Australian Government
Office of the Australian Information Commissioner

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

Submission to the Parliamentary Joint Committee on Intelligence and Security

January 2015

Timothy Pilgrim, Australian Privacy Commissioner

Contents

Introduction

1. As the Australian Privacy Commissioner, I thank the Joint Committee on Intelligence and Security (the Committee) for the opportunity to comment on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Bill). The Bill proposes a data retention scheme that would require certain communications service providers to collect and store limited types of information about individuals' communications (hereinafter referred to as 'telecommunications data'). That information would include telecommunications data that is also personal information.

2. The *Privacy Act 1988* (Cth) (Privacy Act) confers a range of functions on the Australian Information Commissioner which are also conferred on the Privacy Commissioner by operation of the *Australian Information Commissioner Act 2010* (Cth).[1] In 2014, the Government signalled its intention to disband the Office of the Australian Information Commissioner (OAIC) and to maintain the statutory position of Privacy Commissioner, which will continue to carry out statutory functions under the Privacy Act and related legislation.[2] As part of that process, the Privacy Act will be amended to confer the functions under that Act on the Privacy Commissioner (the Commissioner). Those functions include:

    - examining a proposed enactment that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals,[3] and
    - ensuring that any adverse effects of the proposed enactment or the proposal on the privacy of individuals are minimised.[4]

3. In performing those functions the Commissioner is required to have regard to the objects of the Privacy Act.[5] As well as promoting the privacy of individuals, those objectives include recognising that the protection of the privacy of individuals must be balanced with the interests of entities in carrying out their functions and activities.[6]

4. These objectives are consistent with Article 17 of the *International Covenant on Civil and Political Rights*, which provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy. This has been interpreted to mean that, to the extent that there is a restriction on an individual's right to privacy, any interference must be necessary and proportionate. The Office of the United Nations

[1] See s 12 of the *Australian Information Commissioner Act 2010* (Cth) that provides that the Privacy Commissioner has the privacy functions set out in s 9 of that Act.
[2] See Hon George Brandis QC, Attorney-General for Australia, *Streamlined arrangements for external merits review,* (Media Release, 13 May 2014), available online: <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2014/SecondQuarter/13May2014-Streamlinedarrangementsforexternalmeritsreview.aspx>.
[3] See *Privacy Act 1988*, s 28A(2)(a).
[4] See *Privacy Act 1988*, s 28A(2)(c).
[5] See *Privacy Act 1988*, s 29.
[6] See *Privacy Act 1988*, s 2A.

High Commissioner for Human Rights has recently stated in relation to the right to privacy:

> *'[A] limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right … must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.'*[7]

5. In making this Submission, I recognise that the proposed data retention scheme:

   - is intended to ensure that Australian enforcement and security agencies have access to the information necessary to perform their law enforcement and national security functions
   - is intended to standardise the types of telecommunications data collected and retained by service providers to address variations in business practices, both across those providers and over time, and
   - is not intended to extend existing powers of enforcement and security agencies to access telecommunications data.[8]

   However, the proposed data retention scheme would require service providers to handle personal information in a way that may otherwise be inconsistent with those providers' obligations under the Privacy Act. For example, under Australian Privacy Principle (APP) 3 organisations, which would include some service providers covered by the proposed data retention scheme, must only collect personal information that is reasonably necessary for their functions or activities. Further, under APP 11, those providers should generally only retain personal information for as long as necessary to carry out their functions and activities. The proposed data retention scheme may result in service providers collecting more personal information than is necessary for their business purposes, and retaining that information for longer than is necessary for those purposes.

6. Accordingly, I have considered the Bill in light of the functions conferred on the Commissioner and the objectives of the Privacy Act. In particular, the comments and recommendations that I make below are intended to assist the Committee in determining whether the scheme appropriately balances the needs of Australian enforcement and security agencies to access telecommunications data with the protection of the privacy of individuals.

[7] See Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014), p23.
[8] See Explanatory Memorandum to the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Explanatory Memorandum), p3.

Executive Summary

7. The proposed data retention scheme requires service providers to collect a large volume of personal information and this has the potential to significantly impact on the privacy of individuals that use the services of those providers. I acknowledge that the intention of the scheme is to standardise the types of telecommunications data collected and retained by service providers. However, developments in communications technology mean that much more personal information will be collected and retained by all service providers under the proposed data retention scheme than is currently, and would otherwise be, collected and retained.

8. Further, while I acknowledge that the Bill limits the type of telecommunications data that service providers will be required to collect and retain to 'non-content' information, the collection and retention of such a large volume of personal information has the potential to build a detailed picture of an individual's activities, relationships and behaviours.

9. Therefore, consideration should be given to whether the intrusion upon individuals' privacy that results from the collection and retention of each kind of information is necessary and proportionate to the benefit of Australian enforcement and security agencies being able to use that information in carrying out their functions and activities. This approach will help ensure that any data retention scheme is the least privacy intrusive means of addressing the needs of Australian enforcement and security agencies, and that it is consistent with community expectations about the handling of personal information.

10. Therefore, if the Committee finds that a data retention scheme is necessary, it is important that any scheme only require service providers to:

    - collect the minimum amount of information necessary to meet those needs, and
    - retain that information for the minimum amount of time necessary to meet those needs.

11. Further, any data retention scheme must be accompanied by privacy safeguards. In that regard, I believe that further enhancements to the safeguards currently contained in the Bill are required. I outline these additional safeguards in the table of recommendations below and, in more detail, in section C of this submission, titled 'Additional privacy safeguards'.

12. In addition to these, it is critical that the data retention scheme is accompanied by a regulatory framework and a security framework that provide the necessary level of privacy protections, transparency and accountability. Given the potential for the proposed data retention scheme to significantly impact on the privacy of individuals, I consider that further enhancements to the current oversight arrangements provided for in the Bill are necessary. I outline what further enhancements I consider necessary in the table of recommendations below and, in more detail, in section D of this submission, titled 'Regulatory oversight arrangements. In section E, titled 'An appropriate security framework', I discuss the implementation of a security framework for the telecommunications sector.

13. In section F, titled 'Access to information by individuals ', I have sought to clarify for the Committee the obligations of service providers to provide individuals with access to telecommunications data under APP 12, contained in the Privacy Act.

14. Finally, in Section G, titled 'Review requirements', I discuss the content of the review of the proposed data retention scheme required to be undertaken by the Committee. Further to that, I propose the inclusion of a five year sunset provision to provide industry, enforcement and security agencies and the public with assurance that the Parliament will consider the effectiveness of the scheme and any oversight measures within a definite timeframe.

Recommendations

Recommendation 1

If the Committee finds that a data retention scheme is necessary, the scheme should only require service providers to:

i. collect the minimum amount of information necessary to meet the needs of Australian enforcement and security agencies, and

ii. retain that information for the minimum amount of time necessary to meet those needs (para 20 to 22).

Recommendation 2

The types of telecommunications data that service providers would be required to collect and retain under the proposed data retention scheme should be sufficiently clear and narrowly described to effectively implement the intentions of the scheme (para 29 to 34).

Recommendation 3

Evidence that shows why it is necessary to retain telecommunications data for a minimum of two years should be made available to the public to the extent practicable (para 35 to 44).

Recommendation 4

The retention period that applies to each type of subscriber information data be expressly set out in the Bill (para 45 to 49).

Recommendation 5

Clarification be provided about the range of services that are intended to be captured by s 187A(3), specifically:

i. when a service provider would be considered to 'operate infrastructure' in Australia, and

ii. what types of communications services it is intended will be prescribed by the regulations because they are not provided by a carrier, carriage service provider or internet service provider (para 50 to 53).

Recommendation 6

Section 187B(2) of the Bill be amended to make it clear that the Communications Access Coordinator's (CAC) power to make a declaration only relates to 'immediate circle' and 'same area' services that meet the requirements under s 187A(3)(para 56 to 59).

Recommendation 7

In the absence of a warrant-based access scheme, the Bill should amend:

i. sections 178 and 179 of Chapter 4 of the *Telecommunications Interception and Access Act 1979* (Cth) (TIA Act) to limit the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security, and

ii. section 182 of the TIA Act to ensure that telecommunications data disclosed under Chapter 4 can only be used or disclosed where it is reasonably necessary to prevent or detect a serious offence and safeguard national security (para 63 to 75).

Recommendation 8

i. Any expansion of the definition of 'enforcement agency' should be made by an amendment to the TIA Act itself (para 76 to 80).

ii. If the declaration power is retained in the Bill, regard should be had to whether there are mechanisms in place:

- for monitoring an authority or body's compliance with a binding scheme, and
- to enable individuals to seek recourse if their personal information is mishandled (para 81 to 85).

iii. Section 176(5) of the Bill be amended to include a requirement for the Commissioner to be consulted before any additional authorities or bodies are declared to be an 'enforcement agency' (para 85).

Recommendation 9

Section 187K of the Bill be amended to:

i. explicitly include 'the objectives of the Privacy Act' in the list of matters that the CAC must consider before making a decision to exempt, or vary the obligations of, a service provider, and

ii. include a requirement for the CAC to consult the Commissioner in relation to the application (para 86 to 89).

Recommendation 10

i. Service provider's implementation plans should include details of the measures the provider proposes to implement to ensure that telecommunications data that will be collected and retained under the plan is protected from misuse, interference and loss and from unauthorised access, modification and disclosure (para 90 to 92).

ii. Section 187F of the Bill be amended to require the CAC to assess those steps before making a decision about whether to approve that plan (para 93).

iii. Section 187G of the Bill be amended to include a requirement for the CAC to give a copy of the implementation plan to the Commissioner and invite the Commissioner to provide comments (para 94 to 95).

Recommendation 11

Section 187B of the Bill be amended to:

i. explicitly include 'the objects of the Privacy Act' in the list of matters that the CAC must consider before making a declaration that certain services are covered by the data retention scheme, and

ii. include a requirement for the CAC to consult with the Commissioner before making a declaration (para 96 to 98).

Recommendation 12

i. The matters which the Bill proposes to address in regulations should be provided for in the Bill itself (para 99 to 101).

ii. Alternatively, if a decision is made to continue as proposed, that:

- the Bill be amended to include a requirement for public consultation before the making, or variation, of regulations
- the Bill be amended to include a specific requirement that the Commissioner be consulted in the making of any regulations, and
- a privacy impact assessment (PIA) be undertaken before any additional types of telecommunications data, communications services or variations in the retention period are prescribed in regulations (para 102 to 104).

Recommendation 13

The Bill be amended to include a mandatory data breach notification requirement that applies to service providers covered by the proposed data retention scheme (para 105 to 111).

Recommendation 14

i. The Bill be amended to ensure that all service providers that are required to collect and retain telecommunications data under the proposed data retention scheme are subject to the Privacy Act (para 121 to 123).

ii. Alternatively, the Bill be amended to include a provision that requires all service providers to comply with binding rules made by the Commissioner in relation to the handling of personal information required to be collected and retained under the proposed data retention scheme (para 124).

Recommendation 15

Oversight of enforcement agencies' compliance with their obligations under Chapter 4 of the TIA Act rest with the Commissioner (para 125 to 127).

Recommendation 16

The proposed security framework for the telecommunications sector be in place before service providers are required to collect and retain any telecommunications data under the proposed data retention scheme (or an approved data retention implementation plan) (para 128 to 133).

Recommendation 17

The three year review of the proposed data retention scheme include a detailed consideration of:

- the types of services prescribed by the regulations, and
- whether the types of telecommunications data prescribed by the regulations is the minimum amount of personal information necessary to meet the needs of enforcement and security agencies (para 139 to 140).

Recommendation 18

The Bill be amended to include a sunset provision that the proposed data retention scheme expire five years after the end of the implementation period unless reauthorised by the Parliament (para 141 to 143).

A. The privacy impact of the proposed scheme

15. The proposed data retention scheme requires service providers to collect and retain a large volume of personal information and this has the potential to significantly impact on the privacy of individuals. The Statement of Compatibility with Human Rights (the Statement) that accompanies the Bill notes that the proposed data retention scheme will require service providers to collect and store information, including subscriber information, some of which *may* be personal information.[9] I consider that this understates the privacy impact of the proposed scheme.
16. The Privacy Act defines personal information broadly, to include any information about an identified individual or an individual who is reasonably identifiable. Whether an individual is reasonably identifiable from particular information will depend on, among other things, what other information is held about the individual.[10] This means that the types of information that will also be personal information for the purposes of the Privacy Act will not be limited to just subscriber information (such as an individual's name, date of birth and address), but will include information that can be linked to the subscriber information.

[9] See Explanatory Memorandum, p11.
[10] See Office of the Australian Information Commissioner (OAIC), *APP Guidelines* (2014) available online: http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/ (the APP Guidelines), para B.85.

17. While I appreciate that the proposed data retention scheme is intended to standardise the types of telecommunications data collected and retained by service providers, I understand that this means that some service providers will be required to collect and retain telecommunications data that they currently have no business need to collect or retain. This issue was raised by iiNet it its response to the Industry Consultation Paper[11] and is also acknowledged by the Explanatory Memorandum, which states that *'[s]ome service providers may initially need to modify their systems to ensure they meet this minimum standard'.*[12] This was further confirmed in the first hearing on the Bill held by the Committee on 17 December 2014, in which the Attorney General's Department explained that the types of data that service providers will be required to collect and retain under the scheme:

> *'are ones that are retained in the telecommunications industry but not necessarily consistently… [n]ot all providers retain all elements, but they are all retained somewhere in the industry, and it is to ensure that those particularly prescribed classes are kept'.*[13]

18. Additionally, even if the Bill effectively limits the type of information that service providers are required to collect and retain about a communication to 'non-content' information, the collection and retention of non-content information (ie, telecommunications data) may still be highly privacy intrusive. This is because telecommunications data, such as the time location and recipient of those communications, has the potential to create a detailed picture of the individual's personal life. The risk that the collection and retention of telecommunications data may significantly limit an individual's right to privacy was specifically identified by the Joint Parliamentary Committee on Human Rights in its Fifteenth Report: Examination of legislation in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011.*[14]

19. By creating a large repository of personal information, the proposed data retention scheme increases the risk and possible consequences of a data breach. This is because the challenge of effectively securing that information from misuse, interference and loss, and from unauthorised access, modification or disclosure will become more difficult as technology evolves. For example, the large volume of personal information held by service providers will be an attractive target for people with malicious and/or criminal intent. One way to help manage the impact on individuals affected by a data breach involving telecommunications data is to amend

[11] See iiNet Limited, *iiNet's response to Industry Consultation Paper – Telecommunications data retention - statement of requirements September 2014 (v 1.1)* (2014) available online: <http://www.iinet.net.au/about/mediacentre/papers-and-presentations/industry-consultation-paper-data-retention.pdf>, p3.

[12] See Explanatory Memorandum, p34.

[13] See Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, p 11, Ms Harmer Acting First Assistant Secretary, Attorney-General's Department.

[14] See Joint Parliamentary Committee on Human Rights, Parliament of Australia, *Fifteenth Report: Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011* (2014) available online: <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Completed_inquiries/2014/Fifteenth_ConReport_of_the_44th_Parliament>, para 1.34 .

the Bill to include a mandatory data breach notification requirement that applies to services providers. I discuss this option at 105 to 111below.

B. Assessing whether the data retention scheme is necessary and proportionate

20. In order to be a necessary and proportionate response to meeting the needs of Australia's enforcement and security agencies, any data retention scheme should only require service providers to:
    - collect the minimum amount of information necessary to meet those needs, and
    - retain that information for the minimum amount of time necessary to meet those needs.
21. To assess this, consideration should be given to each type of telecommunications data that service providers would be required to collect and retain. This involves balancing the intrusion upon individuals' privacy that results from the collection and retention of each type of telecommunications data with the benefit of Australian enforcement and security agencies being able to use that information in carrying out their functions and activities.
22. This approach will ensure that the collection and retention of each type of telecommunications data is a necessary and proportionate element of any data retention scheme. It will also help ensure that the scheme is the least privacy intrusive means of addressing the needs of Australian enforcement and security agencies and that it is consistent with community expectations about the handling of personal information.

Telecommunications data required to be collected and retained

23. The Bill does not set out the specific types of telecommunications data that service providers would be required to collect and retain under the proposed data retention scheme. Rather, s 187A(1) imposes an obligation on service providers to keep information 'of a kind' prescribed by the regulations or documents containing information of that kind. Subsection 187A(2) then sets out the 'kinds' of information that may be prescribed in broad terms. Importantly, s 187A(4) sets out a number of exclusions to the obligation to retain telecommunications data. In particular, s 187A(4)(a) provides that service providers are not required to keep, or cause to be kept, information that is the 'content or substance of a communication'.
24. I understand that the column titled 'Draft data set' in the document titled 'Data Retention Bill – Proposed data set'(the proposed data set document) sets out the types of telecommunications data that are currently intended to be prescribed in the regulations (the prescribed data set). I raise a number of issues about the prescribed data set, including:
    - its potential to reveal detailed information about an individual despite the exclusion of content information

- the risk that, despite the exclusion, content information may be collected and retained as a result of the proposed data retention scheme
- that the Bill and prescribed data set do not clearly describe the information that is required to be collected and retained, which:
    - makes it difficult to assess the privacy impact of the scheme as a whole, and
    - creates uncertainty that may result in service providers collecting and retaining more information than is intended to be required, and difficulties in compliance and enforcement.

The privacy impacts of collecting 'non-content' information about communications

25. As explained above, even where the telecommunications data that service providers are required to collect and retain is not the content or substance of communications, it can still reveal detailed information about an individual and be highly privacy intrusive. For example:
    - Appendix A summarises the outcomes of two studies into the privacy impacts of collecting, retaining and analysing non-content telecommunications data.
    - Appendix B considers the privacy impacts of collecting location data, in particular location data associated with Short Message Service (SMS) messages.

Risk of inadvertent collection of content

26. It is unclear whether the proposed data retention scheme may, in some circumstances, necessitate the collection of the content of communications in order for service providers to ensure that they comply with their obligations under that scheme.
27. Subsection 187A(4) sets out a number of exclusions to the obligation to retain telecommunications data. In particular, s 187A(4)(a) provides that service providers are not required to keep, or cause to be kept, information that is the 'content or substance of a communication'. However, some types of communications are delivered in a way that makes it difficult to distinguish between the content of a communication and information about that communication.
28. For example, in general, internet-based communications are delivered as a single stream of data. I understand that, with respect to unencrypted communications, it is possible to automatically extract telecommunications data from the data stream, making it possible to retain the telecommunications data without also retaining the content. However, it is unclear how service providers will comply with their obligations where the communication has been encrypted. In that scenario, the practical result may be that the service provider retains the entire encrypted communication, including the encrypted content, in order to ensure that they retain the telecommunications data.

Description of the data set

29. I consider that the description of the types of telecommunications data in the prescribed data set may create a risk that types of data that are not intended to be collected and retained under the data retention scheme may be captured. This is because the types of telecommunications data in the prescribed data set are not clearly and narrowly defined. This, in turn, makes it difficult to assess the privacy impact of the proposed data retention scheme as a whole.

30. Given the wide variety of technologies and communications channels that would be covered by the proposed data retention scheme, it is important that clear, specific, consistent and unambiguous language is used in:

    - the Bill to describe the kinds of information that service providers may be required to collect and retain under that scheme, and
    - the regulations to describe each specific type of telecommunications data in the prescribed data set.

31. By way of example, in Appendix C, I have identified a number of instances in which I consider that s 187A(2), the prescribed data set or the Explanatory Memorandum should be amended to enhance clarity and specificity, or remove inconsistencies.

32. Without further clarification, these ambiguities could create:

    - difficulties in assessing the privacy impacts of the proposed data retention scheme, and whether it is a necessary and proportional response to the needs of Australian enforcement and security agencies
    - uncertainty for regulated service providers that results in the collection and retention of types of data that are not intended to be collected and retained under the proposed data retention scheme, and
    - difficulties in compliance for service providers and enforcement for regulators.

33. Accordingly, consideration should be given to whether each kind of information that may be prescribed under s 187A(2), and each specific type of telecommunications data in the prescribed data set is sufficiently clear and narrowly described to effectively implement the specific intentions of the proposed data retention scheme, and facilitate compliance with and enforcement of the scheme. This may require a reconsideration of the scope and effect of the exclusion in s 187(4)(a), or further limitations on the kinds or types of telecommunications data that may be or will be required to be collected and retained under the proposed data retention scheme.

34. Additionally, I am mindful that the telecommunications data that is prescribed in the regulations will, to a large extent, determine the scope and privacy impact of the proposed data retentions scheme. I make recommendations in relation to the making of regulations at 99 to 104 below.

The retention period

The length of the retention period

35. As discussed above, to ensure that the data retention scheme is a necessary and proportionate response to meeting the needs of Australian enforcement and security agencies, the scheme should only require service providers to retain telecommunications data for the minimum amount of time necessary to meet those needs.

36. Publicly available evidence, including evidence put forward by Australian enforcement and security agencies, provides some evidence to suggest that a data retention scheme with a retention period of up to one year may be necessary to enable those agencies to investigate serious offences and threats to national security. However, in assessing whether this evidence does, in fact, support some form of data retention scheme, the evidence should be considered in light of the impact on the privacy of individuals who will be affected by the scheme.

37. The evidence put forward by Australian enforcement and security agencies, including evidence provided to the Committee at the hearing on 17 December 2014, states that telecommunications data that is less than one year old is used in a large proportion of investigations. Specifically, the Australian Federal Police (AFP) made submissions to the Committee about the central role that telecommunications data plays in the majority of their investigations.[15] Further, the Australian Security Intelligence Organisation (ASIO) submitted to the Committee that 90% of the telecommunications data obtained by ASIO is less than 12 months old.[16]

38. However, the case for a longer data retention period is less clear. This may be because the Committee has been provided with evidence that supports a longer retention period but which has not been released publicly.[17] For example, the Explanatory Memorandum provides that 'enforcement and national security agencies advise that a data retention period of two years is appropriate to support critical investigative capabilities'[18], but does not go on to provide or cite evidence for that advice. In addition, no other specific quantitative evidence for the necessity of the two year retention period has been provided in the Statement or Explanatory Memorandum.

39. With respect to the international experience with similar retention schemes, the Explanatory Memorandum states:

> *'The proposed two year period draws on international experience in relation to the use and value of telecommunications data and achieves a balance between*

[15] See Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, p 3, Mr Colvin, Commissioner, Australian Federal Police.

[16] See Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, p 21, Ms Hartland, Director General, Australian Security and Intelligence Organisation.

[17] See, for example, Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, p 5, Ms Hartland, Director General, Australian Security and Intelligence Organisation.

[18] See Explanatory Memorandum, p 19.

supporting the operational requirements of agencies and minimising privacy impacts associated with the retention of data.'[19]

40. In that respect, I note that the Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness (SECILE) report *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*[20] found a lack of quantitative evidence to support the effectiveness of data retention schemes in the European Union (EU). That reports notes that in 2013 EU member states that supported the data retention directive, including Austria, Ireland, Italy, the United Kingdom and Spain, were unable to provide statistical data that demonstrated the effectiveness of the scheme.[21]

41. The evidence provided to the Committee by enforcement and security agencies is consistent with the experience of similar data retention schemes in international jurisdictions. For example, in 2013 the European Commission found that, amongst EU member states:

- approximately 67% of requests by investigators for communications data related to communications made in the three months prior to the request
- approximately 89% of requests related to communications made in the six months prior to the request, and
- approximately 11% of requests related to communications that were 6-12 months old.[22]

42. However, the experience with similar data retention schemes in international jurisdictions has not produced quantitative evidence that supports the proportionality of a two year retention period.

43. Accordingly, on the information available to me, it is not clear whether a retention period of two years is the minimum amount of time necessary to meet the needs of enforcement and security agencies.

44. I recommend that the Statement clearly set out evidence that shows why it is necessary to retain telecommunications data for a minimum of two years (or, in the case of certain subscriber information, for longer periods). If that is not practicable because of confidentiality or security reasons, then it may be open to the Committee to request and consider the evidence that establishes the necessity of the retention of each of the kinds of data proposed to be collected and retained, and the length of the retention period for each kind of data. The Committee could then communicate to the public that it has considered that evidence, and state the Committee's conclusions.

---

[19] See Explanatory Memorandum, p 18.

[20] See Jones and Hayes, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy* (2014) SECILE, available online: <http://secile.eu >.

[21] See Jones and Hayes, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy* (2014) SECILE, available online: <http://secile.eu>, p 32, including footnote 138.

[22] See European Commission, *Evidence for necessity of data retention in the EU* (2013) available online: <http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf>, p 7.

The retention period for subscriber information

45. Subsection 187C(1) of the Bill provides that the retention period for subscriber information, (that is, information of a kind specified by s187A(2)(a)) is the life of the account plus two years. Subsection 187C(2) then enables regulations to prescribe that certain types of subscriber information are only to be retained for two years, or some other maximum period.

46. I acknowledge that the stated purpose of the longer retention period is to ensure that information about the relevant subscriber associated with an account is available throughout the life of the account, and for as long as any records relating to communications sent using that account are retained.[23] However, it is not clear that it is necessary for the Bill to require each type of subscriber information set out in s 187A(2)(a) to be retained for the life of the account plus two years.

47. The Explanatory Memorandum describes the types of telecommunications data intended to be captured by s 187A(2)(a) as including:

    - 'billing and payment information'
    - 'information about an account, telecommunications device, or other relevant service that is or has been associated with a relevant service, which may include:
        - any information relating to contracts, plans, agreements or arrangements relating to the relevant service, or to any related account, service or device
        - any identifiers, either permanent or transient, that the service provider uses in relation to the account, device or relevant service'
    - 'the status of the relevant service or any related account, service or device', and
    - 'any quantitative data about the capacity or use of the account of the relevant service or a related account, service or device.'[24]

    It is not clear why each of these types of telecommunications data are required to be retained for the life of the account plus two years as a default.

48. In addition, the proposed data set document states that it is intended that the regulations will limit the retention period for items 1 (c) to (f) of the prescribed data set to two years. Given that intention is made clear in the proposed data set document, there does not appear to be a compelling reason for that limitation not to be contained in the Bill.

49. Therefore, I recommend that the retention period that applies to each type of telecommunications data described in s 187A(2)(a) be expressly set out in the Bill.

Services covered by the data retention scheme

50. To provide certainty about which service providers will be required to collect and retain telecommunications data under the proposed data retention scheme, and to

[23] See Explanatory Memorandum, p 48.
[24] See Explanatory Memorandum, pp 37 and 38.

assess the privacy impacts of the scheme, it should be easy to ascertain the types of services to which the scheme applies.

51. Subsection 187A(3) defines the types of services that are covered by the proposed data retention scheme. I understand that there are three requirements that must be satisfied before a service will be covered:

    - first, the service must be for carrying a communication or enabling a communication to be carried by means of guided or unguided electromagnetic energy (which I understand is used for making most communications)
    - second, the service must be operated by a carrier (which includes a carriage service provider, CSP), an internet service provider (ISP) or a person prescribed by the regulations, and
    - third, the carrier, CSP, ISP or person operating the prescribed service must own or operate infrastructure in Australia that enables the provision of any service that it provides that is covered by the scheme.

52. I appreciate that s 187A(3) is broadly framed to ensure that the proposed data retention scheme is able to remain up-to-date with changes in technology, business practices and the law enforcement and national security threat landscape. However, I consider that this may result in confusion about what services are intended to be covered by the data retention scheme. In particular, what services that operate 'over-the-top' (OTT) of other services that carry communications are covered by the scheme.[25]

53. Therefore, I recommend that clarification be provided about the range of services that are intended to be captured by s 187A(3), specifically:

    - when a service provider would be considered to 'operate infrastructure' in Australia, and
    - what types of communications services it is intended will be prescribed by the regulations because they are not provided by a carrier, CSP or ISP.

Additional services prescribed by regulation

54. I am also mindful that the volume of telecommunications data that is required to be collected and retained under the proposed data retention scheme may depend, to a large extent, on what services are prescribed by the regulations. For example, the inclusion of OTT web-based email services may significantly increase the amount of email telecommunication data that is collected and retained. Further, as technology and communications services evolve, additional services may be prescribed that significantly affect the amount and nature of the telecommunications data collected and retained under the scheme.

[25] The Statement of Compatibility with Human Rights that accompanies the Bill suggests that the scheme is intended to apply to certain OTT services, including Voice over Internet Protocol (VoIP), instant messaging and e-mail. However, I understand that there are a broad range of other OTT services; for example, social networking services, web-based instant messaging services, image sharing services and communication channels in online-gaming platforms; see the Explanatory Memorandum, p 41.

55. I make recommendations in relation to the making of regulations at 99 to 104 below.

Services not covered by the data retention scheme

56. Section 187B(1) provides that the proposed data retention scheme will not apply to certain services. The Explanatory Memorandum explains that the intention of this section is to exclude services that are not provided to the general public (for example, services provided by a university, corporation or government agency) and services that are provided in a single place (such as free wi-fi services in a cafe or restaurant). However, these exclusions can be overridden by the Communications Access Coordinator (CAC) who, under 187B(2), may declare that the obligations of the proposed data retention scheme apply to a service.

57. The Explanatory Memorandum states that:

> *'subsection 187B(2) will provide that the CAC can declare that the provider of an 'immediate circle' or 'same area' service (as defined in subsection 187B(1)) is nevertheless required to retain telecommunications data in relation to the relevant services according to the requirements of subsection 187A(1).'*[26]

58. However, as currently worded, the subsection gives the CAC a general power to declare that the obligations of the data retention scheme apply to any service, irrespective of whether the service meets the three requirements of s 187A(3). Therefore, I recommend that s 187B(2) be amended to make it clear that the CAC's power to make a declaration only relates to services that meet the requirements of s 187A(3), but that would otherwise be excluded under s 187B(1).

59. I have made some further recommendations about the exercise of this declaration power in the 'Regulatory oversight arrangement' section below.

C. Additional privacy safeguards

60. Given the privacy impact of any form of data retention scheme, such a scheme must be accompanied by privacy safeguards.

61. In making the comments below, I appreciate that the Bill does provide for some additional safeguards – specifically, limiting the agencies that may authorise the disclosure of telecommunications data by a service provider and the creation of a new oversight regime administered by the Commonwealth Ombudsman. Nonetheless, I consider that further enhancements to these safeguards are required.

62. In addition to appropriate oversight and security arrangements (which are discussed in more detail at paras 112 to 133), these further safeguards should include:

    - limiting the purpose for which an authorisation can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security

[26] See Explanatory Memorandum, p 66.

- a requirement to consult the Commissioner before declaring any additional authorities or bodies to be an 'enforcement agency'
- a requirement for the CAC to consult the Commissioner and to consider the privacy impact of the decision before exercising a discretion to:
    - exempt, or vary, the obligations of certain service providers under the proposed data retention scheme
    - approve a data retention implementation plan, or the amendment of such a plan, and
    - declare that the data retention scheme applies to a service
- a requirement for the Commissioner to be consulted before the making, or variation, of any regulations affecting the proposed data retention scheme, and
- a mandatory data breach notification requirement that requires service providers to notify the Commissioner and any affected individuals if they experience a data breach that involves telecommunications data collected and retained under the scheme, in line with Guidelines made by the Commissioner.

Authorisations made under Chapter 4 of the TIA Act by enforcement agencies

63. I am mindful that there has been a large amount of public discussion, including in submissions made to this Committee, about whether there is a need for access to telecommunications data to be on the basis of a warrant issued to the relevant enforcement agency by a court or tribunal. Further, that these discussions centre around the potentially intrusive nature of telecommunications data that service providers would be required to be collect and retain under the proposed data retention scheme. While I do not advocate for warrant based access in this submission, these concerns require careful consideration.

64. The Explanatory Memorandum notes the greater privacy sensitivity of stored communications, which reveal the content and substance of a person's discussions with others, relative to telecommunications data (that is, information other than the content of the communication).[27] However, as I explain above, telecommunications data (that is, information about an individual's communications), such as the time, location and recipient of those communications, has the potential to be used to create a detailed picture of the individual's personal life.

65. The Joint Parliamentary Committee on Human Rights noted:

> *'The term 'data' is undefined in the TIA Act. Because of the significant developments in technology since the TIA Act was passed, the types of data that can now be accessed without a warrant is considerably broader than was the case when the access provisions under the TIA Act were enacted.*[28]

[27] See Explanatory Memorandum, p 66.

[28] See Joint Parliamentary Committee on Human Rights, Parliament of Australia, *Fifteenth Report: Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011*

66. The blurring of the distinction between telecommunications data and the content of the communications means that additional oversight is necessary. However, consideration needs to be given to whether a warrant scheme, similar to that which applies to accessing stored communications, is the most appropriate form for this additional oversight to take.

67. In particular, consideration should be given to whether a requirement to obtain a warrant on an investigation-by-investigation basis would impose a disproportionate burden on the ability of enforcement and security agencies to perform their legitimate functions when balanced with the impact on individuals' privacy that would occur in the absence of such a requirement. Factors to consider might include:

    - the role of telecommunications data in the investigative processes of Australian enforcement and security agencies
    - the current number of authorisations made for access to telecommunications data and the resource requirements of obtaining a warrant for a similar number of authorisations
    - the additional workload of the Australian judiciary, and
    - other oversight measures that might be implemented to safeguard privacy.

    I note that these issues were also raised in the evidence given to this Committee by representatives of the AFP, the Australian Crime Commission and ASIO at the hearing on 17 December 2014.[29]

68. There has also been discussion of an alternative requirement for enforcement and security agencies to obtain a 'generic' warrant to access telecommunications data. This was discussed at the hearing on 17 December 2014, where an example was given of a warrant to authorise access to telecommunications data for all terrorism investigations.[30] I do not consider that such a generic warrant regime (as discussed at the hearing) would provide the necessary level of scrutiny to be effective to increase the current level of oversight of the disclosure of telecommunications data.

69. However, in the absence of a warrant-based access regime, and recognising the changing nature of communications technology and the telecommunications data that it creates, I consider that it is essential that the Bill be amended to limit the purpose for which telecommunications data may be used and disclosed.

(2014) available online: <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Completed_inquiries/2014/Fifteenth_ConReport_of_the_44th_Parliament>, para 1.47.

[29] See Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, pp 17 to 20, Ms Hartland, Director General, Australian Security and Intelligence Organisation; Mr Colvin, Commissioner, Australian Federal Police; Mr Dawson, Chief Executive Officer, Australian Crime Commission.

[30] See Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, pp 18, Ms Hartland, Director General, Australian Security and Intelligence Organisation; p 18.

Limitation on the purposes for which telecommunications data may be used or disclosed

70. Currently, an enforcement agency may make an authorisation under Chapter 4 of the TIA Act in relation to any investigation where it is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.[31] The Bill does not propose to change this statutory threshold.

71. However, while the proposed amendment to the definition of 'enforcement agency' (discussed in more detail at 76 to 85 below) will help ensure that only agencies that have functions involving the investigation of serious offences and threats to national security have access to telecommunications data, it will not ensure that the purpose of that access is always to enable the exercise of one of those functions. Where an enforcement agency has a range of functions, including functions that involve the investigation of minor offences, there is nothing in Chapter 4 that would prevent the agency authorising the disclosure of telecommunications data where it is satisfied that it is necessary for the investigation of a minor offence.

72. This concern was raised by the Joint Parliamentary Committee on Human Rights in its *Fifteenth Report: Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011*, which recommended that the Bill amend Chapter 4 of the TIA Act to circumstances where it is necessary for the investigation of certain serious offences.[32]

73. In the absence of a warrant-based access scheme, I recommend that Chapter 4 of the TIA Act should be amended to limit the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security. Further, that once an authorisation has been made and information has been disclosed, that the use and further disclosure of that information be limited to the original purpose of the authorisation.

74. In saying this, I am aware that s 182 of the TIA Act already creates an offence for the unlawful use and disclosure of information disclosed under Chapter 4. However, I note that the exemptions to this offence remain quite broad and would not prevent telecommunications data being used or disclosed where it is reasonably necessary for the investigation of a minor offence. Given the volume of information that would be available to enforcement agencies under the data retention scheme, and the potential that this has to significantly impact upon the privacy of individuals, I consider that additional limitations on use and disclosure are necessary. These limitations are particularly important in relation to enforcement agencies that are not subject to the protections afforded by the Privacy Act, or a binding scheme that provides a comparable level of privacy protection, such as some state or territory police forces.

[31] See *Telecommunications (Interception and Access) Act 1979,* ss 178 and 179.

[32] See Joint Parliamentary Committee on Human Rights, Parliament of Australia, *Fifteenth Report: Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011* (2014) available online: <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Completed_inquiries/2014/Fifteenth_ConReport_of_the_44th_Parliament>, para 1.49.

75. With this in mind, I recommend that the Bill should amend:

- sections 178 and 179 of Chapter 4 of the TIA Act to limit the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security, and
- section 182 of the TIA Act to ensure that telecommunications data disclosed under Chapter 4 can only be used or disclosed where it is reasonably necessary to prevent or detect a serious offence and safeguard national security.

The definition of 'enforcement agency'

76. Only an 'enforcement agency' within the meaning of the TIA Act can authorise the disclosure of telecommunications data under Chapter 4 of that Act. The Bill amends the definition of 'enforcement agency' to include only those bodies with responsibility for investigating or enforcing serious criminal offences and authorities or bodies declared by the Minister by legislative instrument.

77. In view of the large volume of personal information that will be available to enforcement agencies under the proposed data retention scheme and public concern about that information being accessed for the investigation of relatively minor offences or civil matters,[33] it is appropriate that access to this information should be restricted to bodies with responsibility for investigating serious offences. I therefore welcome the amendment of the definition of 'enforcement agency' to include only those bodies with responsibility for investigating or enforcing serious criminal offences.

Declarations by the Minister

78. Under the proposed s 176A(3) the Minister may, by legislative instrument, declare an authority or body to be an enforcement agency. A declaration will, therefore, be subject to two levels of scrutiny, ministerial and parliamentary.

79. Given public concern about telecommunications data being accessed for the investigation of relatively minor offences, I consider that it is more appropriate that any expansion of the definition of 'enforcement agency' is made by an amendment to the TIA Act itself. A similar view was expressed by the Senate Standing Committee for the Scrutiny of Bills:

[33] See, for example, Professor George Williams, Civil Liberties Australia, *Holes in metadata bill make it unacceptable*, 5 January 2015, available online: <http://www.cla.asn.au/News/metadata-bill-holey-unacceptable/>; Roger Clarke, *Data Retention as Mass Surveillance: The Need for an Evaluative Framework*, 27 November 2014, available online: <http://www.rogerclarke.com/DV/DRPS.html#ASD>; Alex Achlotzer, Electronic Frontiers Australia, *Five things we learned about the Government's data retention regime in 2014,* 11 January 2015, available online: <https://www.citizensnotsuspects.org.au/five-things-about-data-retention/>.

> *'[G]iven the highly intrusive nature of the scheme, it may be considered that any expansion of the agencies that can* access *telecommunications data should be determined by Parliament not legislative instrument.'*[34]

80. As an alternative, that Committee suggested that the disallowance process for this type of ministerial declaration be amended to require the scrutiny of each house of Parliament. Although my preferred approach would be for any amendment to the definition to be made by an amendment to the TIA Act, I consider that this could offer an alternative approach.

Additional scrutiny of the types of 'enforcement agencies'

81. If the declaration power is retained in the Bill, there should be additional and ongoing scrutiny of the types of authorities and bodies that are declared to be 'enforcement agencies' under the TIA Act.

82. Whether an authority or body should be an enforcement agency will depend upon a range of factors, including whether the authority or body is subject to appropriate privacy oversight in relation to its handling of personal information. This is reflected in s 176A(4), which sets out the matters that the Minister must have regard to when deciding to make a declaration. Those matters include whether the authority or body is required to comply with:

- the Australian Privacy Principles (APPs)
- a binding scheme that provides a comparable level of protection to personal information as the APPs, or
- has agreed in writing to comply with such a scheme in relation to personal information disclosed under Chapter 4 of the TIA Act.[35]

83. While I welcome the inclusion of this provision, I consider that regard should also be had to whether such a binding scheme provides a mechanism:

- for monitoring the authority or body's compliance with the scheme, and
- to enable individuals to seek recourse if their personal information is mishandled.

84. In saying this, I appreciate that the Minister can revoke a declaration that an authority or body is an enforcement agency if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force (such as where a body declared to be an enforcement agency is shown to have failed to comply with such a scheme). In that respect, I consider that such mechanisms may assist the Minister in exercising that discretion.

[34] See Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Alert Digest No 16 of 2014* (2014) available online: <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Alerts_Digests/2014/index>, p 6.

[35] See the Bill, s 176A(4)(c).

85. In addition, to assist the Minister in considering the matters in s 176A(4)(c), I recommend that s 176(5) of the Bill be amended to require the Commissioner to be consulted before making a declaration under s 176A(3).

Functions of the Communications Access Co-ordinator

Discretion to exempt (or vary the obligations of) certain service providers from the data retention scheme

86. Subsection 187K(1) of the Bill permits the CAC to exempt a service provider from some or all of the obligations under the proposed data retention scheme, or to vary those obligations. The Statement asserts that this exemption facility indirectly strengthens the right to privacy of individual customers in that it provides a method of reducing data retention obligations.[36] However, the process for making an exemption or variation does not build in consideration of the privacy impact. Therefore, while I support the inclusion of a mechanism to exempt certain service providers from some or all of the obligations under the proposed data retention scheme, I recommend that this process be amended to ensure that the privacy interests of individuals are considered in the decision to exempt, or vary the obligations of, a service provider, and that the Commissioner is consulted.

87. I understand that, where a service provider applies to the CAC for an exemption or variation, the CAC is required to give certain enforcement agencies and security authorities a copy of the application before making a decision (s 187K(5)). The CAC may also give the Australian Communications and Media Authority (the ACMA) a copy of the application.

88. The CAC is also required to take into account the matters listed in s 187K(7) before making a decision. I note that those matters focus on the interests of law enforcement and national security, the telecommunications industry and the service provider. While the CAC is required to take into account the objects of the *Telecommunications Act 1997* (Cth) (Telecommunications Act), which includes the long-term interests of end-users of carriage services, there is no explicit obligation to take into account the impact on the privacy of individuals.

89. Given the volume and sensitivity of personal information that service providers may be required to collect and retain under the proposed data retention scheme, and the Commissioner's responsibility for overseeing the handling of that information by service providers subject to the Privacy Act, I recommend that s 187K of the Bill be amended to:

    - explicitly include 'the objectives of the Privacy Act' in the list of matters that the CAC must consider before making a decision to exempt, or vary the obligations of, a service provider, and
    - include a requirement for the CAC to consult the Commissioner in relation to the application.

[36] See Explanatory Memorandum, p 18.

Approve a data retention implementation plan or an amendment of such a plan

90. If the Bill is passed, 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.

91. Under s 187E(2), an implementation plan must specify details of the existing practices of the service provider in relation to the collection and storage of telecommunications data, and details of interim arrangements that the service provider proposes to implement prior to achieving full compliance with the proposed data retention scheme. 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. Consistent with my recommendations below, this will ensure that the appropriate security protections are in place before service providers are required to collect and store any additional information under the scheme (or an approved data retention implementation plan).

92. However, it is not clear to me on the face of the Bill, and from reading the Explanatory Memorandum,[37] that these details are required to be included in an implementation plan under the current wording of s 187E(2). To address this, the Explanatory Memorandum could be amended to include further details of the type of information service providers should include in an implementation plan. This will also help provide greater certainty and clarity to service providers when drafting implementation plans.

93. It follows that the CAC should be required to take these security measures into account when deciding whether to approve an implementation plan. To achieve this, I recommend amending s 187F of the Bill, which sets out the matters that the CAC must take into account before making a decision to approve an implementation plan, to require the CAC to assess the steps that the service provider proposes to take to protect the information from misuse, interference and loss and from unauthorised access, modification and disclosure.

94. I understand that under s 187G, as with applications for exemptions, the CAC is required to give certain enforcement agencies and security authorities, and may also give the ACMA, a copy of the implementation plan and invite them to provide comments on the plan to the CAC. Further, if the enforcement agency or security authority requests an amendment to the implementation plan that the CAC considers is reasonable, the CAC is required to request the service provider to make that amendment. If the service provider does not accept the amendment, the request for amendment is referred to the ACMA for determination.[38]

95. Given that the Commissioner is responsible for ensuring that service providers covered by the Privacy Act comply with their obligations under that Act, including their security obligations under APP 11.1, I recommend that s 187G be amended to

[37] See Explanatory Memorandum, p 50.
[38] See the Bill, s 187G.

include a requirement for the CAC to give a copy of the implementation plan to the Commissioner and invite the Commissioner to provide comments.

Declare that the data retention scheme applies to a service that a service provider operates

96. As discussed above, under s 187B(2) of the Bill, the CAC has a power to declare that certain services are covered by the data retention scheme.

97. When exercising that declaration power, the CAC is required to take certain matters into account. Like the CAC's power to exempt a service provider from some or all of the obligations under the proposed data retention scheme, those matters focus on the interests of enforcement and security agencies, the telecommunications industry and the service provider. While the CAC is required to take into account the objects of the Telecommunications Act there is no explicit obligation to take into account the impact on the privacy of individuals.

98. If this declaration power is retained in the Bill in its current form, I recommend that s 187B of the Bill be amended to:

- explicitly include 'the objects of the Privacy Act' in the list of matters that the CAC must consider before making a declaration that certain services are covered by the data retention scheme, and
- include a requirement for the CAC to consult with the Commissioner before making a declaration.

Regulation making powers

99. The Bill allows for regulations to be made that affect the scope of the data retention scheme. Specifically, regulations relating to:

- the services covered by the data retention scheme
- the kinds of telecommunications data that service providers will be required to collect and retain, and
- the retention period that applies to each item of telecommunications data of a kind in s 187A(2)(a).

100. I appreciate that the intention of these regulation-making powers is to ensure that the proposed data retention scheme is sufficiently flexible to adapt to rapid and significant future changes in communications technology and industry practices. Further, consistent with my recommendations above, I appreciate that each item of the prescribed data set needs to be described clearly and narrowly, and that this requires a level of technical detail that may be uncommon in primary legislation. However, as set out above, each of these regulation-making powers has the potential to substantially affect the privacy impact of the proposed data retention scheme. For this reason, considered together with the significant amount of public concern that has been expressed about the scope of the scheme, I believe that it would be more appropriate for these matters to be addressed in the Bill itself.

101. A similar view was expressed by the Senate Standing Committee for the Scrutiny of Bills:

> *'Again, although the Committee accepts that regulation-making powers are in some cases justified by the necessity to build in scope for flexible regulatory responses to changing circumstances, how this scheme—which is highly intrusive of individual privacy—should be applied in a new technological context is a matter which will raise significant questions of policy that are not appropriately delegated by the Parliament to the executive government'*.[39]

102. However, if a decision is made to continue as proposed, I make the following recommendations:

- that the Bill be amended to include a requirement for public consultation before the making, or variation of, regulations. I consider that such a requirement will add certainty and clarity to, and increase community confidence in, the proposed data retention scheme[40]
- given the responsibilities conferred on the Commissioner, which includes oversight of service providers handling of personal information, that the Bill should be amended to include a specific requirement that the Commissioner be consulted in the making of any regulations, and
- given the privacy impact that may result from the exercise of these particular regulation-making powers, that a privacy impact assessment (PIA) should be undertaken before any additional types of telecommunications data, communications services or variations in the retention period are prescribed.[41]

103. Finally, I agree with the suggestion made by the Implementation Working Group that 'any proposed future changes to the regulations should only come into effect after Parliament has had an opportunity to review the proposal and the disallowance period has expired'.[42]

---

[39] See Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Alert Digest No 16 of 2014* (2014) available online: <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Alerts_Digests/2014/index>, p 3.

[40] Legislative instruments are subject to the consultation requirements in Part 3 of the *Legislative Instruments Act 2003.* However, s 18 of that Act provides for a number of circumstances where consultation may be unnecessary or inappropriate. For example, where an instrument is required as a matter of urgency or where an instrument is required because of an issue of national security.

[41] A PIA is a written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. The OAIC has published a guide to undertaking Privacy Impact Assessments, see OAIC, *Guide to undertaking privacy impact assessments*, (2014), available online: <http://www.oaic.gov.au/privacy/privacy-archive/privacy-resources-archive/privacy-impact-assessment-guide>.

[42] See Data Retention Implementation Working Group, *Report 1 of the Data Retention Implementation Working Group* (2014), Australian Government, Attorney General's Department, Recommendation 5.

Existing precedent for a requirement that the Commissioner be consulted in the making of regulations, codes or other legislative instruments

104. There are existing precedents for a requirement that the Commissioner be consulted in the making of regulations, both in the TIA Act itself and in other legislation. I have outlined some of these precedent below:

- Under s 183(3) of the TIA Act the CAC must consult the Information Commissioner before making a determination that prescribes additional requirements that relate to the form of authorisations made under Chapters 3 and 4 of the TIA Act.
- Under s 134 of the Telecommunications Act, the ACMA must consult the Commissioner before determining or varying an industry standard that relates to privacy and before revoking such an industry standard.
- Under s 100 in the Privacy Act, before the Governor General makes regulations under APP 9.3, prescribing an organisation or class of organisations that can handle government related identifiers, the Governor General must be satisfied that the Commissioner has been consulted. This consultation requirement is included because the making of such regulations would authorise the organisation to handle government identifiers where they would otherwise not be permitted by the APPs.
- Under s 6F of the Privacy Act, before the Governor General makes regulations prescribing that a state or territory authority or instrumentality be treated as an organisation for the purpose of the Privacy Act, the Governor General must consult the Commissioner about the desirability of that authority or instrumentality being subject to the Privacy Act.
- Under s 85ZZ(1)(b) of Part VIIC of the *Crimes Act 1914*, which establishes the Commonwealth spent convictions scheme, it is a function of the Commissioner to advise the Minister whether an exclusion to that scheme should be given and whether there should be any restrictions on the circumstances in which an exclusion would apply.

A mandatory data breach notification requirement

Data breach notification under the Privacy Act

105. APP 11 provides that entities covered by the APPs (APP entities) must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. While notification of data breaches to the Commissioner and affected individuals may be a reasonable step to protect personal information under APP 11, it is not an express requirement under the Privacy Act. Therefore, our office accepts data breach notifications for APP entities on a voluntary basis. The OAIC has published a guide to voluntary data

breach notification, which provides general guidance for agencies and organisations when responding to a data breach involving personal information that they hold.[43]

Mandatory data breach notification

106. As I explain above, the proposed data retention scheme would require service providers to collect and retain a large volume of information, including personal information, and that this has the potential to be highly intrusive. By way of example, Appendices A and B also include a discussion of the potential privacy impacts of the collection and retention of that information, including the potential for telecommunications data to reveal a detailed picture of a person's personal life. Accordingly, telecommunications data retained under the scheme is likely to be a target for people with malicious or criminal intent. In the event of a security breach resulting in unauthorised access to or disclosure of telecommunications data, affected individuals would face increased risks of identity theft, fraud, harassment or embarrassment. I note that 46% of breaches in Australia during 2013 were attributable to malicious or criminal attacks, which were the most prevalent cause of data breaches.[44]

107. There has been an upward trend in the voluntary notification of data breaches to our office.[45] This is consistent with national and global trends that also reflect an increase in the number and severity of data breaches.[46]

108. Further, I note that Australian service providers have experienced significant issues in handling and keeping personal information secure. Major telecommunications services providers that will be covered by the scheme are amongst the 20 entities most complained about to our office. Further, since 2010, major telecommunications companies have been the subject of 13 Commissioner's own motion investigations, including:

- a 2011 incident in which the personal information of 734,000 customers was inadvertently made available online,[47] and
- a 2013 incident in which the subscriber information of 15,775 customers, including over 100 silent line customers, was inadvertently made available online.[48]

[43] See OAIC, Data breach notification — A guide to handling personal information security breaches (2014), available online: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.

[44] See Ponemon Institute, *2014 Cost of Data Breach Study* (2014), available online: <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>, p 8.

[45] See OAIC, *Annual Report 2013-14* (2014), available online: <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance#s6>, p 93.

[46] See Verizon, *2014 Data Breach Investigations Report*, available online: <http://www.verizonenterprise.com/DBIR/2014/>, p 8.

[47] See OAIC, *Telstra Corporation Limited: Own motion investigation report* (2012), available online: <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited>.

[48] See OAIC, *Telstra Corporation Limited: Own motion investigation report* (2014), available online: <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014>.

In both instances, the relevant service provider was found to have breached the APPs.

109. Notification is an important mitigation strategy for individuals affected by a data breach. Specifically, notification can enable individuals to take steps to reduce their exposure to risks, which cannot be taken by other entities. For example, an individual may be able to change credit card numbers or seek to have compromised identifiers reissued.

110. Given the volume and sensitivity of information to be collected and retained under the proposed data retention scheme, I recommend that the Bill should be amended to include an obligation for service providers to notify the Commissioner and affected individuals in the event that they experience a data breach affecting telecommunications data collected and retained under the scheme (and where other appropriate conditions are met, such as where the data breach could give risk to a real risk of serious harm to affected individuals[49]).

111. When considering the possibility of a mandatory notification requirement, the Committee may wish to consider the following:

- In its 2008 report *For your information: Australian privacy law and practice*, the Australian Law Reform Commission recommended that the Privacy Act be amended to introduce a mandatory data breach requirement.[50] In making that recommendation, the ALRC considered a number of different notification mechanisms and international examples.
- A mandatory data breach notification requirement has since been introduced under s 75 of the *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act) relating to unauthorised collection, use or disclosure of health information included in a consumer's eHealth record, or where the security of the PCEHR system has been or may be compromised. This offers another possible model of how a mandatory data breach notification obligation could be implemented.

D. Regulatory oversight arrangements

112. In addition to the enhanced privacy safeguards discussed above, it is critical that the proposed data retention scheme is accompanied by a regulatory framework that provides the necessary level of privacy protections, transparency and accountability.

113. I believe that the following characteristics are central to an effective privacy regulatory framework:

[49] See OAIC, Data breach notification — A guide to handling personal information security breaches (2014), available online: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.

[50] See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report No 108 (2008), Recommendation 51-1, available online: <http://www.alrc.gov.au/publications/51.%20Data%20Breach%20Notification/alrc%E2%80%99s-view>.

- consistency in the standards that regulate how personal information should be handled across different entities
- transparent consultation in relation to any variation of those standards, and
- centralised oversight of the handling of personal information across different entities.

These characteristics will help to ensure a holistic approach to regulation, increase regulatory certainty, ensure administrative simplicity and improve transparency.

114. In light of these observations and given the significant impact on privacy that may result from the introduction of the proposed data retention scheme, I consider that further enhancements to the current oversight arrangements provided for in the Bill are necessary. I recommend that the Bill be amended to:

- ensure that all service providers that are required to collect and retain telecommunications data under the scheme should be subject to the Privacy Act or required to comply with binding rules made by the Commissioner in relation to the handling of personal information, and
- give the Commissioner oversight of enforcement agencies compliance with Chapter 4 of the TIA Act.

Oversight of service providers

115. As explained above, I do not consider that the Bill clearly states what communications services will be covered by the proposed data retention scheme under s 187A(3). This means that it is not possible to identify, with certainty, which service providers will be required to collect and retain telecommunications data. Without this clarity, it will be difficult for the Commissioner to identify which service providers covered by the Privacy Act are also covered by the proposed data retention scheme, and to monitor those providers' handling of telecommunications data.

116. Importantly, different service providers may be subject to different levels of oversight in relation to their handling of personal information collected and retained under the proposed data retention scheme. For example, service providers that are also APP entities within the meaning of the Privacy Act will be required to handle any personal information that they collect and retain in accordance with the APPs. However, not all service providers are APP entities. An APP entity includes most Australian Government (and Norfolk Island Government) agencies and some private sector organisations. Importantly, some small businesses with an annual turnover of $3 million or less ('small business operators'; SBOs) and State or Territory authorities (or prescribed State instrumentalities) are not APP entities and are generally not subject to the APPs.[51]

117. The Telecommunications Industry Ombudsman has advised me that, as at 13 December 2014, 1254 ISPs and CSPs were members of its scheme. Of those members, only 85 were the subject of 25 or more complaints during the 2013-14

[51] See *Privacy Act 1988*, s 6 (definition of 'agency') and s 6D.

financial year. Based on the relatively low number of complaints received by most of the TIO's members, and the substantial direct engagement the TIO has with its members as part of its complaint handling and industry outreach activities, the TIO suggests that a large proportion of members have comparatively small customer bases, and therefore a proportion of those members may be SBOs for the purpose of the Privacy Act. This is supported by a market share analysis; in 2014, just three service providers – Telstra, Vodafone, and Optus/Singtel – held approximately 74% of the Australian telecommunications market, with the remaining 26% being split between a large number of smaller service providers.[52]

118. While some State or Territory authorities may be subject to State or Territory based privacy legislation, not all jurisdictions have their own privacy legislation, including Western Australia and South Australia.

119. I also acknowledge that SBOs that are also CSPs will be required to comply with the *Telecommunications Consumer Protections Code*, registered under Part 6 of the Telecommunications Act by the ACMA, which has powers to enforce compliance with the Code. Paragraph 4.6.3 of that Code includes obligations in relation to CSPs' storage and security of personal information. However, the obligations in that Code do not cover the full range of matters covered by the APPs and do not enable individuals to seek recourse if their personal information is mishandled by the service provider. Further, the Code does not apply to SBOs that are not CSPs but that may be covered by the proposed data retention scheme, such as ISPs and other service providers that operate services prescribed by regulations under s 187A(3)(b)(iii).

120. As the Bill is intended to standardise the types of telecommunications data that are collected and retained by service providers, the protections and oversight that apply to the handling of that information should also be standardised. I recommend two alternative options for standardising the protections that apply to service providers below. If adopted, both options will result in the Commissioner having oversight of compliance with those protections. I consider that this is appropriate because:

- the Commissioner is already responsible for the oversight of a large proportion of service providers that will be required to comply with the data retention scheme, and
- the responsibilities conferred on the Commissioner by the Privacy Act provide the necessary expertise and experience in privacy regulation, including in the regulation of the telecommunications industry and online services.

Option 1: Bringing all service providers under the jurisdiction of the Privacy Act

121. To ensure that all service providers apply the same standards of protection when handling personal information collected and retained under the proposed data retention scheme, I recommend that all service providers that are not APP entities

[52] See The Australian, *Cashed up Vodafone looks for mergers*, 11 February 2014, available online: <http://www.theaustralian.com.au/business/companies/cashed-up-vodafone-looks-for-mergers/story-fn91v9q3-1226824111497>, original data via <www.ibisworld.com.au>.

be brought within the jurisdiction of the Privacy Act. For the following reasons, I consider that the Privacy Act is the most appropriate mechanism to ensure that telecommunications data, that is also personal information, is afforded the necessary level of protection:

- the Privacy Act is the privacy oversight mechanism with which the public is most familiar and, therefore, reflects current community expectations about the handling of personal information, and
- the Privacy Act, as principles-based legislation, is flexible enough to accommodate the information handling practices of the diverse range of service providers (both in terms of their size and business models) that would be subject to the proposed data retention scheme whilst still providing a minimum level of privacy protection.

122. There is precedent for this recommendation in both the *Anti-Money Laundering/Counter Terrorism Financing Act 2006* (Cth) (AML/CTF Act) and the *Healthcare Identifiers Act 2010* (Cth) (Healthcare Identifiers Act). I have outlined this precedent below:

- Under s 6E(1A) of the Privacy Act small businesses that are reporting entities for the purposes of AML/CTF Act are required to comply with the Privacy Act when handling personal information collected for the purposes of complying with obligations under the AML/CTF Act and the AML/CTF Rules. This includes small businesses that may be exempt from obligations under the Privacy Act in terms of any other business activities they undertake.
- Under s 29(2) of the Healthcare Identifiers Act, State and Territory authorities are treated as organisations (and therefore bound by the Privacy Act) for certain purposes.

123. Applying these two examples in the context of the data retention scheme:

- a provision similar to the current s 6E(1A) of the Privacy Act could be inserted into the Privacy Act; this provision could require SBOs that are subject to the proposed data retention scheme to comply with the APPs when handling any information that they collect and retain in accordance with the scheme, and
- a provision analogous to s 29(2) of the Healthcare Identifiers Act could be inserted into the Bill; this provision could require that service providers that are also State or Territory authorities be treated as organisations when any handling personal information that they are required to collect and retain under the proposed data retention scheme.

Option 2: Compliance with binding rules made by the Commissioner

124. If Option 1 is not adopted, I recommend that the Bill be amended to include a provision that requires all service providers to comply with binding rules made by the Commissioner in relation to the handling of personal information required to be collected and retained under the proposed data retention scheme. Further, that a breach of those rules constitute an interference with the privacy of an individual under s 13 of the Privacy Act. This would ensure that there is consistent protection

and oversight of service providers handling of telecommunications data and that individuals' have access to appropriate remedies if their personal information is mishandled.

Oversight of enforcement agencies

125. I welcome the creation of the additional oversight powers to assess enforcement agencies' compliance with Chapter 4 of the TIA Act.

126. I understand that these powers have been conferred on the Commonwealth Ombudsman because of the Ombudsman's existing responsibilities relating to the oversight of enforcement agencies. In particular, the Ombudsman has existing audit functions to assess enforcement agencies' compliance with the record keeping and destruction requirements in relation to the issuing of preservation notices and access to stored communications under Chapter 3 of the TIA Act.

127. However, for the following reasons I recommend that oversight of enforcement agencies' compliance with their obligations under Chapter 4 of the TIA Act should rest with the Commissioner:

- When combined with the Commissioner's existing oversight responsibilities, namely:
    - oversight of service providers' handling of telecommunications data, and
    - responsibility under s 309 of the Telecommunications Act to ensure that carriers and CSPs are keeping appropriate records of authorisations made by enforcement agencies under Chapter 4, and
    - oversight of enforcement agencies handling of information disclosed under Chapter 4 of the TIA Act for those enforcement agencies that are also APP entities (including, for example, the AFP and Customs)

  these oversight powers would enable the Commissioner to monitor the handling of telecommunications data collected and retained under the proposed data retention scheme throughout its lifecycle – that is, from collection to disclosure to destruction. Centralising oversight of the handling of telecommunications data in this way will ensure that there is a holistic approach to oversight of the scheme, improve transparency and ensure administrative simplicity.
- The Commissioner has the expertise required to understand and address the privacy impacts that may arise from the handling of the large volume of personal information that would be available to enforcement agencies if the Bill is passed.
- The Commissioner has existing processes and procedures necessary for assessing enforcement agencies' compliance with Chapter 4 of the TIA Act.

E. An appropriate security framework

128. The Bill does not prescribe how the retained communications data is to be stored or any specific security standards that service providers must implement to ensure that the information that they are required to collect and store under the proposed data

retention scheme is adequately protected. Further, the Bill does not include any mechanism for prescribing such standards or requirements.

129. The Statement notes that service providers already have arrangements for the storage and protection of this information consistent with their existing obligations under the Privacy Act or applicable state or territory privacy legislation.[53] However, as I explain above, different service providers may be subject to different levels of oversight in relation to their handling of personal information, including different security standards. Consistent with my comments above, given that the scheme is intended to standardise the types of telecommunications data that is collected and retained by service providers, and the potential for this to significantly impact on the privacy of individuals, the security measures that protect that information should also be standardised at a level that is commensurate with the risk to privacy.

130. The Government has acknowledged the need for additional protection, as indicated by the following statement made by Communications Minister, Malcolm Turnbull, in his second reading speech for the Bill:

> *'[T]he government is considering reforms to strengthen the security and integrity of Australia's telecommunication infrastructure by establishing a security framework for the telecommunications sector. This will provide better protection for information held by industry in accordance with the data retention scheme. The government expects this reform will be finalised well before the end of the data retention implementation period.'*[54]

131. Further to this, the Statement indicates that the *Telecommunications and Other Legislation Amendment Bill 2014* will implement these reforms by introducing a new obligation on carriers and CSPs to do their best to prevent unauthorised access and unauthorised interference to telecommunications networks and facilities, including where a carrier or CSP outsources functions. The Statement explains that these reforms are intended to complement the protections which already exist in the Privacy Act.[55] However, I am not aware of that Bill being tabled in Parliament and have not been consulted on a draft version of that Bill. Given the Commissioner's responsibility for oversight of service providers' handling of information collected and retained in compliance with the data retention scheme, where those providers are subject to the Privacy Act, I would welcome the opportunity to provide input into the development of any additional security obligations. In that respect, I note that the OAIC has recently published a *Guide to securing personal information* to help agencies and organisations to meet their obligations under the APPs to take reasonable steps to protect personal information.[56]

---

[53] See Explanatory Memorandum, pp 12-13.

[54] Malcolm Turnbull, Member for Wentworth - Minister for Communications, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Second Reading Speech*, 30 October 2014,<http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F4a3ea2e7-05f5-4423-88aa-f33e93256485%2F0010%22>

[55] See Explanatory Memorandum, p 13.

[56] See OAIC, *Guide to securing personal information* (2015), available online: <http://www.oaic.gov.au/news-and-events/news/privacy-news/guide-to-securing-personal-information>.

132. Further, while I support the establishment of a security framework for the telecommunications sector, I consider that this framework should be in place before service providers are required to collect and store any information under the proposed data retention scheme (or an approved data retention implementation plan). If this is not possible, my recommendation that the Bill be amended to require a service provider's data retention implementation plan to specify, in relation to each service, the steps that the provider will take to protect the information become essential.

133. In addition, as is discussed above, any security framework for the telecommunications sector (and any security systems and procedures included in a data retention implementation plan) should include a mandatory data breach notification requirement.

F. Access to information by individuals

134. I understand that some service providers are concerned about the impact that the proposed data retention scheme may have on their existing obligation under the Privacy Act to provide individuals with access to their personal information.[57] For example, in the first hearing on the Bill held by the Committee on 17 December 2014, the Communications Alliance stated that *'we are concerned about the precedent that may be set that enables hundreds of thousands or more individuals to demand access to their metadata'*.[58] In light of these concerns, I have taken this opportunity to clarify service providers' obligations under APP 12.

135. Organisations within the meaning of the Privacy Act are required to comply with the APPs when handling personal information that they collect and retain. If the Bill is passed, this will include personal information collected and retained in compliance with the proposed data retention scheme by service providers covered by the Privacy Act. APP 12 requires those service providers to give an individual access to any personal information that the provider holds about the individual on request, subject to certain exceptions (such as where giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body).[59] APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

136. Under APP 12, an organisation may impose a charge on an individual for giving access to their personal information, provided the charge is not excessive. The OAIC's APP guidelines explain that items that may be charged for include:

    - staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to the individual

[57] See *Privacy Act 1988*, Australian Privacy Principle 12.
[58] See Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, p 11, Mr Stanton CEO, Communications Alliance.
[59] See *Privacy Act 1988*, Australian Privacy Principle 12.3.

- staff costs in reproducing and sending the personal information
- costs of postage or materials involved in giving access, and
- costs associated with using an intermediary.[60]

137. Whether a charge is excessive will depend on the nature of the organisation, including the organisation's size, resources and functions, and the nature of the personal information held. Importantly, a charge by an organisation for giving access must not be used to discourage an individual from requesting access to personal information. The following are examples of charges that may be considered excessive:

- a charge that exceeds the actual cost incurred by the organisation in giving access
- a charge that reflects shortcomings in the organisation's information management systems. An individual should not be disadvantaged because of the deficient record management practices of an organisation.

138. I believe that APP 12 provides a balanced approach to ensuring individuals are able to gain access to their personal information whilst also recognising the operational requirements of organisations.

G. Review requirements

139. I support the requirement in s 187N for the Committee to review the operation of the data retention scheme 3 years after the end of the implementation period. However, given that the scope and the privacy impact of the proposed data retention scheme is determined, to a large extent, by the regulations, I suggest that it should be clear that the review should include a detailed consideration of:

- the types of services prescribed by the regulations, and
- whether the of the types of telecommunications data prescribed by the regulations is the minimum amount of personal information necessary to meet the needs of enforcement and security agencies.

140. This clarity could be provided in the Explanatory Memorandum to the Bill.

141. In addition, I recommend that the Bill should be amended to include a sunset provision that the proposed data retention scheme expire five years after the end of the implementation period unless reauthorised by the Parliament. This would take effect two years after the review of the scheme, thereby giving Parliament time to consider the outcome of that review.

142. I consider that the inclusion of a sunset clause will provide industry, law enforcement and security agencies and the public with assurance that the Parliament will consider the effectiveness of the scheme and any oversight

[60] See the OAIC's APP Guidelines, Chapter 12, available online: <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-12-app-12-access-to-personal-information>, paragraphs 12.77-12.81.

measures within a definite timeframe. Further, it will also provide those stakeholders with assurance that they will have a further opportunity to comment on the necessity and proportionality of any data retention scheme that is implemented.

143. Finally, that five year period will provide enforcement and security agencies and industry with an opportunity to collect further quantitative evidence about the necessity for a data retention scheme in Australia. For example, evidence about the age of any telecommunications data used in the investigation of serious offences and threats to national security.

Appendix A – summaries of studies into the privacy impacts of collecting 'non-content' information about communications

1. In one recent experiment, security researchers were able to develop an accurate and highly detailed profile of an individual from a single week's worth of telecommunications data (but excluding content of communications), including:
    - determining the individual's place of employment, position, and work habits (such as the times of his arrival and departure from work, what time he eats lunch, when during the evening he responds to work emails, when he goes to bed)
    - determining the individual's personal interests
    - inferring the individual's political opinions
    - determining the individual's travel routes to and from his place of employment
    - inferring a social network based on the individual's phone and e-mail records, including identifying his romantic partner and close friends, and information about those individuals, and
    - comparing the individual's telecommunications data to leaked information from high profile data breaches, thereby enabling them to crack his social networking passwords and online shopping accounts.[61]
2. Similarly, in the Stanford Law School Centre for Internet and Society's Metaphone study, using only telephone call telecommunications data spanning a few months, researchers were able to:
    - accurately identify the romantic partners of target individuals[62]
    - develop accurate and detailed social maps illustrating the social networks and connections of individuals,[63]
    - infer sensitive details about individuals, including:
        - religious views
        - political opinions
        - health problems including, in certain cases, inferring that an individual had been diagnosed with multiple sclerosis and where they were being

[61] Dimitri Tokmetzis, *How your smartphone passess on almost your entire life to the Secret Service,* translated from the original Dutch, available online: <http://www.statewatch.org/news/2014/jul/bits-of-freedom-on-the-metadata-of-your-phone.pdf>

[62] Jonathan Mayer and Patrick Mutchler, *Metaphone: Seeing Someone?*, 27 November 2013, available online: <http://webpolicy.org/2013/11/27/metaphone-seeing-someone/>

[63] Jonathan Mayer and Patrick Mutchler, *Metaphone: The NSW Three-Hop,* 9 December 2013, available online: <http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/#more-579>

treated, and that another individual had scheduled and received an abortion.[64]

3. See also the discussion of the privacy impacts of collecting and analysing location data associated with SMS messages, in Appendix B, and the discussion of dynamic IP address allocation logging and Network Address Translation logs, in Appendix C.

4. Further, in December 2013, Fairfax Media commissioned NCG Group to analyse metadata captured from an email address belonging to Senator David Leyonhjelm, with the Senator's permission. In accordance with the proposed data retention scheme, NCG Group did not consider the content of communications, or web browsing data. With the remaining communications data, and using off-the-shelf software tools, NCG Group was able to accurately infer, amongst other things:

   - that Senator Leyonhjelm was planning a trip to the Whitsunday Islands, including the airline and hotel that the Senator was planning to use
   - the Senator's interest in hunting and gun laws, and the identities of individuals interested in the reform of gun laws
   - the times when the Senator was in his office.[65]

[64] Jonathan Mayer and Patrick Mutchler, *Metaphone: The Sensitivity of Telephone Metadata,* 12 March 2014, available online: <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>

[65] Mark White, The Sydney Morning Herald, *What we found when we captured Senator David Leyonhelm's metadata,* available online: <http://www.smh.com.au/technology/technology-news/what-we-found-when-we-captured-senator-david-leyonhjelms-metadata-20141219-1242rf.html>

Appendix B – the privacy impacts of collecting location data associated with SMS messages

Scope of the data set with respect to location information

1. The data set may require the collection of types and amounts of information that would enable, or be equivalent to, real-time location monitoring.

2. The proposed data set document makes it clear that it is not the intention of the proposed data retention scheme to enable location monitoring:

   '…the location records to be kept by service providers will not allow continuous monitoring or tracking of devices… [p]recise or real-time location information, such as GPS location is also not part of data retention'.

3. Item 6 of the prescribed data set is 'the location of the equipment or line used to send or receive a communication at the start or end of that communication'. The Explanatory Memorandum describes this kind of information as '[t]he physical and logical location of the line, equipment or telecommunications device used to send or receive a communication'.[66] The Explanatory Memorandum further explains that '[e]xamples include cell tower locations and public wireless local area network (WLAN) hotspots'.

4. The proposed data set document states that '[l]ocation records will be limited to the location of a device at the start and end of a communication, such as a phone call or SMS message'. That document also states that '[t]his would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication'.

5. However, even location information limited to that described above may reveal detailed information about the movements, location and, as a consequence, information about the behaviours of individuals at a level approaching the equivalent effect of real-time location tracking. By way of example, I consider below trends and behaviour in SMS messaging, and how the collection of location information associated with SMS messaging alone could approach the equivalent effect of real-time location monitoring.

Case study – location information associated with SMS messages

6. SMS messaging (via cellular telephone networks, as opposed to internet-based messaging services) is an extremely popular communications channel, with some demographics sending up to 100 messages a day:

   - In 2012, Telstra's 13.8 million customers[67] (representing approximately 46% of Australia's 30.2 million mobile services at that time[68]) sent 12.05 billion SMS

[66] See the Explanatory Memorandum, page 42.
[67] See *Telstra Corporation Limited and controlled entities Director's Report for the year ended 3 June 2014*, available online: <http://asx.com.au/asxpdf/20120809/pdf/427xrwkp2nstyp.pdf>, p 2.

messages. In 2013, this figure was approximately 13.5 billion; equating to 37 million text messages a day.[69]

- International research strongly suggests that this usage is dominated by younger users:
  - In 2010, American teenagers aged 13-17 were found to send on average 3,339 SMS messages a month, or 6 SMS messages per waking hour.[70]
  - Similarly, a study by the Pew Research Centre in 2012 found that American phone users aged 14-17 were sending and receiving 181 SMS messages a day on average.[71]
  - In 2014, Experian found that American phone users aged 18 to 24 sent 67 SMS messages and received 61 SMS messages per day,[72] at a relatively consistent rate during waking hours.[73]

7. The Explanatory Memorandum and the prescribed data set suggest that the location data associated with SMS messages that could be collected under s 187A(2) would be the location of the relevant cell tower or wi-fi hotspot.[74] However, it is not clear whether service providers may or will be required to retain information about signal strength or whether devices are within range of multiple cell towers; this information could be used to determine location to within several metres using signal triangulation techniques.

8. The example above shows how even if the collection of location information was restricted to the sending and receiving of SMS messages, this could still result in the collection of up to 100 points of location data per day. Over a period of 2 years, this would reveal a great deal of information about an individual's movements and behaviours and, could, itself achieve a level approaching an equivalent effect to real-time tracking.[75] The impact would be increased if that information as combined with location information from other kinds of communications, such as emails sent from a home or work computer, or calls made from a home or work fixed line phone.

---

[68] See ACMA, *Communications Report 2011-2012*, available online: <http://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/communications-report-2011-12>, p 8.

[69] See Greg McCall, *20 years of Telstra*, 27 April 2013, available online: <http://exchange.telstra.com.au/2013/04/26/20-year-of-telstra/>

[70] See Neilsen, *US teen mobile report calling yesterday, texting today, using apps tomorrow*, 14 October 2010, available online: <http://www.nielsen.com/us/en/insights/news/2010/u-s-teen-mobile-report-calling-yesterday-texting-today-using-apps-tomorrow.html>

[71] See Pew Research Centre, *Teens, Smartphones & Texting*, 19 March 2012, available online: <http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Teens_Smartphones_and_Texting.pdf>, p 12.

[72] See Experian, *2013 Digital Marketer Report*, available online: <http://www.experian.com/marketing-services/2013-digital-marketer-report.html?WT.srch=PR_EMS_DMReport_020813_DMReport%22>, p 103.

[73] See Experian, *2013 Digital Marketer Report*, available online: <http://www.experian.com/marketing-services/2013-digital-marketer-report.html?WT.srch=PR_EMS_DMReport_020813_DMReport%22, p 104.

[74] See the Explanatory Memorandum, p 42; proposed data set document, item 6.

[75] See, for example, this visualisation of cell tower information collected over 6 months: <http://www.zeit.de/datenschutz/malte-spitz-data-retention>.

Appendix C - Examples of suggested amendments to s 187A(2), the prescribed data set and the Explanatory Memorandum

1. This Appendix identifies a number of instances in which I consider that s 187A(2), the prescribed data set or the Explanatory Memorandum should be amended to enhance clarity and specificity, or remove inconsistencies.

Section 187A(2)

2. Section 187A(2) sets out the 'kinds' of information that may be prescribed by regulation under s 187A(1) as information that service providers are required to collect and retain under the proposed data retention scheme.
3. Section 187A(2)(a) states that these kinds of information include characteristics of any of the following:
   - the subscriber of a relevant service
   - an account relating to a relevant service
   - a telecommunications device relating to a relevant service, and
   - another relevant service relating to a relevant service.

Characteristics

4. The term 'characteristics' is a broad term that could be interpreted to include a range of information. The Explanatory Memorandum attempts to clarify the meaning of this term by providing that this kind of information may include 'Internet Protocol (IP) addresses, port numbers or other network identifiers which may be used on a permanent or transient basis', and acknowledging that service providers may also need to retain network address translation (NAT) logs.[76] It is not clear whether these examples are intended to be exhaustive. Without further clarification, there is a risk that service providers may collect and retain information additional to that intended to be required under the proposed data retention scheme.

'Related' to a relevant service

5. It is unclear from the Bill, the prescribed data set, and the Explanatory Memorandum when an account, device or service is 'related' to a relevant service.

[76] Network address translation (NAT) is a method of translating IP addresses from one network to another. For example, each ISP with its own network will allocate users a temporary IP address. However, when a user sends a message out of that private network it will use NAT to convert that temporary IP address into a public IP address. When the response comes back, the ISP can use NAT to translate the public IP address back to the allocated temporary IP address (even if that temporary address has changed) to direct the response back to the user.

6. The Explanatory Memorandum provides that this kind of information may include '[i]nformation about an account, telecommunications device, or other relevant service that is or has been associated with a relevant service, including identifiers, either permanent or transient, that the service provider uses in relation to the account'.[77] However, it is also unclear what 'associated' means in this context.

7. For example, the majority of modern mobile devices are able to access the internet, and are able to share that internet connection (via, for example, wi-fi or Bluetooth connections) with other devices. Where a user temporarily shares their phone's internet connection (being a relevant service) with another device, and then that other device is used to send communications, it is not clear on the face of the Bill, the prescribed data set or Explanatory Memorandum whether the other device would be considered to 'relate to' or be 'associated with' the relevant service.

The source of the communication

8. Section 187A(b) of the Bill states that the kinds of information that service providers may be required to collect and retain include information relating to the source of a communication. Item 2 of the prescribed data set is '*[a]ny* identifiers of a related account, service or device from which the communication has been sent by means of the relevant service' [emphasis added]. This is a high level and broad description that could create uncertainty when applied to communications sent via the internet.

9. The proposed data set document provides that '[t]he source of a communication includes the phone from which a call was made, the account from which an email was sent or the IP address allocated to a person connected to the internet'. Similarly, the Explanatory Memorandum provides that '[a]n example of an identifier of the source of a communication is a telephone number'.[78] These examples do not adequately address the uncertainties raised by the numerous internet-based communications which use multiple identifiers. For example, identifiers of a related account, service or device from which an email has been sent could include:

   - the email address of the sender, analogous to a telephone number
   - the URL address of the source mail server via which the email was sent
   - the IP address of that source mail server address, and
   - the addresses of intermediary mail servers that act as message transfer agents, through which the email passed on its way to its destination.[79]

10. It is unclear from the Bill, proposed data set document or the Explanatory Memorandum which of these identifiers would be considered to be the 'source of the email communications' or 'a related account, service or device from which the email has been sent' and, therefore, be required to be collected and retained by service providers.

[77] See the Explanatory Memorandum, p 37.
[78] See the Explanatory Memorandum, p 39.
[79] See, for example: <http://www.fraudaid.com/images/headers/head12.gif>

11. More specificity is needed in the Bill, prescribed data set and/or the Explanatory Memorandum, particularly for the most common internet–based communications channels, such as email.

12. I note that this issue has been considered by the Data Retention Working Group. Recommendation 4 of the Working Group's first Report is:

> *'Against the background of the desirability of certainty to support industry implementation and the necessity of retention of all relevant identifiers to support communications attribution, the IWG recommends that the Government change the phrase "any identifiers" in items 2 and 3 of the data set to "identifiers". Additionally the IWG saw merit in developing additional explanatory material providing specific examples of the application of data set elements in relation to identifiers across a selection of current service types.'*[80]

13. I agree that the Working Group's recommendation and proposed explanatory material would add clarity to the scope of item 2 of the prescribed data set. However, it would be more desirable if the scope of item 2 was clear on the face of the prescribed data set.

The destination of the communication

14. Section 187A(c) of the Bill states that the kinds of information that service providers may be required to collect and retain include information relating to the destination of a communication. Item 3 of the prescribed data set is:

> *'Any identifiers of the account, telecommunications device or relevant service to which the communication:*
>
> *(a) has been sent; or*
>
> *(b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.'*

15. As discussed above with respect to item 2, similar issues arise in relation to identifying the 'destination' of communications delivered via the internet.

End-point of a communication, or transitional points?

16. The proposed data set document explains that '[t]he destination of a communication is the recipient'.

17. The proposed data set document further explains that the 'destination' of a communication includes 'destinations for online services, such as the user name, number and/or IP address of a Voice over IP (VoIP) call'. As with the example of the 'source' of emails discussed above, it is unclear whether identifiers of transitional servers used to deliver VoIP calls would also be required to be retained.

[80] See Data Retention Implementation Working Group, *Report 1 of the Data Retention Implementation Working Group*, available online: <http://www.aph.gov.au/DocumentStore.ashx?id=f261eba5-534c-4627-906c-a1bdd142b394, p 8.

18. Further, the Explanatory Memorandum is inconsistent in its description of the destination of a communication. For example, page 14 of the Explanatory Memorandum provides examples of the destination of a communication, namely 'telephone numbers and e-mail addresses'. However, page 40 provides:

> *'This kind of information may include any identifiers allocated to an account, telecommunications device or service to which a communication is sent. An example would be the* ***identifiers of an e-mail server*** *used to deliver an e-mail to its recipient/s'* [emphasis added].

19. An email server is a transitional point for an email, rather than a final destination; the intended recipient of an email will generally be unable to access the email until it has been accessed on, or downloaded from the email server to a computer or other device. By analogy, this is equivalent to recording the location of the post office to which a letter is transported, prior to its delivery to the address on the envelope.

20. In that respect, the Bill, prescribed data set and Explanatory Memorandum would benefit from amendment to clarify whether the Bill intends that the end-point of a communication be retained, or that information about the servers via which an email or other communication has passed on its way to the destination email address also be retained and, if so, to what extent.

21. I note that this issue has been considered by the Data Retention Working Group. The Working Group proposes adding explanatory text to the proposed data set document relating to item 3 of the prescribed data set:.

> *'In all instances, the identifiers retained to identify the destination of the communications are the ones relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider'*.[81]

22. I consider that the Working Group's proposed explanatory material would add clarity to the scope of item 3 of the prescribed data set. However, it would be more desirable if the scope of item 3 was clear on the face of the prescribed data set.

[81] See Data Retention Implementation Working Group, *Report 1 of the Data Retention Implementation Working Group*, available online: <http://www.aph.gov.au/DocumentStore.ashx?id=f261eba5-534c-4627-906c-a1bdd142b394, p 3.