7

Safeguards and oversight

Introduction

7.1 The Committee accepts the need for a mandatory data retention scheme, and notes it is of critical importance that any such regime includes appropriate safeguards to ensure accountability and protect the privacy of individuals.

7.2 Strengthening safeguards and privacy in line with community expectations was one of the objectives of the Attorney-General's Department's 2012 discussion paper, *Equipping Australia against emerging and evolving threats,* which formed the basis for this Committee's 2012-2013 inquiry into reforms to national security legislation.

7.3 On the basis of the discussion paper, the Committee examined matters relating to privacy protection and oversight arrangements during that inquiry. Some of the Committee's conclusions and recommendations are reflected in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill).

7.4 In this chapter, the Committee examines specific safeguards and oversight mechanisms set out in the Bill. In particular, the role of the Commonwealth Ombudsman is significantly expanded, with the Ombudsman empowered to inspect, inquire into and report on the issuing of preservation notices and agencies' access to stored communications and telecommunications data.

7.5 The chapter also examines matters raised in evidence that are outside the scope of the Bill, but which were addressed by the Committee in the previous inquiry, including a mandatory data breach notification scheme.

Commonwealth Ombudsman

7.6 This section sets out the elevated role of the Commonwealth Ombudsman and the enhanced safeguards and oversight arrangement that will apply in relation to Chapters 3 and 4 of the TIA Act.

7.7 In its 2013 report, the Committee noted the limitations of the existing regime and broad support expressed by submitters for a revised oversight arrangement. The Committee recommended that a review of the oversight arrangements under the TIA Act be undertaken by the Attorney-General's Department and, in relation to any mandatory data retention legislation, that it include *inter alia*:

> oversight of agencies' access to telecommunications data by the ombudsman and the Inspector-General of Intelligence and Security.[1]

7.8 Some of the identified limitations of the existing arrangement include:

- no oversight regime for Commonwealth, State and Territory enforcement agencies accessing telecommunications data,
- the Commonwealth Ombudsman's role in relation to preservation notices and access to stored communications is limited to monitoring compliance by agencies with their record destruction and record-keeping obligations, and
- no public reporting obligation.[2]

7.9 The Committee notes that the regime proposed in the Bill was developed in consultation with the Commonwealth Ombudsman's office.[3]

7.10 According to the Explanatory Memorandum, the proposed provisions in Schedule 3, including powers, scope and reporting obligations:

> are intended to enable the Ombudsman to provide public assurance and to enhance levels of transparency and public accountability.[4]

---

1 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* Canberra, May 2013, pp. 19-22, 192.

2 Commonwealth Ombudsman, *Submission 74,* p. 2.

3 Ms Katherine Jones, Deputy Secretary, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 3.

4 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum,* p. 81.

Overview of provisions

7.11 The Bill amends the TIA Act to establish a record-keeping, inspection and oversight regime relating to:

- the issue of preservation notices by criminal law-enforcement agencies,
- the access to, and dealing with, stored communications by criminal law-enforcement agencies, and
- the access to, and dealing with, telecommunications data by criminal law-enforcement agencies and enforcement agencies.[5]

7.12 In evidence to the Committee, the Commonwealth Ombudsman noted that while the Bill expands the Ombudsman's role in relation to Chapters 3 and 4, it will not affect his role in relation to Chapter 2 of the TIA Act, which remains limited to assessing compliance with destruction and record keeping requirements.[6]

7.13 The proposed amendments will require Commonwealth, State and Territory enforcement agencies to keep prescribed information and documents necessary to demonstrate that they have exercised their powers under Chapters 3 and 4 in accordance with their obligations under the TIA Act. Proposed sections 151 and 186J list the information or records that must be retained in some detail. The Explanatory Memorandum explains that:

> the specificity of the oversight provisions is intended to provide sufficient clarity to enable agencies to be properly versed as to what the Ombudsman would require to be kept and made available at inspections.[7]

7.14 An agency must retain the relevant documents for a period of three years or until the Ombudsman reports to the Minister under section 186J.

7.15 A proposed new Division 1 will replace existing Divisions 1 and 2 of Part 3-5 of the TIA Act and a new Chapter 4A will set out the Ombudsman's role and powers. Proposed section 186B will require the Commonwealth Ombudsman to inspect the records of an enforcement agency. In doing so, the Ombudsman's powers will include:

---

5 Data Retention Bill, *Explanatory Memorandum*, p. 80.

6 Mr Colin Neave, Commonwealth Ombudsman, *Committee Hansard,* Canberra, 29 January 2015, p. 42.

7 Data Retention Bill, *Explanatory Memorandum*, p. 80.

- full and free access to all records of the agency relevant to the inspection, including the power to take copies of or extracts from records,
- access to premises, and
- requiring staff of an agency to give the Ombudsman any information in the staff member's possession or that they have access to that is relevant to the inspection.

7.16 The Ombudsman also has the power to obtain information either in writing or by requiring an officer to answer questions, and there are penalties for failure to comply. Further, a person cannot be excused on the basis that they might incriminate themselves or make themselves liable to a penalty.

7.17 The Ombudsman must report to the Minister at the end of each financial year and must present his or her report to the Parliament.

7.18 The proposed regime is similar to that contained in Part 6 of the *Surveillance Devices Act 2004*.

7.19 The Explanatory Memorandum states:

> Tailored oversight provisions in relation to the use by agencies of preservation notices and their access to and dealing with stored communications are important inclusions in the Bill because:
>
> - the use of preservation notices by criminal law-enforcement agencies potentially impacts on individual privacy, in that agencies can use such notices to ensure that carriers and carriage service providers preserve the private stored communications of persons where the agency intends to later apply to for a stored communications warrant to access those communications in connection with the investigation of a serious contravention, and
> - the access to and dealing with stored communications by criminal law-enforcement agencies also potentially impacts on individual privacy. As such, it is important that access to, and dealing with, such communications occurs only as permitted under the TIA Act.[8]

Matters raised in evidence

7.20 The Commonwealth Ombudsman, Mr Colin Neave, commented on the proposed regime, advising the Committee that:

8 Data Retention Bill, *Explanatory Memorandum,* p. 85.

> Overall, we support the proposed provisions regarding the expanded and additional oversight functions for the Commonwealth Ombudsman, under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*, regarding the preservation and access to stored communications and access to telecommunications data. The proposed emphasis of the inspection roles and reporting requirements align with the work that we presently do in the office. The minister to whom we report—and this is a provision we support—must also table in parliament my report on the results of our inspections, thus making it publicly available.[9]

7.21 Mr Neave went on to state that:

> we are satisfied that the design of the oversight functions proposed by the bill are sufficient for my office to provide the expected level of assurance that agencies are meeting their obligations in complying with powers under Chapters 3 and 4 of the act.[10]

7.22 Finally, Mr Neave emphasised to the Committee that his office has 'the necessary expertise and experience to perform the functions.'[11]

7.23 However, while the Ombudsman's office has the requisite expertise and experience, Mr Neave also told the Committee that it does not have the resources necessary to perform this additional role. Mr Neave explained that:

> Over the past 10 years the Ombudsman's presence in the area of overseeing agencies' use of covert, coercive and intrusive powers has grown significantly. We no longer just investigate matters of administration on complaint or on our own motion of action taken by the majority of Australian government agencies. The role of providing public assurance that agencies are using their intrusive powers as parliament intended is a key function of the Commonwealth Ombudsman. This oversight is extremely important, for, unlike the matters about which my office receives complaints, the public would not—and in most cases should not—

9 Mr Colin Neave, Commonwealth Ombudsman, *Committee Hansard,* Canberra, 29 January 2015, p. 42.

10 Mr Colin Neave, *Committee Hansard,* Canberra, 29 January 2015, p. 42.

11 Mr Colin Neave, *Committee Hansard,* Canberra, 29 January 2015, p. 42. See also, Commonwealth Ombudsman, *Submission 74*, p. 1.

> have knowledge of agencies undertaking these covert and intrusive activities.
>
> Under nine different regimes authorising these types of powers, during a financial year my office currently oversees approximately 20 Commonwealth, state and territory enforcement agencies; conducts 60 inspections and reviews; generates approximately 100 reports on the result of these inspections; and regularly reports to parliament on the results of our oversight activities. However, I am concerned that this bill is proposing expanded and new oversight functions in an environment where my office continues to have oversight functions without any additional resources. Just lately, we were empowered with an oversight role in relation to preservation notices under Chapter 3 of the Telecommunications (Interception and Access) Act 1979 and the delayed notification search warrants under Part IAAA of the Crimes Act 1914, as well as the role of Norfolk Island ombudsmen. All the additional important functions were prescribed without any funding to my office.
>
> The oversight function being proposed under Chapter 4 will significantly increase our inspection workload. If my office continues to be the prescribed statutory oversight function authority without funding, this will reduce the level of assurance that we can provide in overseeing covert and intrusive powers. Furthermore, this pressure reduces my office's ability to provide effective oversight of other extraordinary powers of law enforcement where we do not have a statutory inspections role.
>
> …
>
> I should also say in relation to resources that our strong preference is for the Ombudsman's office to be directly funded for the oversight role. If the bill is passed, there should be a budget mechanism for my office to receive departmental appropriations directly and not through other departments.[12]

7.24 Participants in the inquiry generally supported the expanded role for the Commonwealth Ombudsman.[13] Mr Matthew Lobb of Vodafone commented in relation to the Ombudsman's role:

12 Mr Colin Neave, *Committee Hansard,* Canberra, 29 January 2015, pp. 42-43.

13 Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard,* Canberra, 29 January 2015, p. 13; Mr Michael Griffin AM, Commissioner, Australian Commission for Law Enforcement Integrity, *Committee Hansard,* Canberra, 29 January 2015, p. 34; Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone, *Committee Hansard,*

> Undoubtedly, there are our obligations—privacy obligations and data retention obligations—and the Privacy Commissioner can play that role. But it not must not be overlooked that we see the role of the Ombudsman as ensuring that the law enforcement agencies' activities are consistent with the legislation; and we think it is important that the Ombudsman play a role in telling the public that they can trust what the law enforcement agencies are doing. I think that is a very important role, particularly as we expand that function.[14]

7.25 The Privacy Impact Assessment prepared by the Australian Government Solicitor described the Ombudsman's expanded role as 'privacy enhancing' as it will provide a mechanism to identify specific instances of non-compliance as well as any general agency practices which may create a risk of non-compliance.[15]

7.26 Other submitters recognised the need for additional funding. For example, in their joint submission, Dr John Selby, Professor Vijay Varadharajan and Dr Yvette Blount stated:

> the Bill does not include specific provisions for additional funding for the Commonwealth Ombudsman so as to be able to adequately resource its new oversight task. Oversight without sufficient resources provides only the illusion of scrutiny, rather than the actual scrutiny necessary to determine whether the intrusive powers being granted to government agencies by this legislation are being used in a limited, proper manner, and not being abused.[16]

7.27 Similarly, the councils of civil liberties across Australia stated:

> The Commonwealth Ombudsman's Office is not well resourced. This is a significant and important new role. It is obviously

---

Canberra, 29 January 2015, p. 60; Australian Commission for Law Enforcement Integrity, *Submission 48,* p. 8; Uniting Church Justice and International Mission Unit, *Submission 76*, p. 10; Corruption and Crime Commission of Western Australia, *Submission 100,* p. 2; Australian Communications Consumer Action Network, *Submission 120,* p. 11; Mr Scott Millwood, *Submission 121,* p. 14; Australian Privacy Foundation, *Submission 75*, p. 3; Guardian Australia, *Submission 132,* p. 12; Law Council of Australia, *Submission 126,* p. 28.

14 Mr Matthew Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 67.

15 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979,* 15 December 2014, p. 24 (appended to Attorney-General's Department, *Submission 27).*

16 Dr John Selby, Professor Vijay Varadharajan and Dr Yvette Blount, *Submission 114,* p. 8.

> important that the Government provides additional resources to the Ombudsman to allow this role to be implemented effectively.[17]

7.28 In contrast to others, the Muslim Legal Network (NSW) argued that oversight by the Commonwealth Ombudsman was inadequate and will not provide accountability and transparency.[18]

7.29 While generally supporting the Ombudsman's role, the councils of civil liberties across Australia drew attention to Australia's obligations under the International Covenant on Civil and Political Rights:

> [T}he Government should provide for effective oversight which will ensure accountability for arbitrary or unlawful interference by enforcement agencies with the right to privacy as required by the International Covenant on Civil and Political Rights (ICCPR) 33 Moreover, the ICCPR states that parties must ensure victims of violations of the Covenant have an effective remedy.[19]

7.30 The councils went on to argue:

> The Ombudsman's oversight role will neither provide for effective oversight nor provide any remedy or sanction for unlawful access. Under the provisions in Schedule 3, unlawful conduct on the part of enforcement agencies in accessing telecommunications data may never come to light, because the Ombudsman is not required to report on any contravention of the TIA Act. Moreover, there is no requirement to inform a person whose telecommunications data had been accessed. In fact, to do so would be an offence punishable by 2 years imprisonment pursuant to s181B of the TIA Act.
>
> In the circumstances, unlawful access to telecommunications data will likely go unknown and even if the Ombudsman reports on such conduct, there is no provision for any sanction.[20]

7.31 The Law Council of Australia also expressed concern that there is no provision for oversight of the manner in which investigations are conducted.[21]

---

17 Councils for civil liberties across Australia, *Submission 129,* p. 15. See also Guardian Australia, *Submission 132,* p. 18; Law Council of Australia, *Submission 126,* p. 28.

18 Muslim Legal Network (NSW), *Submission 198,* p. 8.

19 Councils for civil liberties across Australia, *Submission 129,* p. 14.

20 Councils for civil liberties across Australia, *Submission 129,* pp. 14-15.

21 Mr Peter Leonard, Chairperson, Media and Communications Committee, Law Council of Australia, *Committee Hansard,* Canberra, 30 January 2015, p. 32.

7.32 In evidence to the Committee, the Australian Privacy Commissioner suggested that oversight of agencies' compliance with Chapter 4 would more effectively sit with his office rather than the Commonwealth Ombudsman. His reasons for this suggestion were as follows:

- combining oversight responsibilities would enable the Commissioner to monitor the handling of telecommunications data 'throughout its lifecycle – that is, from collection to disclosure to destruction',
- it would provide 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, and
- the Commissioner has existing processes and procedures necessary for assessing enforcement agencies' compliance with Chapter 4 of the TIA Act.[22]

Committee comment

7.33 The Committee supports the substantially expanded role for the Commonwealth Ombudsman outlined in the Bill. The Committee considers that the elevated position of the Commonwealth Ombudsman is an essential safeguard that will provide significant reassurance to the Parliament and the community.

7.34 The Committee notes that the proposed regime was developed in consultation with the Ombudsman and that he considers his office has the necessary expertise and experience to fulfil this function.

7.35 The Committee has significant concerns however about the Commonwealth Ombudsman's statements about the lack of resources available to his office to fulfil this oversight function. The Committee agrees with the Ombudsman that, without appropriate resources, the level of assurance that can be provided by the Ombudsman's office will be reduced.

7.36 The Committee considers that the Government should provide additional financial resources for the Office of the Commonwealth Ombudsman in line with the Ombudsman's increased oversight responsibilities.

22 Office of the Australian Information Commissioner, *Submission 92*, p. 34.

Recommendation 29

The Committee recommends that the Government consider the additional oversight responsibilities of the Commonwealth Ombudsman set out in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 and ensure that the Office of the Commonwealth Ombudsman is provided with additional financial resources to undertake its enhanced oversight responsibilities.

7.37 While the Committee notes the concerns of some participants regarding the Ombudsman's role, the Committee considers that it is the appropriate body to undertaken oversight of Chapters 3 and 4 of the TIA Act. The Committee considers that the effectiveness of this safeguard mechanism is a matter that should be considered when this Committee undertakes its legislated review of the mandatory data retention scheme.

7.38 The Committee also notes the view of the Australian Privacy Commissioner about oversight of Chapter 4 of the TIA Act. However the Committee did not receive sufficient evidence on this matter to conclude that the proposed oversight arrangement, as outlined in the Bill, should be amended.

Inspector-General of Intelligence and Security

7.39 The Inspector-General of Intelligence and Security (IGIS) currently oversights and reports on access to telecommunications data by the Australian Security Intelligence Organisation (ASIO), under the *Inspector-General of Intelligence and Security Act 1986*.

7.40 ASIO is the only Australian intelligence agency falling within the oversight remit of the IGIS that has the authority under the TIA Act to request telecommunications data from carriers.[23]

7.41 In her submission, the IGIS explained her office's oversight:

> OIGIS staff regularly examine ASIO telecommunications data authorisations as part of the regular program of inspection of ASIO inquiries and investigations. During these inspections, OIGIS staff review the records of a selected sample of cases. The

23 Inspector-General of Intelligence and Security, *Submission 131,* p. 4.

> inspection team looks at records associated with activities that form part of the ASIO inquiry or investigation. This includes telecommunications data authorisations (historical and prospective), warrants, and any other activities that form part of the inquiry or investigation.
>
> In relation to telecommunications data authorisations, the inspections examine:
>
> - whether the authorisation was approved at the appropriate level, noting that approval for prospective data authorisations must be at a higher level than historical data authorisations
> - whether the collection of that information is related to ASIO's functions
> - whether there was compliance with the Attorney-General's Guidelines, in particular whether the activity was proportionate to the gravity of the threat, and whether there was sufficient justification for not using less intrusive methods to obtain the data.[24]

7.42 The Bill does not propose any changes to the IGIS's oversight role as outlined.

7.43 In her submission, the IGIS indicated that ASIO has demonstrated a consistently high level of compliance with the organisation's obligations.[25]

7.44 The Committee sought the IGIS's views on a recommendation by the Law Council of Australia that:

> ASIO's record keeping procedures in relation to preservation notices, stored communications and telecommunications data, should be brought into line with other enforcement agencies under proposed sections 151 and 186A of the TIA Act; and
>
> IGIS should be required to inspect those records annually in similar terms to proposed subsection 186B(1) of the TIA Act.[26]

7.45 In response, the IGIS told the Committee:

> Based on my experience, I do not see the need for such an amendment in that ASIO records are comprehensive anyway and we have full access to ASIO records. Although we are not required in my legislation to conduct particular inspections, we have hitherto seen ASIO powers as intrusive and always conducted

24 Inspector-General of Intelligence and Security, *Submission 131,* pp. 4-5.

25 Inspector-General of Intelligence and Security, *Submission 131,* p. 5.

26 Law Council of Australia, *Submission 126,* p. 29.

> those inspections. For a small office, I think we do need to have the flexibility to adjust our resources according to what we consider to be most sensitive at any particular time. Having said that, we would never ignore the use of these powers by ASIO. We would always conduct inspections. In my view, the current system is working perfectly well and I do not see the need to have more prescriptive legislation for our oversight.[27]

Committee comment

7.46 As noted above, the Bill does not propose any changes to current arrangements for the oversight of ASIO by the Inspector-General of Intelligence and Security. The Committee notes the IGIS' comments concerning the adequacy of this regime and the organisation's high level of compliance with its obligations.

Review by the Parliamentary Joint Committee on Intelligence and Security

7.47 Recommendation 43 of the Committee's 2013 report recommended, in relation to a mandatory data retention regime, that 'the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement'.[28]

7.48 Proposed section 187N of the Bill provides that the Committee:

> must review the operation of [Part One] as soon as practicable after the third anniversary of the end of the implementation phase for this Part … [and] give the Minister a written report of the review.

7.49 Therefore, in practical terms, the review would not commence until five years after the Bill receives royal assent.

7.50 The Explanatory Memorandum justifies this timeframe as follows:

> The data retention scheme will not be fully functional until at least two years after its commencement as industry begins to collect and retain the required data in accordance with the implementation

27 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard,* Canberra, 29 January 2015, p. 41.

28 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* Canberra, May 2013, p. 193.

> arrangements. In addition, investigations and prosecutions span many years, and they provide the most effective barometer through which the data retention scheme is best empirically assessed. Review three years after the conclusion of the implementation phase will provide both practical industry experience and a sound evidence base for considering the operation of the scheme.[29]

7.51 In terms of the scope of the review, the Australian Privacy Commissioner advocated that:

> Given the scope and the privacy impact of the proposed data retention scheme is determined, to a large extent, by the regulations … the review should include 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.[30]

7.52 The Commissioner also considered that the review should require the collection of further quantitative evidence about the necessity of the scheme, including the age of telecommunications data used in investigations or serious offences and national security threats.[31]

7.53 Some participants advocated for the inclusion of a sunset clause in the Bill. The Australian Privacy Commissioner considered that a sunset clause for expiry of the scheme five years after the implementation period would:

> 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 measures within a definite timeframe. Further, it will also provide those stakeholders with assurance that they will have further opportunity to comment on the necessity and proportionality of any data retention scheme that is implemented.[32]

7.54 In its submission, Guardian Australia also supported a sunset provision in the Bill. Guardian Australia argued that the scheme should also be reviewed by the PJCIS after two years, stating '[b]y 2017, the results of the

---

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

30 Office of the Australian Information Commissioner, *Submission 92,* p. 37.

31 Office of the Australian Information Commissioner, *Submission 92,* p. 38.

32 Office of the Australian Information Commissioner, *Submission 92,* pp. 37-38.

2016 UK review of its similar scheme should be available to inform the Committee's work'.[33]

7.55 Other submitters advocated for an annual review by the Committee.[34]

Committee comment

7.56 The Committee notes the rationale that has been presented for a longer period prior to review of the mandatory data retention scheme by this Committee. The Committee agrees with the importance of having a sound evidence base that draws on practical experience to inform its considerations.

7.57 On balance, the Committee considers that two years after the implementation period of the regime provides an appropriate timeframe to adequately review its operation. The Committee considers it is desirable that a report be presented to the Parliament within three years of the end of this implementation period.

Recommendation 30

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require the Parliamentary Joint Committee on Intelligence and Security to commence its review no later than the second anniversary of the end of the implementation period.

The Committee considers it is desirable that a report on the review be presented to the Parliament no later than three years after the end of the implementation period.

7.58 Further, Committee considers that there are a number of matters that should be included in the terms of reference for that review. In particular, the Committee advises that the scope of the review should include:

- the effectiveness of the scheme,
- the appropriateness of the dataset and retention period,
- costs,

33 Guardian Australia, *Submission 132,* p. 9.

34 Muslim Legal Network (NSW), *Submission 198,* p. 9; Pirate Party Australia, *Submission 124,* p. 11.

- any potential improvements to oversight,
- regulations and determinations made,
- the number of data breaches, and
- the number of complaints about the scheme to relevant bodies.

7.59 The effectiveness of that review will require statistical data on many of the matters listed above. However, during the course of this inquiry, the Committee was informed on numerous occasions that the data it sought was not collected. The Committee considers that, to facilitate an effective future review, it is essential that appropriate statistical data be retained by agencies.

7.60 The Committee notes that records of data access requests must be kept for three years or until the Ombudsman has made a report about those records. To assist its review, the Committee recommends that agencies be required to retain records for the period from commencement of the regime until the Committee's review is concluded.

Recommendation 31

At the time of the review required to be undertaken by the Parliamentary Joint Committee on Intelligence and Security under proposed section 187N of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, the Committee recommends that the Attorney-General request the Committee to examine the following issues:

- **the effectiveness of the scheme,**
- **the appropriateness of the dataset and retention period,**
- **costs,**
- **any potential improvements to oversight,**
- **regulations and determinations made,**
- **the number of complaints about the scheme to relevant bodies, and**
- **any other appropriate matters.**

To facilitate the review, the Committee recommends that agencies be required to collect and retain relevant statistical information to assist the Committee's consideration of the above matters. The Committee also recommends that all records of data access requests be retained for the period from commencement until the review is concluded.

Finally the Committee recommends that, to the maximum extent possible, the review be conducted in public.

7.61 With regard to the proposed sunset clause, the Committee acknowledges the comments of the Australian Privacy Commissioner concerning the opportunity for further input from stakeholders. The Committee considers however that the matters identified by the Commissioner can be considered during the Committee's mandated review.

7.62 In this instance, the Committee concurs with the views of Professor George Williams of the Gilbert + Tobin Centre of Public Law, who argued:

> I would actually prefer a narrower regime that deals properly with the issue. I have not put forward the need for a sunset clause, and that is because I think it would be much better to get the legislation in the form it ought to be. This measure is not unknown in other countries; there are many nations that have data retention

> regimes. We already have a form of ad hoc data retention in Australia. I would say, though, that if we do not incorporate the sort of safeguards that many of the submissions are urging then a sunset clause and a mandatory review would be necessary, but it would be very inadequate to do that as opposed to just getting the legislation right in the first place.[35]

7.63 The Committee also notes that Recommendation 43 of its 2013 report recommended a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security. This part of the recommendation has not been addressed in the Bill. The Committee has, however, made recommendations throughout the report concerning aspects of the mandatory data retention regime that it considers should be subject to oversight by this Committee.

7.64 Given the expansion of the Committee's oversight and review role through both this Bill and the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*, the Committee sees development benefits in agencies providing a standing secondee to the Department of the House of Representatives, which provides staff to support the Committee. The Committee's expectation is that any secondee arrangement would be open to supplementation should this be required for more complex inquiries.

Recommendation 32

The Committee recommends that the Attorney-General coordinate the provision of a standing secondee or secondees to the secretariat of the Parliamentary Joint Committee on Intelligence and Security, in recognition of the additional oversight and review requirements associated with the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* and the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

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

Annual reporting

7.65 In its 2013 report, the Committee recommended that there should be an annual report to Parliament on the operation of any mandatory data retention scheme.[36]

7.66 Proposed section 187P of the Bill provides that an annual report on the operation of Part 1 of the Bill must be prepared as soon as practicable after 30 June each year. This report is to be included in the report required under subsection 186(2) of the TIA Act.

Committee comment

7.67 To promote transparency and accountability, the Committee considers that the annual report should include details relating to:

- costs of the scheme,
- use of implementation plans,
- category of purpose for accessing data, including a breakdown of types of offences,
- age of data sought,
- number of requests for traffic data, and
- number of requests for subscriber data.

7.68 The Committee also considers it would be useful for the Attorney-General's Department to provide an annual briefing to the Committee on the matters included in this report.

36 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* Canberra, May 2013, p. 193.

Recommendation 33

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require the annual report prepared under section 187P to include:

- **costs of the scheme,**
- **use of implementation plans,**
- **category of purpose for accessing data, including a breakdown of types of offences,**
- **age of data sought,**
- **number of requests for traffic data, and**
- **number of requests for subscriber data.**

The Committee also recommends that the Attorney-General's Department provide the Committee with an annual briefing on the matters included in this report.

7.69 Further, as discussed in Chapter 6, the Committee recognises concerns raised by inquiry participants about the types of offences for which data retained under the proposed scheme may be accessed. To provide reassurance to the Parliament and the community, the Committee considers that enhanced accountability and oversight is prudent.

7.70 As set out in Chapter 6, the Committee has recommended that when authorising access to telecommunications data, any interference with the privacy of any person that may result from the disclosure must be justifiable and proportionate. Authorising officers would be required to have regard to the gravity of the conduct being investigated, the reason for the proposed disclosure, and its likely relevance and usefulness to the investigation.

7.71 The Committee also welcomes the expanded powers of the Commonwealth Ombudsman to oversight agencies' access to telecommunications data under Chapter 4 of the TIA Act.

7.72 The Committee considers that the oversight provided by the Commonwealth Ombudsman and Inspector-General of Intelligence and Security (in relation to ASIO) would be further enhanced by greater Parliamentary involvement in monitoring the regime. This could be achieved through this Committee being empowered to review relevant annual reports, in line with House of Representatives Standing Order

215(c) and Senate Standing Order 25(20), which enable legislative and general purpose standing committees to initiate inquiries into matters raised in the annual reports of departments and agencies.

7.73 This will require legislative change to, for the first time, enable the Committee to look at operational matters in the limited area of authorisation of access to telecommunications data relating to ASIO and the AFP, consistent with the Committee's remit. As with other sensitive material, these matters would be dealt with in private. The Committee also suggests that State governments look at putting in place oversight provisions in this area.

Recommendation 34

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to provide that the Committee may inquire into any matter raised in the annual report prepared under proposed section 187P, including where this goes to a review of operational matters.

Legislative change to the *Intelligence Services Act 2001* should be implemented to reflect this changed function.

The Committee further recommends that the Commonwealth Ombudsman and Inspector-General of Intelligence and Security provide notice to the Committee should either of them hold serious concerns about the purpose for, or the manner in which, retained data is being accessed.

Privacy protections and data security

7.74 Essential to the integrity of a mandatory data regime must be the assurance of privacy protections and mechanisms to ensure the security of data. The following sections examine the requirements to comply with the Australian Privacy Principles, concerns regarding the security of retained data, and in the event of data breaches, a possible mandatory data breach notification scheme.

Privacy Act 1988 and Australian Privacy Principles

7.75 The Attorney-General's Department noted that improper access to telecommunications data is a criminal offence punishable by up to two years imprisonment. The Department also noted that telecommunications providers that retain information are subject to the *Privacy Act 1988* (the Privacy Act) and *Telecommunications Act 1997* (the Telecommunications Act), which require providers to deal with information in a manner that is consistent with those laws.[37]

7.76 Schedule 1 of the Privacy Act contains 13 Australian Privacy Principles (APPs), which dictate the standards, rights and obligations for the handling, holding, accessing and correction of personal information.[38] The APPs generally apply to Australian government agencies, private sector organisations with an annual turnover of $3 million or more, and some private sector organisations, such as health providers, with an annual turnover of less than $3 million.[39]

7.77 APP 11 concerns the security of personal information and states:

> 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
>
> (a) from misuse, interference and loss; and
>
> (b) from unauthorised access, modification or disclosure.
>
> 11.2 If:
>
> (a) an APP entity holds personal information about an individual; and
>
> (b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and
>
> (c) the information is not contained in a Commonwealth record; and

37 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 28.

38 Office of the Australian Information Commissioner, 'About Privacy', <http://www.oaic.gov.au/privacy/about-privacy> viewed 26 February 2015.

39 Office of the Australian Information Commissioner, 'Australian Privacy Principles', <http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles> viewed 26 February 2015.

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

The entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.[40]

7.78 The Privacy Impact Assessment prepared by the Australian Government Solicitor observed that 'a threshold consideration is whether the service providers to which the new regime will apply are entities which are required to comply with the Privacy Act'.[41] The Assessment then went on to state:

> We understand from discussions with officers of the Department that the vast majority of service providers will be organisations within the meaning of the Privacy Act and thus subject to the Privacy Act. However, we understand there are a small number of service providers that may be a small business operator within the meaning of s 6D of the Privacy Act, and for that reason may not be required to comply with the Privacy Act.[42]

7.79 The Australian Privacy Commissioner also highlighted that different service providers may be subject to different levels of oversight in relation to the handling and retention of personal data. For example, they might be APP entities, subject to state/territory legislation in some, but not all, jurisdictions, or have a small business exemption. [43]

7.80 The Commissioner argued that:

> 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.[44]

7.81 The Commissioner went on to make two recommendations:

40 Office of the Australian Information Commissioner, 'Privacy Fact Sheet 17: Australian Privacy Principles', January 2014, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles> viewed 26 February 2015.

41 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979,* 15 December 2014, p. 9 (appended to Attorney-General's Department, *Submission 27).*

42 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979,* 15 December 2014, p. 9 (appended to Attorney-General's Department, *Submission 27).*

43 Office of the Australian Information Commissioner, *Submission 92,* p. 31.

44 Office of the Australian Information Commissioner, *Submission 92,* p. 32.

- First, that all providers be subject to the Privacy Act, and
- Secondly, should the first recommendation not be adopted, that all service providers comply with binding rules made by the Australian Privacy Commissioner.[45]

7.82 Mr Mark Newton, submitting in a private capacity, made a similar point:

> The vast majority of ISPs in Australia are small enough to remain below the thresholds required for protection of private data under the Privacy Act, yet the Bill contains no stipulations at all about how the data should be collected, how it can be used, where it can be stored, and what ISPs are permitted to do with it outside the purpose for which it has been collected. And yet this data constitutes the most extreme example imaginable of 'Personally Identifying Information', being specifically intended for the frictionless mass identification of individuals.
>
> It is inexplicable that such privacy-sensitive legislation can be proposed in this day and age without any reference whatsoever to the Privacy Act 1998 or the Australian Privacy Principles regulated by the Office of the Australian Information Commissioner.[46]

7.83 FutureWise similarly commented that the Bill:

> does not impose any requirements for data security or privacy on the carriage service providers, but seems to rely on the provisions of the Privacy Act. However, not all services providers will fall within the scope of the Privacy Act in which case there is little privacy protection at all.[47]

7.84 The Privacy Impact Assessment noted that the Government had decided against legislative amendment to deem all service providers to be organisations for the purposes of the Privacy Act because:

- carriage service providers within the meaning of the Telecommunications Act are required to observe and comply with the Communications Alliance Telecommunications Consumer Protections Code (the Code). The Code is registered under Part 6 of the Telecommunications Act by the ACMA, which has powers to enforce compliance. A key principle enshrined in the Code is that consumers 'will enjoy open, honest and fair dealings with their Supplier, *and have their*

45 Office of the Australian Information Commissioner, *Submission 92,* p. 8.

46 Mr Mark Newton, *Submission 123,* pp. 7-8.

47 FutureWise, *Submission 128,* p. 14.

privacy protected' (our emphasis), and several provisions of the Code relate to protection of privacy.

- The functions of the Telecommunications Industry Ombudsman (TIO) include investigating and facilitating the resolution of complaints about any interference with the privacy of an individual by a telecommunications provider, both in terms of non-compliance with applicable privacy requirements under the Privacy Act (such as the APPs) and also breach of any applicable industry specific privacy standards. Most service providers will be within the jurisdiction of the TIO, and if an individual believes their privacy has been breached and is unable to resolve the matter with the service provider, they will be entitled to seek the assistance free of charge from the TIO through its dispute resolution scheme.[48]

7.85 Some submitters expressed general dissatisfaction with the present regime. The Victorian Commissioner for Privacy and Data Protection, for example, disagreed that the security regime overseen by the Australian Privacy Commissioner was a suitable mechanism to assess industry's compliance with the Australian Privacy Principles as well as monitoring industry's non-disclosure obligations under the Telecommunications Act.[49]

7.86 Australian Lawyers for Human Rights also considered the Australian Privacy Principles to be inadequate, arguing that:

> There are numerous areas in which the Privacy Principles will not fit well with the Bill and will need to be modified.[50]

7.87 Similarly, the Australian Privacy Foundation submitted that:

> the current legal controls on the use, disclosure and security of such data, including those established under the *Privacy Act 1988* (Cth) and Part 13 of the *Telecommunications Act 1997* (Cth), are inadequate.[51]

Data security

7.88 The Bill is silent on the issue of data security. This issue was raised, however, by numerous submitters to the inquiry.

---

48 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979,* 15 December 2014, pp. 9-10 (appended to Attorney-General's Department, *Submission 27).*

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

50 Australian Lawyers for Human Rights, *Submission 88,* pp. 2-3.

51 Australian Privacy Foundation, *Submission 75*, p. 2.

7.89 Many submitters generally cited data security as a concern.[52] Other submitters expressed more particular concerns that:

- the stored data would become a target or 'honey pot',[53] both for those with criminal or malicious intent and those with civil litigation claims,[54] particularly if stored in a single location rather than across multiple platforms,
- the Bill does not prevent offshore storage,[55]

---

52 M Hope, *Submission 18,* p. 1; B Ridgway, *Submission 20,* p. 4; J O'Callaghan, *Submission 29,* p. 1; D Donnelly, *Submission 30,* p. 2; Commissioner for Privacy and Data Protection (Victoria), *Submission 39,* p. 9; H Murdoch, *Submission 40,* p. 1; F Maley, *Submission 49,* p. 1; W Delaforce, *Submission 51,* p. 1; B Skurrie, *Submission 63,* p. 1; M Deerbon, *Submission 65,* p. 1; Name withheld, *Submission 78,* p. 1; C Cresswell, *Submission 79,* p. 2; Australian Lawyers for Human Rights, *Submission 88,* p. 6; Ms Terri Butler MP, *Submission 91,* p. 7; Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94,* p. [8]; Amnesty International Australia, *Submission 95,* p. 3; Dr Paul Bernal, *Submission 99,* p. 6; R Graf, *Submission 105,* pp. 4-5; Dr John Selby, Professor Vijay Varadharajan and Dr Yvette Blount, *Submission 114,* p. 4; Law Institute of Victoria, *Submission 117*, p. 5; Australian Communications Consumer Action Network, *Submission 120,* p. 11; S Millwood, *Submission 121,* p. 12; M Newton, *Submission 123;* p. 6; Law Council of Australia, *Submission 126,* p. 21; FutureWise, *Submission 128,* p. 14; A Naughton, *Submission 136,* p. 1; G Curtis, *Submission 141;* p. 3; A/Professor Einar Thorsteinsson, *Submission 147,* p. 1; A Layton-Bennett, *Submission 151,* p. 2; A Barut, *Submission 172,* p.1; C Sanderson, *Submission 173,* p. 1; A Cavanna, *Submission 191,* p. 1.

53 Commissioner for Privacy and Data Protection (Victoria), *Submission 39,* p. 11; V Hesse, *Submission 15*, p. 1; F Maley, *Submission 49,* p.1; A Doodkorte, *Submission 53,* pp.1-2; M Setiawan, *Submission 60*, p. 2; Ms Terri Butler MP, *Submission 91,* p. 9; P Schnackenburg, *Submission 103,* p. 1; F Rauch Valenti, *Submission 104,* p. 1; R Graf, *Submission 105,* p. 5; T Darling, *Submission 113,* p. 1; Name withheld, *Submission 116,* p. 1; Australian Communications Consumer Action Network, *Submission 120,* p. 11; Pirate Party Australia, *Submission 124,* p. 10; FutureWise, *Submission 128,* p. 13; A Layton-Bennett, *Submission 151,* p. 2; Australian Privacy Foundation, *Submission 75,* p. 15; A Naughton, *Submission 136,* p. 1; G Curtis, *Submission 141;* p. 3; R Lammers, *Submission 148,* p. 1; J McPherson, *Submission 153,* p. 2; E Stocker, *Submission 163,* p. 1; S Vicarioli, *Submission 175,* p. 1; L Milne, *Submission 179,* p. 1; S Whitewood, *Submission 181,* p. 1; Name withheld, *Submission 188,* p. 2; Name withheld, *Submission 192,* p. 2.

54 Communications Alliances and ATMA, *Submission 6,* p. 14; B Ridgway, *Submission 20,* p. 3; Private Media, *Submission 77,* p. [2]; Ms Terri Butler MP, *Submission 91,* p. 8, 14; Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94,* [5]; R Graf, *Submission 105,* pp. 4-5; Australian Information Industry Association, *Submission 109,* p. 4; M Newton, *Submission 123;* p. 6; Australian Privacy Foundation, *Submission 75,* p. 16; Law Council of Australia, *Submission 126,* p. 21.

55 P Freak, *Submission 26,* p. 1; Commissioner for Privacy and Data Protection (Victoria), *Submission 39,* p. 10; A Cooksley, *Submission 43,* p. 1; M Setiawan, *Submission 60*, p. 2; Name withheld, *Submission 78,* p. 1; R Graf, *Submission 105,* pp. 4-5; Australian Information Industry Association, *Submission 109,* p. 4; Law Institute of Victoria, *Submission 117*, p. 5; S Millwood, *Submission 121,* pp. 12-13; M Newton, *Submission 123;* p. 6; Pirate Party Australia, *Submission 124,* p. 10; Law Council of Australia, *Submission 126,* p. 21; A Naughton, *Submission 136,* p. 1; H Stock, *Submission 152,* p. 1; A Layton-Bennett, *Submission 151,* p. 2; K Matchett, *Submission 162,* p. 1; A Cavanna, *Submission 191,* p. 1;.

- the Bill does not explicitly require data to be destroyed at the end of the retention period,[56] and
- substantial amounts of data will need to be retained under the scheme, increasing the level of risk.[57]

7.90 The Privacy Impact Assessment noted that due to the obligations imposed by the scheme:

> There is naturally a concern that the longer the period for which data is required to be retained, the greater the risk the security of that data may be compromised.[58]

7.91 While acknowledging that currently there are risks to the security of data that must be managed, Telstra also explained to the Committee that the requirement to create a centralised platform for retention of data under the Bill creates an enhanced target. Telstra commented at a public hearing:

> [Y]ou are quite right to say that the existence of a large dataset with a lot of personal and other information contained within it could be an attraction for people for a variety of reasons.[59]

7.92 Telstra also acknowledged that additional measures will be required to secure customer data. Telstra indicated that it would continue to invest in the necessary systems and that the company was 'well placed to implement these additional security measures'.[60]

7.93 Electronic Frontiers Australia also outlined concerns with the security of retained data:

> [T]his legislation will result in the creation of what will be massive databases of very, very valuable personal information that will be honey pots to organised crime and to any sort of person that can potentially access it. Now, the scope of risk, for example, for systems administrators who must look after this data to be compromised in some way is very high. As Steve Dalby from iiNet said in a room not far from here last year, when asked about this, 'Look, we're a business; we're going to try and find the lowest cost

56 Amnesty International Australia, *Submission 95,* p. 3; Law Institute of Victoria, *Submission 117*, p. 5; Law Council of Australia, *Submission 126,* p. 21; FutureWise, *Submission 128,* p. 13.

57 Victorian Commissioner for Privacy and Data Protection, *Submission 39,* p. 10.

58 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979,* 15 December 2014, p. 18 (appended to Attorney-General's Department, *Submission 27).*

59 Mr James Shaw, *Committee Hansard,* Canberra, 29 January 2015, p. 8.

60 Telstra, *Submission 112,* p. 4; Mr James Shaw, *Committee Hansard,* Canberra, 29 January 2015, p. 7.

> option for storing this data, and right at the moment the lowest cost option for storing data is in China'. So there is a very real risk also—as this committee, I am sure, is only too well aware—of this sort of information being compromised by foreign intelligence agencies as well.[61]

7.94 Arguing that the existing security regime is not 'fit for purpose', the Victorian Privacy Commissioner made the following points:

- APP 11 is the only security obligation created by the *Privacy Act 1988* and is too abstract to provide concrete security guidance,
- the Privacy Act does not apply to 90 percent of the private sector because of the small business exemption,
- the Bill does not prevent retained data being transmitted to, and stored in, offshore cloud computing services that are under the control of foreign corporations and foreign governments,
- the amount of data that will be stored is magnitudes greater than at present,
- the Australian Privacy Commissioner does not have direct jurisdiction over contracted service providers, and
- commercial entities (that will store the data) are not required to adhere to the same level of data security standards as government agencies.[62]

7.95 The Law Council of Australia raised concerns that 'there does not appear to be a minimum set of standards for government agencies and service providers to ensure security of retained telecommunications data'.[63]

7.96 Mr Tom Courtney, submitting in an individual capacity, argued:

> As storing the data will have to be implemented by the ISP's it will not necessarily have the appropriate security controls. It is the very likely that ISPs will implement the cheapest solution at the expense of security which would lead to this data being easily hacked by any malicious person or organisation.[64]

7.97 The Explanatory Memorandum states:

---

61 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard,* Canberra, 29 January 2015, p. 26.

62 Victorian Commissioner for Privacy and Data Protection, *Submission 39,* pp. 9-11.

63 Law Council of Australia, *Submission 126,* p. 24.

64 Mr Tom Courtney, *Submission 23,* p. 1.

> The Privacy Act and proposed Telecommunications Sector Security Reforms (TSSR) will, in combination, require service providers to do their best to prevent unauthorised access to and unauthorised interference with retained telecommunications data. In addition, the Privacy Commissioner will continue to have oversight of carriers' collection and retention of personal information under the Bill where service providers are subject to the Privacy Act, including the ability to conduct assessments to ensure compliance with the APPs.[65]

7.98 As noted above, APP 11 requires APP entities to take reasonable steps to protect information from misuse, interference, loss and authorised access, modification or disclosure. The Attorney-General's Department noted that while the Bill includes no additional requirement to destroy retained data, APP 11.2 requires entities to destroy personal information when no longer required for legitimate purposes.[66]

7.99 It is important to recognise, however, that not all providers are APP entities.

7.100 The Explanatory Memorandum notes, however, that non-APP entities are subject to the data protection obligations set down in Part 13 of the *Telecommunications Act 1997,* and are subject to oversight from the Information Commissioner.[67]

7.101 The need for additional protection of data has been acknowledged by the Government and is expected to occur through the Telecommunications Sector Security Reform. The Minister for Communications, the Hon Malcolm Turnbull MP, stated in his second reading speech:

> The government is also 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.[68]

7.102 In this regard, the Attorney-General's Department commented that:

---

65 Data Retention Bill, *Explanatory Memorandum,* p. 13.

66 Attorney-General's Department, *Submission 27,* p. 33.

67 Data Retention Bill, *Explanatory Memorandum,* p. 13.

68 Hon Malcolm Turnbull MP, Minister for Communications, *House of Representatives Official Hansard,* No. 18 2014, Thursday, 30 October 2014, p. 12563.

> [I]t is preferable to implement a holistic security framework for the telecommunications sector, rather than imposing specific, standalone and potentially duplicative security obligations that apply only to a relatively narrow subsection of the information held by industry.[69]

7.103 In 2013, this Committee recommended that any legislation for a proposed data retention regime should ensure that the retained telecommunications data is 'stored securely by making encryption mandatory'.[70]

7.104 On this issue, the Department noted that:

> Using the word 'encryption' does beg the question of what type of encryption and to what standard and in what respect. I think it certainly reflects the intent of this committee, and the recommendation was understood as being about importing a degree of protection for the data. But it is fair to say that, in our engagement with the industry, while some providers asked for certainty and for a prescriptive approach to how to go about doing things, others have been very clear on the fact that being very prescriptive about how a measure should be implemented fetters their ability to run their businesses, which of course are ones that they must run at a profit.[71]

7.105 In a supplementary submission, the Department further advised the Committee that:

> In relation to mandatory encryption of retained data, there may be complexity in imposing such a requirement. Placing encryption on new databases could be a simple and inexpensive process. However, retro-fitting encryption on existing legacy systems is likely to be a more difficult and expensive endeavour for industry. This could particularly be the case of the significant amounts of telephony information held on legacy networks.[72]

7.106 Optus explained to the Committee that encryption was one of many potentially valuable tools for securing retained data:

> I think it is worthwhile and imminently conceivable. Clearly you would look at all the security and preventive regimes—encryption

69 Attorney-General's Department, *Submission 27,* p. 37.

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

71 Ms Harmer, Attorney-General's Department, *Committee Hansard*, Canberra, 30 January 2015, p. 73.

72 Attorney-General's Department, *Submission 27.3*, p. 1.

> is one of them, and segregating data. … If it is a well-defined database and it is not the entire set of data or processes that we maintain, it should be a relatively straightforward task to segregate it for security purposes, and possibly encrypt it, if need be. It is a sensible thing to have things like electronic sand traps—all the access protocols that we apply to the most sensitive information already.[73]

7.107 Communications Alliance provided similar evidence:

> **Mr Stanton:** The service providers already need to comply with the government's Information Security Manual and with the Protective Security Policy Framework, which are both pretty stringent requirements that need to be met today. Peter, perhaps you might be better placed to address the question directly.
>
> **Mr Froelich:** I think the two documents, the PSPF and the ISM, that John has raised are trigger documents. In fact, whenever we go through any cost-recovery exercise with the government those are part of the compliance objectives the government puts in front of us. So we have very stringent requirements around security. But, beyond that, as an industry, we have every reason and every intention to protect the privacy and security of our customers. For our industry members, there would be no reason why we do anything less with their data under this regime than we do under anything else. All of those security structures and tools available to us—firewalls, physical security and encryption—we would put in place to ensure that our customers' privacy and security is maintained along with the interface with government as well. Those are standard practices now in the way we deal with law enforcement and national security and the way we deal with customers' data.[74]

7.108 The Australian Privacy Commissioner indicated that he considered a security framework for the telecommunications sector should be in place 'before service providers are required to collect and store any information' under the data retention regime.[75] Further:

---

73 Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Optus, *Committee Hansard*, Canberra, 30 January 2015, p. 22.

74 Mr John Stanton, Chief Executive Officer, Communications Alliance and Mr Peter Froelich, Industry Member, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, pp. 39-40.

75 Office of the Australian Information Commissioner, *Submission 92*, p. 36.

> 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 becomes essential.[76]

Mandatory data breach notification

7.109 In its 2013 report, the Committee recommended in relation to mandatory data retention that any legislation include 'a robust, mandatory data breach notification scheme'.[77] This recommendation has not been implemented as part of the Bill.

7.110 In evidence, the Australian Privacy Commissioner noted the risks associated with a data breach and expressed the view that one effective mechanism to manage this risk is a mandatory data breach notification scheme.[78] The Commissioner made the following comment in relation to this issue:

> 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 intent and/or criminal intent. One way to help manage the impact on individuals affected by a data breach involving telecommunications data is to amend the Bill to include a mandatory data breach notification requirement that applies to service providers.[79]

7.111 The Commissioner noted national and international trends that reflect an increase in the number and severity of data breaches.[80] The Commissioner also pointed out that:

---

76 Office of the Australian Information Commissioner, *Submission 92,* p. 36.

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

78 Office of the Australian Information Commissioner, *Submission 92,* pp. 8, 10, 11.

79 Office of the Australian Information Commissioner, *Submission 92,* p. 11.

80 Office of the Australian Information Commissioner, *Submission 92,* p. 29.

> 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.[81]

7.112 In the Commissioner's view, notification is an important mitigation strategy for any individuals affected by a data breach. For this reason, the Commissioner recommended that the Bill 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).[82]

7.113 The Australian Information Industry Association also indicated its support for 'the development of a mandatory security standard and reporting and auditing requirements particularly in regard to any security breaches'.[83]

7.114 Similarly, the Law Institute of Victoria expressed strong support for a mandatory data breach notification scheme:

> The LIV strongly recommends that the Privacy Act 1988 be amended in accordance with the recommendation of the Australian Law Reform Commission to introduce an obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach (commonly referred to as a mandatory data breach notification scheme). This amendment will ensure that persons who are affected by breaches are aware of them and can seek legal remedies and mitigates the unintended consequences identified in scenarios 5, 6 and 8 [outlined in their submission].[84]

7.115 At present, the Australian Privacy Commissioner accepts data breach notifications on a voluntary basis and has published guidelines to assist

---

81 Office of the Australian Information Commissioner, *Submission 92,* p. 29.

82 Office of the Australian Information Commissioner, *Submission 92,* p. 30.

83 Australian Information Industry Association, *Submission 109,* p. 4; See also, Electronic Frontiers Australia, *Submission 97,* p. 27.

84 Law Institute of Victoria, *Submission 117.1*, p. [10].

organisations to respond to a data breach involving personal information.[85]

7.116 The Commissioner noted, however, that although notification of data breaches to the Commissioner and affected individuals may be a reasonable step, 'it is not an express requirement under the Privacy Act'.[86]

7.117 The Privacy Amendment (Privacy Alerts) Bill 2013 lapsed on prorogation of the 43rd Parliament and was reintroduced as a private Senator's Bill on 20 March 2014.

7.118 This Bill would amend the Privacy Act to introduce mandatory data breach notification provisions for agencies and organisations that are regulated by the Privacy Act. The Explanatory Memorandum for the Bill described mandatory data breach notification as:

> a legal requirement to provide notice to affected persons and the relevant regulator when certain types of personal information are accessed, obtained, used, disclosed, copied, or modified by unauthorised persons. Such unauthorised access may occur following a malicious breach of the secure storage and handling of that information (e.g. a hacker attack), an accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information, or otherwise.[87]

7.119 The scheme would be consistent with a recommendation of the Australian Law Reform Commission (ALRC), which considered that notification should be provided 'to those whose privacy had been infringed when data breaches causing "a real risk of serious harm" occurred'.[88]

7.120 Further, the ALRC considered notification should be compulsory 'unless it would impact upon a law enforcement investigation or was determined by the regulator to be contrary to the public interest'.[89]

---

85 Office of the Australian Information Commissioner, *Submission 92,* p. 29. See also, 'Data breach notification guide: a guide to handling personal information security breaches', August 2014, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches> viewed 26 February 2015.

86 Office of the Australian Information Commissioner, *Submission 92,* p. 28.

87 Privacy Amendment (Privacy Alerts) Bill 2014, *Explanatory Memorandum,* p. 2.

88 Privacy Amendment (Privacy Alerts) Bill 2014, *Explanatory Memorandum,* p. 2.

89 Privacy Amendment (Privacy Alerts) Bill 2014, *Explanatory Memorandum,* p. 2.

Committee comment

7.121 The Committee notes that the Bill does not prescribe how retained communications data is to be stored or any specific security standards. As with protection and oversight, the Privacy Commissioner considered that the security standards should also be standardised at a level that is commensurate with the risk to privacy. The Committee agrees with this view.

7.122 The Committee considers that in the absence of the Telecommunications Sector Security Reform, interim measures to bring all providers into a consistent privacy regime are a necessary step. On the basis of the evidence received, the Committee considers it would be appropriate to require all providers to be subject to either the Australian Privacy Principles or binding rules of the Australian Privacy Commissioner.

7.123 The Committee notes that there is precedent for requiring small businesses to comply with the Australian Privacy Principles. Small businesses with an annual turnover of less than $3 million that are required to collect and retain customer, financial and transaction records under the *Anti-Money Laundering/Counter Terrorism Financing Act 2006* are also required to comply with the Australian Privacy Principles.[90]

7.124 The Committee is mindful, however, of the regulatory burden on small providers. For this reason, the Committee has recommended that the Government's funding model provide sufficient support for smaller service providers who may be unable, amongst other things, to implement privacy controls without up-front assistance.[91]

90 *Privacy Act 1998*, s. 6E(1A).

91 See recommendation 16 of this report.

Recommendation 35

Having regard to the regulatory burden on small providers with an annual turnover of less than $3 million, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require all service providers to be compliant, in respect of retained data, with either the Australian Privacy Principles or binding rules developed by the Australian Privacy Commissioner.

7.125 The Committee acknowledges the security risks associated with the proposed mandatory data retention scheme and the potential for increased unlawful access to personal information. The Committee considers that the security of retained data is a critical issue and the community must be able to have confidence in the security of stored data. The Committee addressed telecommunications security and the proposed Telecommunications Sector Security Reform in its 2013 report.[92] Noting the Minister's statement in his second reading speech, the Committee is strongly of the view that these reforms should be finalised and implemented prior to the end of the implementation period for this Bill.

7.126 The Committee notes that the Bill does not currently provide for mandatory encryption of data retained under the scheme, which was recommended by the Committee in its 2013 report.[93] In the absence of the sector-wide Telecommunications Sector Security Reform, which might dictate security or encryption standards, interim measures that are as or more effective will be required in relation to the proposed data retention regime.

7.127 Consequently, the Committee sought additional information from telecommunications service providers on the capacity to implement mandatory encryption for data retained under the scheme. Based on this information and other evidence provided, the Committee considers that data encryption is a necessary and appropriate measure in order to secure retained data and that this requirement should be included in the Bill. The Committee considers that security standards should be developed in consultation with the Data Retention Implementation Working Group and should be incorporated into regulations. The Committee notes that mandatory encryption may cause technical difficulties in relation to some

92 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* Canberra, May 2013, Chapter 3.

93 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* Canberra, May 2013, Recommendation 42, p. 192.

existing systems used by service providers, and considers that the Communications Access Co-ordinator should be able to authorise other robust security measures, as appropriate, in respect of those instances.

7.128 A mandatory data breach notification scheme is considered one effective mitigation strategy for those affected by a data breach. While the Committee notes that this issue is the subject of broader consideration within Government, the Committee considers that there must be a scheme in place prior to implementation of the Bill. The Committee considers that a mandatory data breach notification scheme would provide a strong incentive for service providers to implement robust security measures to protect data retained under the data retention regime.

7.129 The Committee discussed the importance of security of stored data in relation to its location. The Committee agreed that this underlies the importance of implementing the Telecommunications Sector Security Reform (TSSR). The TSSR Bill should be referred to this Committee. In its consideration, the Committee will consider issues relating to the location of stored data and security.

Recommendation 36

The Committee recommends that the Government enact the proposed Telecommunications Sector Security Reforms prior to the end of the implementation phase for the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

Recommendation 37

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to require service providers to encrypt telecommunications data that has been retained for the purposes of the mandatory data retention regime.

To give effect to this recommendation, the Committee recommends that the Data Retention Implementation Working Group develop an appropriate standard of encryption to be incorporated into regulations, and that the Communications Access Co-ordinator be required to consider a provider's compliance with this standard as part of the Data Retention Implementation Plan process.

Further, the Communications Access Co-ordinator should be given the power to authorise other robust security measures in limited circumstances in which technical difficulties prevent encryption from being implemented in existing systems used by service providers.

Recommendation 38

The Committee recommends introduction of a mandatory data breach notification scheme by the end of 2015.

Concluding comments

7.130 Through the process of this inquiry, the Committee has considered the current utility of telecommunications data to law enforcement and national security investigations. The Committee has noted the inconsistency and degradation of current retained telecommunications data, possible future reductions in retained data and the serious impact this may have on national security and public safety.

7.131 Accordingly, the Committee considered carefully the rationale for a mandatory data retention scheme, and has concluded that such a regime is justified as a necessary, effective and proportionate response. The Committee therefore supports the intention of the Bill.

7.132 While it is imperative to equip security and law enforcement agencies with the capability to conduct investigations, these powers must be contained by appropriate authorisations and balanced by oversight and safeguards. In considering each provision of the Bill, the Committee has sought to confirm that adequate safeguards and oversight mechanisms are in place. The Committee considers that the recommendations made in this report serve to strengthen the functioning and integrity of the proposed data retention regime.

7.133 The Committee thanks the contributors to the inquiry for their input.

Recommendation 39

The Committee recommends that, following consideration of the recommendations in this report, the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be passed.

Dan Tehan MP

Chair

February 2015