem. Without detailed examination of the content of communications at the individual packet level, a service provider may be unable to determine which individuals are likely to have connected or which devices are connected at any point in time because all it "sees" is the wifi or modem device.

4.11 Optus recommends that the data set obligations be adjusted to only require collection of information relating to events that the access service provider can reasonably control, rather than elements which are more directly related to actions that end users take and which providers have no easy method of determining at all, or only via detailed packet inspection of the content of a communication.

Location Information

4.12 The location of equipment may not be known to the service provider in some circumstances, for example, a provider of an 'over-the-top' email, messaging or voice service may not know the location of the underlying fixed, mobile or wifi services or devices being used.

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

Section 5. Costs of implementing data retention

5.1 Optus is currently not in a position to provide a comprehensive response to the question of how much it will cost to comply with the proposed data retention obligations. Optus has been limited in its ability to provide precise estimates because a number of key elements are either not known or not settled yet. These include exemptions, approval of data retention implementation plans, and the finalisation of the data set and associated interpretive issues. While much work has been done in recent months to clarify and refine the data set, it is not settled and draft regulations have not been sighted.

5.2 Once the requirements are settled, Optus will need to urgently initiate a commercial project to scope and review the full set of work steps required to achieve compliance and from there work to assign a cost estimate to each element. This work will take some 3-6 months to complete.

5.3 The task for Optus and Optus group companies (e.g. Virgin Mobile, Uecomm, XYZed Pty Limited, Optus Vision Pty Limited) is to review every service and associated IT systems that deal with customer information and linkages to and from network elements to fully scope current capabilities compared with the new obligations. Optus must then determine whether the services are compliant or whether gaps exists, and if so what steps are required to be taken to remedy the gaps.

5.4 A solution design stage will be required to design the IT and network activity required to capture, store and interrogate the required data for the identified gaps. It is likely that this will in part leverage off existing systems and processes, and in part require that some new systems, processes and interfaces be designed and built. Hardware requirements will also need to be scoped and tendered.

5.5 The aggregate of this activity will inform both a project plan for internal approvals and also feed into a data retention implementation plan, which will be submitted to the Communications Access Co-ordinator for consideration. The Plan will either be agreed, rejected or variations requested by the Co-ordinator.

5.6 One of the additional outcomes of the service review will be that exemptions may be requested for a number of services or situations. If so, then exemption requests will be prepared and also submitted to the Communications Access Co-ordinator for consideration.

5.7 Once these deliberations by the Communications Access Co-ordinator are made Optus will then be in a position to finalise its project plan for implementation and final cost estimates can be calculated with a higher degree of certainty. This will be at a stage well after legislation is complete and passed through Parliament.

5.8 Prior to the completion of the above steps Optus is not in a position to make precise predictions on implementation costs. However, it is clear from the review work which Optus has undertaken to date that the costs are likely to be significant.

Contribution to costs

5.9 Optus holds what it considers to be a reasonable expectation that Government will make a contribution to the capital cost of meeting the proposed new data retention obligations. The obligations require providers to make arrangements to either create or hold data in excess of current commercial needs and to likely incur very substantial compliance costs in doing so.

5.10 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.

5.11 This view is consistent with the opinion expressed by the Committee at Recommendation 42 of its 2013 "Report of Inquiry into Potential Reforms of Australia's National Security Legislation" that any draft legislation for data retention should include the following features:

> "the costs incurred by providers should be reimbursed by the Government".

5.12 To date the Government has made assurances of this nature – that it will make a contribution to costs - but the draft legislation does not contain such provisions.

5.13 **Optus recommends that the Committee make a finding that Government should make a substantial contribution to costs incurred by providers in implementing data retention obligations (reiterating its earlier finding on costs in recommendation 42 of its 2013 "Report of Inquiry into Potential Reforms of Australia's National Security Legislation").**

End.