The Parliament of the Commonwealth of Australia

Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Parliamentary Joint Committee on Intelligence and Security

February 2015
Canberra

ISBN 978-1-74366-270-0 (Printed version)

ISBN 978-1-74366-271-7 (HTML version)

Contents

APPENDICES

Membership of the Committee

Chair	Mr Dan Tehan MP	
Deputy Chair	Hon Anthony Byrne MP	
Members	Hon Jason Clare MP (from 25/11/2014)	Senator David Bushby
	Hon Mark Dreyfus QC MP (from 25/11/2014)	Senator the Hon Stephen Conroy
	Mr Andrew Nikolic AM, CSC, MP	Senator the Hon John Faulkner (until 06/02/2015)
	Hon Tanya Plibersek MP (until 24/11/2014)	Senator David Fawcett
	Hon Philip Ruddock MP	Senator John Williams (from 25/11/2014)
	Hon Bruce Scott MP (until 24/11/2014)	Senator the Hon Penny Wong (until 25/11/2014)

Terms of reference

On 21 November 2014, the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 was referred to the Committee by the Attorney-General.

List of abbreviations

AAT	Administrative Appeals Tribunal
ACC	Australian Crime Commission
ACCAN	Australian Communications Consumer Action Network
ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
ACMA	Australian Communications Media Authority
AFP	Australian Federal Police
AIMIA	Australian Interactive Media Industry Association
ALRC	Australian Law Reform Commission
AMTA	Australian Mobile Telecommunications Association
APPs	Australian Privacy Principles
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
CAC	Communications Access Co-ordinator
CSP	Carriage Service Provider
EU	European Union
FBI	Federal Bureau of Investigation (United States)

HLR	Home Location Records
IGIS	Inspector-General of Intelligence and Security
IP	Internet Protocol
ISM	Information Security Manual
ISP	Internet Service Provider
IWG	Data Retention Implementation Working Group
MEAA	Media, Entertainment & Arts Alliance
PIN	Personal Identification Number
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Privacy Act	*Privacy Act 1988* (Cth)
PSPF	Australian Government Protective Security Policy Framework
PSTN	Public Switched Telephone Network
SMS	Short Message Service
SPoC	Single Point of Contact
Telecommunications Act	*Telecommunications Act 1997* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
TSSR	Telecommunications Sector Security Reforms
US	United States of America
VLR	Visitor Location Records
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

List of recommendations

1 Introduction

Recommendation 1

The Committee recommends that the Government provide a response to the outstanding recommendations from the Committee's 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* by 1 July 2015.

3 The data set

Recommendation 2

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

Recommendation 3

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

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

Recommendation 4

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

Recommendation 5

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

Recommendation 6

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

Recommendation 7

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

Recommendation 8

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

4 Data retention period

Recommendation 9

The Committee recommends that the two-year retention period specified in section 187C of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be maintained.

Recommendation 10

The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 clarify the requirements for service providers with regard to the retention, de-identification or destruction of data once the two year retention period has expired

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

Recommendation 11

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

Recommendation 12

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

Recommendation 13

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

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

Recommendation 14

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

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

Recommendation 15

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

Recommendation 16

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

- provides sufficient support for smaller service providers, who may not have sufficient capital budgets or operating cash flow to implement data retention, and privacy and security controls, without up-front assistance;
- minimises any potential anti-competitive impacts or market distortions;

- accounts for the differentiated impact of data retention across different segments of the telecommunications industry;
- incentivises timely compliance with their data retention obligations;
- provides appropriate incentives for service providers to implement efficient solutions to data retention;
- does not result in service providers receiving windfall payments to operate and maintain existing, legacy systems; and
- takes into account companies that have recently invested in compliant data retention capabilities in anticipation of the Bill's passage.

6 Authority to access stored communications and telecommunications data

Recommendation 17

The Committee recommends that criminal law-enforcement agencies, which are agencies that can obtain a stored communications warrant, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*.

To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as a criminal law-enforcement agency subject to the following conditions:

- the declaration ceases to have effect after 40 sitting days of either House;
- an amendment to specify the authority or body as a criminal law-enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days; and
- the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sittings days for review and report.

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 110A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include investigating serious contraventions.

Recommendation 18

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or its Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 110A(4)(c)(ii) of the *Telecommunications (Interception and Access) Act 1979* include 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.

The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements.

Recommendation 19

The Committee recommends that the Attorney-General's Department review whether:

- the agencies which may access the content of communications (either by way of interception warrants or stored communications warrants) under the *Telecommunications (Interception and Access) Act 1979* should be standardised, and
- the Attorney-General's declaration power contained in proposed section 110A of the *Telecommunications (Interception and Access) Act 1979* in respect of criminal law-enforcement agencies should be adjusted accordingly.

The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by the end of the implementation phase of the data retention regime.

Recommendation 20

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to list the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) as criminal law-enforcement agencies under proposed section 110A of the *Telecommunications (Interception and Access) Act 1979*.

Recommendation 21

The Committee recommends that enforcement agencies, which are agencies authorised to access telecommunications data under internal authorisation, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*.

To provide for emergency circumstances the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as an enforcement agency subject to the following conditions:

- the declaration ceases to have effect after 40 sitting days of either House;
- an amendment to specify the authority or body as an enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days; and
- the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report.

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 176A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include enforcement of the criminal law, administering a law imposing a pecuniary penalty, or administering a law relating to the protection of the public revenue.

Recommendation 22

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or the Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 176A(4)(c)(ii) of the *Telecommunications (Interception and Access) Act 1979* include 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.

The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements.

Recommendation 23

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime.

To enable appropriate exceptions to this prohibition the Committee recommends that a regulation making power be included.

Further, the Committee recommends that the Minister for Communications and the Attorney-General review this measure and report to the Parliament on the findings of that review by the end of the implementation phase of the Bill.

Recommendation 24

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime. Telecommunications service providers should be able to recover their costs in providing such access, consistent with the model applying under the Privacy Act in respect of giving access to personal information.

Recommendation 25

The Committee recommends that section 180F of the *Telecommunications (Interception and Access) Act 1979* be replaced with a requirement that, before making an authorisation under Division 4 or 4A of Part 4-1 of the Act, the authorised officer making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate.

In making this decision the authorised officer should be required to have regard to:

- the gravity of the conduct being investigated, including whether the investigation relates to a serious criminal offence, the enforcement of a serious pecuniary penalty, the protection of the public revenue at a sufficiently serious level or the location of missing persons;
- the reason why the disclosure is proposed to be authorised; and
- the likely relevance and usefulness of the information or documents to the investigation.

Recommendation 26

The Committee acknowledges the importance of recognising the principle of press freedom and the protection of journalists' sources. The Committee considers this matter requires further consideration before a final recommendation can be made.

The Committee therefore recommends that the question of how to deal with the authorisation of a disclosure or use of telecommunications data for the purpose of determining the identity of a journalist's source be the subject of a separate review by this Committee.

The Committee would report back to Parliament within three months.

In undertaking this inquiry, the Committee intends to conduct consultations with media representatives, law enforcement and security agencies and the Independent National Security Legislation Monitor. The review will also consider international best practice, including data retention regulation in the United Kingdom.

Recommendation 27

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to require agencies to provide a copy to the Commonwealth Ombudsman (or Inspector General of Intelligence and Security (IGIS) in the case of ASIO) of each authorisation that authorises disclosure of information or documents under Chapter 4 of the Act for the purpose of determining the identity of a journalist's sources.

The Committee further recommends that the IGIS or Commonwealth Ombudsman be required to notify this Committee of each instance in which such an authorisation is made in relation to ASIO and the AFP as soon as practicable after receiving advice of the authorisation and be required to brief the Committee accordingly.

Recommendation 28

The Committee recommends that the Attorney-General's Department oversee a review of the adequacy of the existing destruction requirements that apply to documents or information disclosed pursuant to an authorisation made under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* and held by enforcement agencies and ASIO.

The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by 1 July 2017.

7 Safeguards and oversight

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.

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.

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.

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.

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.

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.

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.

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.

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.

1

Introduction

The Bill and its referral

1.1 On 30 October 2014, the Minister for Communications, the Hon Malcolm Turnbull MP, introduced the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) into the House of Representatives.

1.2 In his second reading speech, Minister Turnbull stated that the Bill is intended to 'prevent the further degradation of the investigative capabilities of Australia's law enforcement and national security agencies'.[1]

1.3 Minister Turnbull added that the Bill will 'require companies providing telecommunications services in Australia, carriers and internet service providers to keep a limited, prescribed set of telecommunications data for two years'.[2]

1.4 Minister Turnbull also explained that:

> This bill is critical to prevent the capabilities of Australia's law enforcement and national security agencies being further degraded. It does not expand the range of telecommunications metadata which is currently being accessed by law enforcement

1 The Hon Malcom Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12560.

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

agencies. It simply ensures that metadata is retained for a period of two years.[3]

1.5 On 21 November 2014, the Attorney-General, Senator the Hon George Brandis, QC, wrote to the Committee to refer the provisions of the Bill for inquiry and to request it to report by 27 February 2015. He further requested that the Committee should, as far as possible, conduct its inquiry in public.

1.6 In the letter, the Attorney-General informed the Committee that the Bill follows the National Security Legislation Amendment Bill (No.1) 2014 and Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 as the Government's third tranche of legislation in response to the current national security threat.

1.7 The Attorney-General also provided the Committee with a draft data set outlining the specific types of telecommunications data that service providers would be required to retain. The Attorney-General indicated that it was his intention for the data set to be given effect by regulation at the time the Bill received Royal Assent. A copy of the draft data set is included at Appendix A to this report.

2012–13 Inquiry into potential reforms of Australia's national security legislation

1.8 The Committee previously examined a proposal for a mandatory data retention regime in the 43rd Parliament as part of its inquiry into potential reforms of Australia's national security legislation. The then Committee tabled its report before the Parliament on 24 June 2013.[4] A copy of this report is available on the Committee's website at www.aph.gov.au/pjcis.

1.9 The 2013 report made several recommendations of relevance to the data retention regime, only some of which have been addressed in the current Bill. Many of the report's recommendations on other matters were addressed by the National Security Legislation Amendment Bill (No. 1) 2014, which the Committee reported on 17 September 2014. However, a number of recommendations in the 2013 report that are of relevance to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) are yet to be responded to by the Government.

3 The Hon Malcom Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12560.

4 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013.

1.10 The Committee notes that the Senate Legal and Constitutional Affairs References Committee is currently undertaking a comprehensive inquiry examining revision of the TIA Act.

1.11 Without pre-empting the Senate Committee's conclusions, the Committee draws the Government's attention to the recommendations included in its 2013 report that have not yet been responded to (these recommendations are set out in Appendix B). The Committee recommends that the Government respond to those recommendations by 1 July 2015. The Committee notes that the Government response should not in any way delay debate of the Bill.

Recommendation 1

The Committee recommends that the Government provide a response to the outstanding recommendations from the Committee's 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* by 1 July 2015.

Inquiry objectives and scope

1.12 Through its current inquiry, the Committee carefully examined the overall appropriateness of the data retention regime proposed in the Bill and the draft data set. In doing so, the Committee weighed evidence provided by law enforcement and security agencies (both in public and private) that the continued availability of historical telecommunications data was critical for efforts to deal with the current national security environment and the ongoing threat posed by other serious criminal offences; against the financial implications and privacy and data security concerns associated with the proposal.

1.13 The Committee focused on ensuring the Bill incorporates adequate safeguards and accountability mechanisms for the proper application of the laws into the future.

1.14 At the time of the Bill's introduction into the Parliament, the formation of a joint government-industry Implementation Working Group (IWG) on data retention was announced. The IWG comprised senior representatives from both the telecommunications industry and Australian law enforcement and national security organisations. It was established to

discuss implementation, refinement of the draft data set and the cost of the scheme, in parallel with the Committee's inquiry.

1.15 On 16 December 2014, the Attorney-General provided the Committee with a copy of the IWG's first report.[5] The report made 16 recommendations, including four suggesting changes to the draft data set, 11 suggesting additions to the supporting explanatory material, and one recommending changes to the procedure for any future amendments to the data set. The report also included an amended version of the draft data set reflecting the IWG's recommendations. In its submission to the Committee, the Attorney-General's Department explained that the IWG report was intended to assist the Committee's consideration of the proposed data set rather than provide a replacement. A copy of the IWG report's recommendations is included at Appendix C to this report.

Conduct of the inquiry

1.16 The Chair of the Committee, Mr Dan Tehan MP, announced the inquiry by media release on 27 November 2014 and invited submissions from interested members of the public. Written questions were also sent to selected law enforcement agencies and industry organisations. Submissions were requested by 19 January 2015.

1.17 The Committee received 204 submissions, 31 supplementary submissions and two exhibits from sources including individuals, government agencies, statutory authorities, telecommunications companies and industry, legal, community and civil liberties groups. A list of submissions and exhibits received by the Committee is at Appendix D.

1.18 The Committee held three public hearings on 17 December 2014, 29 January 2015 and 30 January 2015. The Committee also held one private hearing and received three private briefings from relevant agencies in Canberra, and visited the Australian Federal Police headquarters for further operational briefings. A list of hearings and the witnesses who appeared before the Committee is included at Appendix E.

1.19 Copies of submissions received and transcripts of public hearings can be accessed on the Committee's website at www.aph.gov.au/pjcis. Links to the Bill and the Explanatory Memorandum are also available on the Committee's website.

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

1.20 This report, while making a number of recommendations to amend the Bill, is designed to inform the next stage of debate which will take place in the Senate and House of Representatives. In some instances the Committee has recommended amendments to the Bill. In other instances the Committee has determined that measures in the Bill require more detailed explanation and has requested that the Attorney-General provide additional information to assist debate of the Bill.

1.21 The provisions of the Bill were intensely debated and there were a variety of views expressed within the Committee. The Committee expects the Bill will be subject to continuing debate in the Parliament and the community.

Report structure

1.22 This report consists of seven chapters:

- This chapter sets out the context, scope and conduct of the inquiry,
- Chapter 2 provides an overview of the Committee's consideration of the case for data retention. The chapter considers whether mandatory data retention can, in principle, be justified as a vital tool for national security and law enforcement investigations, and whether appropriate safeguards and oversight can be put in place. The chapter discusses the adequacy of the current regime, privacy and civil liberties concerns, and the security of the retained data.
- Chapters 3 to 5 discuss the main issues raised in evidence to the inquiry in relation to Schedule 1 to the Bill, and the Committee's comments and recommendations in regard to those issues. These issues were:
  - ⇒ Chapter 3 – Whether the Government's proposed data set should be contained in primary legislation, as opposed to being made in regulations; and the scope of the Government's proposed data set.
  - ⇒ Chapter 4 – The proposed two-year retention period; and whether service providers should be required to destroy telecommunications data retained in accordance with proposed new Division 1 of Part 5-1A at the end of the retention-period.
  - ⇒ Chapter 5 – The range of service providers and services to which data retention obligations are proposed to apply; the implementation arrangements for the proposed data retention regime; and the cost of the proposed data retention scheme.

- Chapter 6 discusses the main issues raised in evidence to the inquiry in relation to Schedule 2 to the Bill, and the Committee's comments and recommendations in regard to those issues. Schedule 2 contains amendments in respect of restrictions on access to stored communications and telecommunications data.
- Chapter 7 examines specific safeguards and oversight mechanisms set out in the Bill. This includes consideration of the expanded role for the Commonwealth Ombudsman set out in Schedule 3 to the Bill, review mechanisms and reporting requirements. The chapter also examines matters raised in evidence that are outside the scope of the Bill, but which were addressed by the Committee in its 2012–13 inquiry, including a mandatory data breach notification scheme.

2

The case for data retention

2.1 When this Committee last considered the issue of mandatory data retention as part of its *Inquiry into potential reforms of Australia's national security legislation*, the then Government had not prepared or released a detailed legislative proposal; the question was dealt with at the conceptual level. The absence of a detailed legislative proposal limited the capacity of the public to make meaningful comment on this issue, and limited the capacity of the Committee to consider and resolve the question of whether such a scheme was, at the most fundamental level, capable of being justified for national security and law enforcement purposes.

2.2 In 2012–13, there was a relatively clear divide between law enforcement and national security agencies in support of the proposal, and organisations and individual submitters in opposition to the proposal.

2.3 In this inquiry, however, the Committee and the public have had the benefit of being able to review draft legislation, a proposed data set, detailed supporting materials and submissions prepared by the Attorney-General's Department and other Government agencies. The Committee has, therefore, received detailed submissions arguing the need for data retention from a wide range of stakeholders.

2.4 Based on the submissions and evidence this Committee has received over the course of this inquiry, the dichotomy between Government and non-Government submissions has weakened. Many organisations and individuals remain opposed to the principle of data retention.[1] However,

---

1 See, for example: Mr Ben Johnston, *Submission 35*, p. 1; Mr Bernard Keane, *Submission 37*, p. 1; Mr Glenn Bradbury, *Submission 38*, p. 1; Blueprint for Free Speech, *Submission 54*, p. 3; Australian Privacy Foundation, *Submission 75*, p. 2; Dr Lesley Lynch, Secretary, New South Wales Council for Civil Liberties, on behalf of joint councils for civil liberties, *Committee Hansard*, Canberra, 30 January 2015, p. 79; Amnesty International, *Submission 95*, p. 1; Law Institute of Victoria, *Submission 117*, p. 1.

the concept of data retention, either as proposed by the Government in Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) or in another form, has attracted support from a broad range of stakeholders. A selection of extracts from evidence provided by these stakeholders is contained below.

Box 2.1 – Selected extracts from submissions expressing in-principle support to data retention

It is Bravehearts' position that Australia should implement a data retention scheme as a critical tool for supporting the investigation of child sexual exploitation matters and other serious offences — Bravehearts, *Submission 33*.

[M]odernising our laws to reflect contemporary technical advances is obviously a sensible, justified and legitimate objective … We then, in short, support the passage of the bill … In particular, we strongly support the bill's proposal to confine the number of agencies that can access retained telecommunications data, and there are other aspects of the bill that we think are extremely useful — Professor Gillian Triggs, President, Australian Human Rights Commission, *Committee Hansard*, Canberra, 29 January 2015.

Metadata has become a vital part of the investigative process, and in almost all instances is a fundamental part of the case for acquiring a warrant with more and wider ranging powers — Alexander Lynch, *Submission 1*.

[W]e do see policy merits in a more standardised set of arrangements to give certainty for agencies, industry and citizens. So the policy intent of the overall framework we do think is an appropriate and worthwhile activity — Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia, *Committee Hansard*, Canberra, 29 January 2015.

The Unit is largely supportive of the Bill, as a very important instrument in the fight against online child sexual abuse. The Australian Federal Police have identified the vital role metadata retention plays in the being able to identify and prosecute offenders engaged in online child sexual abuse. Further, the failure to pass this legislation will undoubtedly assist large numbers of offenders escape detection and prosecution each year, reducing the effectiveness of the Australian Federal Police in combating this crime type — Uniting Church Justice and International Mission Unit, *Submission 76*.

[T]he right to privacy is not absolute and requires an assessment to be made of whether the measures that may limit privacy are both necessary and proportionate to achieve that objective. Applying this in the context of the introduction of a data retention scheme, privacy interests must be balanced with the need to ensure that law enforcement and security agencies have access to the information necessary to perform their functions — Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard*, Canberra, 29 January 2015

I think the previous inquiry exposed the extent to which data is potentially not being retained … we welcome efforts to standardise the data held and restrict access to a named group of agencies — Ms Narelle Clark, Deputy Chief Executive Officer, Australian Communications Consumer Action Network, Committee Hansard, Canberra, 29 January 2015.

2.5 Professor George Williams and Dr Keiran Hardy, submitting in their personal capacity as members of the Gilbert + Tobin Centre of Public Law at the Faculty of Law, University of New South Wales expressed in-principle support for data retention:

> We recognise the importance of standardising the collection of data by communications service providers. Given that telecommunications data can play an important role in investigating serious criminal offences such as terrorism and child pornography, we accept that this data should be available to law enforcement agencies in appropriate circumstances. Having a clear

> and codified legislative scheme for the collection of telecommunications data is a worthy goal that will aid in the prevention of serious crime. [2]

2.6 Mr John Stanton, CEO of Communications Alliance, the primary telecommunications industry body in Australia, gave evidence that the views of members of the telecommunications industry have also shifted since 2012:

> Last time we appeared before the committee back in 2012 we stated on behalf of the industry quite clearly that we did not believe a case had been made for the type of mandatory data retention regime that was at that time being proposed. Today it is fair to say there is something of a range of views among our membership as to whether such a case has now been made, and it depends in part on the final shape of the regime, around which many questions remain. [3]

2.7 However, the Committee does not wish to overstate the level and breadth of support for data retention. It remains a disputed proposal. For example, Blueprint for Free Speech stated that:

> Blueprint remains firmly against the introduction of a data retention regime in Australia. Cementing a place for a mass surveillance regime in Australia bucks international trend and does not reflect necessity or proportionality to the investigation and resolution of serious criminal activity.[4]

2.8 The Committee also received many submissions from individual community members which, by and large, expressed in-principle opposition to the proposed data retention regime. For example, Ms Priya Shaw stated that 'there is no version of this legislation I believe I can in good conscience support'.[5]

2.9 While it is impossible within the confines of this report for the Committee to cite from every individual submission, a representative selection of contributions from individual submitters is contained below.

Box 2.2 – Selected extracts from submissions made by individual community members

> Targeted communications surveillance, undertaken by LEAs via warrant, is a necessary and effective weapon in fighting serious crime including terrorism. However unwarranted blanket data

2 Professor George Williams AO and Dr Keiran Hardy, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales, *Submission 5*, p. 1.

3 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, p. 31.

4 Blueprint for Free Speech, *Submission 54*, p. 14.

5 Ms Priya Shaw, *Submission 47*, p. 1.

retention is fraught with dangers and represents a step change in powers that citizens would be required cede to government — Brian Ridgway, *Submission 54*.

I believe that our security organisations have failed to put a credible case as to why these changes, which impinge on the privacy of all Australians and thus give yet another win to the terrorists who aim to undermine our democracy, are necessary — Albert Lightfoot, *Submission 134*.

This bill will destroy the general public's basic right to privacy in an ill-advised bill resulting in the death of a fundamental democratic freedom — Iain Muir, *Submission 28*.

This metadata reveals far too much about citizens, who have a right to their privacy and who should not be treated like criminals — Fiona Maley, *Submission 49*.

Metadata now provides a more complete, constant and intrusive picture of an individual's lifestyle, habits and relationships than can be obtained by access to content alone — Alexander Lynch, *Submission 1*.

This bill tries to make the distinction that 'metadata' is of lesser importance to regular 'content'. I disagree, as it can be as important or even more important — Adam Cooksley, *Submission 43*.

… the Bill does not define what categories of data industry will be forced to retain. This is the single most critical aspect of the proposed regime, and the Government needs to reveal this information to enable effective and robust consideration of the proposal by the Australian community — Damien Donnelly, *Submission 30*.

Treating all Australians as potential suspects runs contradictory to not only our democracy but our Australian values — Alicia Cooper, *Submission 22*.

Australia's internet is already overly expensive and this policy will just end up costing every Australian citizen more money to use the internet. Whether it is paid for by the ISPs or by the Government, any internet user will have to foot the bill either through higher ISP fees, or through government taxes — Tom Courtney, *Submission 23*.

Not only will the proposed legislation compromise the privacy and freedoms of all Australians that use the internet, but and perhaps most importantly, similar laws around the world both in the United States and Europe have been proven not to work; why would they work here? — Cam Browning, *Submission 44*.

Many terrorists are already familiar with ways to circumvent these proposals meaning that majority of the people who will be affected will be law abiding citizens while the terrorists 'swim through the net' — Peter Freak, *Submission 26*.

The two year data retention duration specified in the legislation has never been justified. It is significantly longer than the retention duration in most other jurisdictions that have implemented similar schemes — Douglas Stetner, *Submission 32*.

This legislation should require a warrant for access to any data retained, as recommended by the Parliamentary Human Rights Committee. This maintains coherence with requirement for judicial oversight and maintains a balance where an external party must be satisfied as to the reason for the request — Barbara Reed, *Submission 154*.

The Australian public needs clear and transparent guarantees that their sensitive personal data information will be protected from hackers or foreign entities, especially in the light of the number of significant data breaches in recent times — Mason Hope, *Submission 18*.

What regulations will be enforced to make sure my private information and property are not stolen or leaked out onto the internet? Can the Australian Government guarantee that my information will be protected? Can ISPs do the same? Is it even possible to make such a guarantee? — Josh O'Callaghan, *Submission 29*.

With vast amounts of very revealing, very telling, very intimate data sitting in one place, these data centres will be a primary target of cybercriminals and hackers from all around the world — Daniel Scott, *Submission 61*.

Copyright holders will demand access to these stores of metadata likely pressing down on service providers via threats of litigation. These will be used in turn to self-police their intellectual property

— Iain Muir, *Submission 28*.

This bill is an attack on the personal freedoms of Australian citizens and particularly undermines the ability of journalists and whistle-blowers to expose corruption and misconduct in government agencies — Dr Peter Evans, *Submission 57*.

A similar metadata storage plan has already been considered and rejected by the European Union's Court of Justice — please give this plan the same consideration that it was given there — Bethany Skurrie, *Submission 63*.

2.10 The Committee has been requested to review the Government's proposal to establish a mandatory telecommunications data retention regime, including appropriate exemptions, safeguards and oversight mechanisms, and to provide advice to the Parliament on these important issues.

2.11 In this process, the Committee is mindful of the advice of the Australian Information Commissioner, Professor John McMillan, who has previously noted that the question of data retention raises a number of interrelated policy issues, and argued for the need to carefully distinguish between these issues when discussing data retention:

> [T]he term 'data retention' in fact camouflages a whole range of other issues. There is the question of data capture, data minimisation, data security, data storage and data use … My anecdotal observation of the debate is that all of those issues are sort of tossed around fairly indiscriminately, and all under the umbrella of 'data retention'. At the end of the day what we clearly need is to untangle those issues and work through them on a systematic and principled basis.[6]

2.12 This chapter addresses this issue through consideration of the following topics:

- the adequacy of the current regime,
- privacy and civil liberties concerns, and
- security of the retained data.

2.13 The Committee notes that the final two topics are closely related, as the potential for security breaches has significant ramifications for the proportionality and privacy risks associated with the proposed scheme.

2.14 Subsequent chapters of this report will address the substance of the proposed data retention regime, the implementation process, the cost of the proposed regime, arrangements for access to telecommunications data by government and non-government entities, and oversight and security arrangements.

6 Professor John McMillan, Australian Information Commissioner, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 23 April 2014, p. 22.

Is the current regime adequate?

2.15 The following section provides an overview of the current regime for access to telecommunications data by national security and law enforcement agencies, including the types of data that are regularly accessed. The section concludes with a discussion of how the declining availability of telecommunications data, in conjunction with other challenges, is impacting on agencies operational capabilities and outcomes.

Overview of the current regime

2.16 At present, 'enforcement agencies' and the Australian Security Intelligence Organisation (ASIO) may access telecommunications data under an internal authorisation issued under Part 4-1 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

2.17 Telecommunications data is information about a communication or the parties to a communication, as distinct from the content or substance of that communication. Access to the actual content or substance of communication, such as a recording of a voice call, or the body or subject line of an email, is prohibited except under a warrant.[7]

2.18 During the course of the Committee's 2012–13 *Inquiry into potential reforms of Australia's national security legislation*, the Attorney-General's Department provided a document outlining the types of data it considered to be telecommunications data. In summary, telecommunications data includes:

- 'information that allows a communication to occur', such as the time, date and duration of the communication, the identifiers of the services and devices involved, and certain information about the location of the respective devices (such as which cell tower or access point the device was connected to), and
- 'information about the parties to the communication', such as their name, address and contact details, billing and transaction information, and general account information.[8]

2.19 An enforcement agency is defined to include the Australian Federal Police (AFP) or the police force of a State or Territory, as well as a limited number of crime commissions, integrity bodies, the Australian Customs

7 *Telecommunications (Interception and Access) Act 1979* (TIA Act), sections 7, 108 and 172.

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

and Border Protections Service (Customs) and the CrimTrac Agency. However, the definition also contains an open-ended provision permitting 'any body whose functions include administering a law imposing a pecuniary penalty; or administering a law relating to the protection of the public revenue'.[9]

2.20 The power to authorise access to historic telecommunications data by an enforcement agency is limited to:

- the head of an agency,
- the deputy head of an agency, or
- a management-level officer or employee of the agency authorised, in writing, by the head of the agency.[10]

2.21 These authorised officers may only authorise access to historic telecommunications data where access to that particular data is 'reasonably necessary' for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue. Authorisations may only be made after considering whether any interference with the privacy of any person is justifiable, having regard to the likely relevance and usefulness of the data, and the reason why access is proposed to be authorised.[11]

2.22 In 2012–13, more than 80 Commonwealth, State and Territory enforcement agencies accessed historic telecommunications data under the TIA Act. In total, those agencies made 330 640 authorisations for access to historic telecommunications data,[12] resulting in a total of 546 500 disclosures.[13] The Queensland Police Service explained that, depending on how a service provider counts their disclosures, a single authorisation may result in a number of disclosures:

> [A]n authorisation requesting all information in relation to the connection of a mobile service requires a number of separate requests to be submitted to one telecommunications company as they will only provide information to specific request such as 'subscriber information', 'point of sale', 'copy of customer contract' and 'payment details'. It is this information together that would

9 TIA Act, section 5.

10 TIA Act, section 5AB.

11 TIA Act, Part 4-1.

12 Attorney-General, *Telecommunications (Interception and Access) Act 1979: Report for the year ending June 2013*, Commonwealth of Australia, 2013, pp. 47–51.

13 Australian Communications and Media Authority, *Communications Report 2012–13*, p. 54.

satisfy the documents/data being requested under the original authorisation.[14]

2.23 Previous evidence from the AFP indicates that approximately 85 per cent of data authorisations relate to subscriber information, such as name and address information, with only 15 per cent relating to 'traffic data', such as call charge records.[15] Victoria Police similarly provided evidence to this Committee that such subscriber checks 'make up the overwhelming majority of historical data requests made by Victoria Police'.[16] This evidence is consistent with the detailed operational briefings provided by a number of law enforcement and national security agencies to this Committee. However, the absence of more detailed, publicly-available information about the use of law enforcement agencies' use of powers under Chapter 4 of the TIA Act is an issue with the existing regime.[17] The Committee has made recommendations in support of enhanced collection of statistical information and annual reporting arrangements in Chapter 7 of this report.

2.24 For ASIO, authorisations for access to historic telecommunications data may only be made where the person making the authorisation is 'satisfied that the disclosure would be in connection with the performance by the Organisation of its functions'.[18] The Inspector-General of Intelligence and Security described the threshold set by the TIA Act as 'low', but also noted that ASIO must additionally comply with the Attorney-General's Guidelines, issued under section 8A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act),[19] which provide, among other things, that:

- the initiation and continuation of investigations shall be authorised only by the Director-General, or an officer at or above Executive Level 2 authorised by the Director-General for that purpose,[20]

14 Queensland Police Service, *Submission 19*, p. [3].

15 Australian Federal Police (AFP), *Submission 25*, Senate Legal and Constitutional Affairs References Committee, *Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, pp. 5–6.

16 Victoria Police, *Submission 8*, p. 2.

17 See, for example: PJCIS, *Report of the inquiry into potential reforms of Australia's national security legislation*, Canberra, May 2013, Recommendation 3; Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats* (2012), p. 26; *Submission 26*, Senate Legal and Constitutional Affairs References Committee, *Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, p. 28.

18 TIA Act, Part 4-1.

19 Inspector-General of Intelligence and Security (IGIS), *Submission 131*, p. 3.

20 *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* (Attorney-General's Guidelines),

- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence,[21]
- inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest,[22] and
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.[23]

2.25 The number of data authorisations made by ASIO is not publicly reported on national security grounds. However, the former Director-General of Security, Mr David Irvine, recently provided evidence to the Senate Legal and Constitutional Affairs References Committee that the number of authorisations made by ASIO for access to telecommunications data each year is 'proportionate… with other individual agencies.'[24] This Committee is aware of the number of data authorisations made by ASIO, and can confirm the accuracy of Mr Irvine's statement.

Utility of telecommunications data for national security and law enforcement investigations

2.26 Mr David Vaile and Mr Paolo Remati, from the Cyberspace Law and Policy Community of the University of New South Wales Law Faculty, identified the value of telecommunications data to law enforcement and national security investigations:

> Many uses of telecommunications metadata, and content for that matter, for targeted law enforcement and criminal intelligence purposes are widely accepted and uncontroversial. Use of large volumes of metadata may also be justified in some cases. It is important to support such law enforcement and intelligence capabilities, since they have proven useful and there is a consensus that they can be appropriately regulated based on years of policy refinement.[25]

Guideline 8.1.

21 Attorney-General's Guidelines, Guideline 10.4(a).

22 Attorney-General's Guidelines, Guideline 10.4(b).

23 Attorney-General's Guidelines, Guideline 10.4(d).

24 Mr David Irvine AO, Director-General of Security, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 21 July 2014, p. 10.

25 Mr David Vaile and Mr Paolo Remati, Cyberspace Law and Policy Community, University of New South Wales Law Faculty, *Submission 194*, p. 2.

2.27 However, several submitters asserted that telecommunications data is of no value to law enforcement and national security investigations. For example, Mr Peter Freak stated that:

> This kind of information not only is intrusive but does absolutely nothing to stop a potential terrorist attack. Despite this, it does however waste law enforcement resources that could be otherwise spent catching actual terrorists.[26]

2.28 The Attorney-General's Department submitted that:

> telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, and almost any activity prejudicial to security that has been facilitated, enabled or carried out via communications technology. Electronic communications, by definition, do not leave a physical footprint, allowing individuals and groups to plan and carry out such activities without risk of detection via many 'traditional' investigative techniques. As such, the records kept by telecommunications companies about the services they have provided (telecommunications data) are often the only source of information available to agencies to identify and investigate individuals and groups using communications technologies for such purposes.[27]

2.29 The Committee also received detailed evidence from agencies about the role telecommunications data plays in their investigations. Agencies emphasised that telecommunications data is used extensively, and provides significant value, in serious and complex investigations.

2.30 Ms Kerri Hartland, then Acting Director-General of Security, confirmed that 'communications data has been critical to the disruption of terrorist attacks in Australia',[28] and provided the Committee with a detailed, unclassified summary of the use of telecommunications data in Operations Pendennis[29] and Neath.[30] ASIO's assessment was that, in both cases, had relevant telecommunications data not been available ASIO would have been blind to critical information, including the existence of covert communications between members of the terrorist groups, and the

26 Mr Peter Freak, *Submission 26*, p. 1.

27 Attorney-General's Department, *Submission 27*, p. 14.

28 Ms Kerri Hartland, Acting Director-General of Security, Australian Security Intelligence Organisation (ASIO), *Committee Hansard*, Canberra, 17 December 2014, p. 5.

29 ASIO, *Submission 12.1*, p. 33; Operation Pendennis involved the disruption of planned mass casualty attacks in Sydney and Melbourne in 2005-06 resulting in the arrest of 22 men, 18 of whom were convicted of terrorism offences.

30 ASIO, *Submission 12.1*, p. 34; Operation Neath involved the disruption of a planned attack on Holsworthy Barracks in Sydney in 2009, resulting in the arrest of 5 men, 3 of whom were convicted of terrorism offences.

full scope of the network of persons involved, with potentially 'disastrous' consequences.[31] ASIO provided the Committee with further, classified, evidence on the use of telecommunications data in these operations.

2.31 The Director-General of Security, Mr Duncan Lewis, also provided the Committee with a detailed explanation of how ASIO uses telecommunications data in the early stages of its investigations:

> When an individual comes to ASIO's attention, there are a range of methods that can be applied to establish whether that person's activities are relevant to security or not. Requesting historical communication data is often one of the most useful as well as one of the least intrusive methods of establishing those matters of fact. In many cases a simple subscriber check on a phone number is sufficient to determine that there is actually no investigation required and the matter can be put aside.[32]

2.32 Mr Lewis also highlighted the importance of reliable access to telecommunications data to counter-espionage investigations:

> Less known, of course, is the way in which historical communication data has been of assistance to us as we tackle the problems of counterespionage. We provided a submission to the committee which you have all seen, and I know one of my colleagues gave evidence in a closed session.[33]

2.33 The AFP explained in its submission that telecommunications data is a 'cornerstone of contemporary policing' and allows the AFP to:

- identify suspects and/or victims,
- exculpate uninvolved persons,
- resolve life threatening situations like child abduction or exploitation,
- identify associations between members of criminal organisations,
- provide insight into criminal syndicates and terrorist networks, and
- establish leads to target further investigative resources.[34]

2.34 The AFP advised that telecommunications data is accessed only on a 'case by case basis according to identified operational needs', and has provided fundamental information across the full suite of the AFP's investigative functions, including:

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

32 Mr Duncan Lewis AO DSC CSC, Director-General of Security, ASIO, *Committee Hansard*, Canberra, 30 January 2015, p. 65.

33 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 64.

34 AFP, *Submission 7.1*, p. 3.

> counter terrorism, serious and organised crime, firearm and drug trafficking, child protection operations, cybercrime, crimes against humanity such as slavery, people smuggling and human trafficking, as well as community policing in the ACT and airports.[35]

2.35 At a public hearing, Commissioner Andrew Colvin provided further, detailed information about the AFP's use of telecommunications data in particular classes of investigations:

> Looking at AFP investigations commenced between July and September of this year, 2014, I can advise that telecommunications data has been used in 92 per cent of counterterrorism investigations, 100 per cent of cybercrime investigations, 87 per cent of child protection investigations and 79 per cent of serious organised crime investigations.[36]

2.36 Victoria Police highlighted to the Committee how changes in the broader communications environment are requiring agencies to rely on telecommunications data as an increasingly integral part of their investigations:

> In an age where there is an ever-increasing reliance across virtually all elements of our community on telecommunications in its various forms, coupled with increasingly sophisticated telecommunications technologies, law enforcement must be able to stay abreast of the tools of the trade or the modus operandi of the similarly empowered and sophisticated criminal element who are always amongst us.
>
> One of the touchstones of investigation that junior investigators are taught is the notion that every contact leaves its trace. In the past, this was intended to draw the investigator's attention to the possibilities of fibres, fingerprints and DNA evidence. In the present, this thinking is just as applicable to the opportunities provided to serious and organised crime investigators by metadata …
>
> An investigation can be considered to be a process underpinned by a series of logical and ordered steps, and the identification, analysis and interpretation of the traces that an offender has left behind in the course of his or her preparatory actions or actual offending will always be amongst the critical first steps that can ultimately determine the success or otherwise of an investigative

35 AFP, *Submission 7.1*, p. 3.

36 Commissioner Andrew Colvin, AFP, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

> process, whether such traces are in the form of a fingerprint or a call charge record.[37]

2.37 The Australian Securities and Investments Commission (ASIC) highlighted the important role that telecommunications data plays in the initial stages of an investigation, and noted that the absence of such information can result in investigations failing before they truly even commence.[38]

2.38 Mr Michael Griffin, the recently-appointed Commonwealth Law Enforcement Integrity Commissioner, and a former Director of Military Prosecutions for the Australian Defence Force; Examiner of the Australian Crime Commission; and Principal Member, Senior Member and Member of the Administrative Appeals Tribunal, Migration Review Tribunal and Refugee Review Tribunal, and of the Veterans' Review Board, explained the role historic telecommunications data plays in anti-corruption investigations involving compromised law enforcement officials:

> I have had the benefit of being briefed on all of [the Australian Commission for Law Enforcement Integrity's] current operations as well as a number of past investigations. In my review of these cases, the thing that has struck me the most is the lengths to which corrupt officers will go to cover their tracks. Accordingly, telecommunications data is essential to finding corrupt conduct and can be crucial to its successful prosecution.
>
> …
>
> [T]he particular area of interest to us relates to people who are presently covering their tracks, and very recently covering their tracks. It is unlikely that the connections they have made will be present contemporaneously. Therefore, it is the historical record that is important to us, and looking at our history of investigations, we are of the view that the two-year period works for us. Although, as you will see from Operation Heritage-Marca, we have looked at historical data, where it has been available, that has gone back several years, indeed to 2006 in Operation Heritage-Marca.[39]

2.39 The AFP also drew the Committee's attention to the important role that telecommunications data plays in enabling and supporting the use of

---

37 Inspector Gavan Segrave, Intelligence and Covert Support Command, Victoria Police, *Committee Hansard*, Canberra, 30 January 2015, p. 44.

38 Australian Securities and Investments Commission (ASIC), *Submission 24*, p. 9.

39 Mr Michael Griffin AM, Integrity Commissioner, *Committee Hansard*, Canberra, 29 January 2015, pp. 34–35.

other investigative powers that Parliament has granted law enforcement and national security agencies:

> Intercepted or accessed content played a role in at least 328 convictions [by the AFP] over the past five years. In each of these cases telecommunications data was a crucial tool to ensure that those more intrusive capabilities were appropriately targeted and deployed.[40]

2.40 The New South Wales Police Force (NSW Police) also provided further evidence in support of the nexus between telecommunications data and telecommunications interception.[41]

What data is accessed?

2.41 Victoria Police emphasised to the Committee that the extensive use of telecommunications data at the early, intelligence stages of investigations should not be misinterpreted as agencies engaging in unjustified 'fishing expeditions':

> I think there is potential for some observers to misconstrue this idea of law enforcement using metadata in terms of intelligence. It needs to be tied back to an understanding of the investigative process … It is important for people to understand that in most instances metadata is used at the early stages of investigations when police are trying to get an understanding of a whole range of things in relation to the circumstances under investigation. I think this is what we mean when we talk about it being used in an intelligence sense, not that it is some broad fishing expedition because we have nothing better to do.[42]

2.42 South Australia Police explained to the Committee how the concepts of 'reasonable necessity' and 'relevance', which are core elements of the statutory test for authorised officers making a data authorisation under Chapter 4 of the TIA Act, are applied:

> The legislation talks about it being reasonably necessary and relevant. To me, if person A is murdered, who has had contact with that person in the previous 24 hours, 48 hours, seven days is quite relevant to that murder investigation, and that is what we are asking at that point in time. It is the same with a drug

40 AFP, *Submission 7.1*, p. 5.

41 Detective Superintendent Arthur Kopsias APM, Commander, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard*, Canberra, 30 January 2015, p. 49.

42 Inspector Segrave, *Committee Hansard*, Canberra, 30 January 2015, p. 59.

> trafficker: whom that person has had contact with is relevant to that investigation.[43]

2.43 The Director-General of Security also drew the Committee's attention to how the limits and controls on ASIO's access to telecommunications data, which are contained in both the TIA Act and the *Attorney-General's Guidelines* made under section 8A of the *Australian Security Intelligence Organisation Act 1979*, are applied in practice:

> ASIO is careful to ensure that the level of intrusion into individual privacy remains proportionate to that threat and in accordance with the guidelines that were provided by the Attorney-General. It is not and will not be the case that ASIO automatically requests the maximum amount of data available. Should this bill become law, ASIO will continue to request access to historical communication data needed only for the purpose of carrying out our function, regardless of the length of time that data may be available for. We abide by the law.[44]

2.44 In response to a question from the Committee, a senior official of the Australian Commission for Law Enforcement Integrity (ACLEI) confirmed that access to historical telecommunications data would itself likely play a key role in any investigation by ACLEI of any alleged corrupt access to or misuse of telecommunications data by a law enforcement official.[45]

2.45 Telstra noted that there appear to be significant public misconceptions about the nature and extent of access to telecommunications data by Australian law enforcement and national security agencies:

> I think that there is often a lot of mystery around it. Very simply, it is often very simple metadata—the same sorts of information that you might be able to access from your bill: who you called; where you were when you made the call, by cell tower; a name and a billing address. I am sure people perceive that it is mysterious. It is actually, often—most times—very simple metadata.[46]

2.46 Telstra's statement is consistent with the Attorney-General's Department's submission to this inquiry,[47] and the AFP's submission to the Senate Legal and Constitutional Affairs References Committee's *Inquiry into the*

43 Assistant Commissioner Paul Dickson, Crime Service, South Australia Police, *Committee Hansard*, Canberra, 30 January 2015, p. 60.

44 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 65.

45 Mr Nick Sellars, Executive Director, Secretariat, Australian Commission for Law Enforcement Integrity, *Committee Hansard*, Canberra, 29 January 2015, p. 35.

46 Mrs Kate Hughes, Chief Risk Officer, Telstra, *Committee Hansard*, Canberra, 29 January 2015, p. 17.

47 Attorney-General's Department, *Submission 27*, p. 61.

Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979.[48] This evidence indicates that approximately 85 per cent of data authorisations relate to subscriber information, such as name and address information, with only 15 per cent relating to 'traffic data', such as call charge records.

2.47 At a public hearing with the Committee, Victoria Police also highlighted that the number of data authorisations made each year by law enforcement agencies does not reflect the number of persons under investigation using those powers:

> **Inspector Segrave:** The numbers that have been put before you today, in terms of the applications, reflect the uptake of the broader community of the communications technologies that are available. Obviously, they have increased exponentially over time and the law enforcement figures just reflect that. The other point that I would make in relation to those numbers, certainly from a Victoria Police point of view—and I would be confident that that extends across other law enforcement agencies—is that it should not be interpreted that, if we have made 60 000 requests in a year, that is 60 000 individuals. A lot of the organised crime figures that are investigated and where these tools are utilised routinely drop phones and roll phones over, so there are multiple requests in relation to that. There may be multiple requests in relation to call charge records over periods of time, and so on. Another aspect that needs to be understood is that, if you were to drill down into those figures, the actual numbers, in terms of the individuals that are the subject of the applications, are much less than the bottom line figure—[49]

2.48 Victoria Police went on to confirm that there may be many hundreds of requests for telecommunications data for a single investigation that may only relate to 'half a dozen or a dozen individuals'.

> **Mr DREYFUS:** Can I reassure you, Inspector, on behalf of myself and my colleagues, that we have been given, in closed hearings, by the Australian Federal Police and ASIO, multiple examples of exactly what you are talking about. I am not disclosing anything here. For major investigations, there will be hundreds of requests for telecommunications data for a single investigation—
>
> **Inspector Segrave:** Indeed. That is the experience across—

48 AFP, *Submission 25*, Senate Legal and Constitutional Affairs References Committee, pp. 5–6.

49 Inspector Segrave, *Committee Hansard*, Canberra, 30 January 2015, p. 60.

> **Mr DREYFUS:** possibly only covering half a dozen or a dozen individuals, but nevertheless there are hundreds of requests. So, take it from me, and I think I can speak for my colleagues: we are not assuming—it is quite the reverse—that the 60,000 requests from your force or the 122,000 requests from New South Wales describe a number of persons. Far from it. [50]

A 'self-service' regime?

2.49 A number of submissions and witnesses argued that the existing controls in the TIA Act around access to telecommunications data are inadequate. For example, Professor George Williams argued that the current regime for access to telecommunications data is something of an accident of history, and that it should be reformed:

> my underlying concern is that I do not think the current system is appropriate, but I think it is somewhat accidental that we have got to this position where agencies can access vast amounts of data—tens of thousands, perhaps, over a number of years—without any form of clear political accountability. I think the scheme has grown up without actually being designed properly. And if we were starting fresh—let us say we did not have this data access that we have at the moment—I do not think there would be any doubt about the need to have some sort of authorisation process in play. It is just that we have this unfortunate ad hoc regime that I think we need to move beyond.[51]

2.50 The Law Council argued that the introduction of a mandatory data retention regime would increase the risks under an internal authorisation model for access to telecommunications data:

> under the proposed data retention regime, vastly more telecommunications data will be available – both in terms of volume and potentially the quality of the data retained – than is currently the case. This change heightens the risk of an encroachment on rights of privacy.[52]

2.51 The Committee accepts that the adequacy of safeguards around access to telecommunications data are relevant to the proportionality of the proposed data retention regime. Chapters 6 and 7 of this report address the controls and safeguards around telecommunications data in detail.

---

50 Inspector Segrave, *Committee Hansard*, Canberra, 30 January 2015, p. 60.

51 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 11.

52 Law Council of Australia, *Submission 126*, p. 18.

The challenges facing national security and law enforcement investigations

2.52 The Government has indicated that it considers the implementation of a mandatory data retention regime to be an urgent priority to address challenges facing Australia's national security and law enforcement agencies.[53]

2.53 However, the Law Council of Australia argued that the Government has not demonstrated the urgency or pressing social need underpinning the Bill. The Law Council regarded the fact that 'certain features' of the Bill will not commence until six months after Royal Assent, and that the overall scheme will not be fully functional for a further 18 months after commencement, as indicating an absence of such an urgent need.[54]

2.54 In evidence, the Law Council went somewhat further, arguing that there is no evidence that the current regime was ineffective:

> [T]he examples [given] were examples where the metadata had been available under the existing voluntary regime. So that does not demonstrate the necessity of this new regime; it demonstrates that the existing regime is working.
>
> The difficulty is that submitters to this inquiry were asked to take on face value the statement that carriers are in fact reducing the amount of information that they retain such that the voluntary disclosure regime may become less effective over time. I do not think that that has been demonstrated in evidence or at least that I have seen in the submissions.[55]

2.55 Guardian Australia also noted the longstanding nature of the debate around mandatory data retention, including this Committee's consideration of the issue in 2012–13:

> Debate about interception, storage and use of Australians' communications for security and law enforcement purposes is longstanding, not a product of relatively recent concerns about a particular strain of terrorism.[56]

53 The Hon. Tony Abbott MP, Prime Minister, Transcript of Joint Press Conference with the Minister for Justice, the Hon. Michael Keenan MP and the Commissioner of the AFP, Mr Andrew Colvin APM OAM, 5 February 2015, Melbourne.

54 Law Council of Australia, *Submission 126*, pp. 6–7.

55 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 31.

56 Guardian Australia, *Submission 132*, p. 3.

2.56 Mr Virgil Hesse cautioned the Committee against overreacting to recent events, such as the incidents in Sydney, Paris and Ottawa, when considering this proposal:

> Sadly recent events have left State and Federal Law Enforcement asking questions which in hindsight point to a breakdown across the Law Enforcement's and their ability to adequately monitor one individual who had intentions no one person could predict.
>
> I would ask the Committee to be very careful in reacting emotively with regard to this aberration when considering the third tranche of legislation, that being the Data Retention component.[57]

2.57 The Committee noted evidence that data retention would likely not have enabled agencies to prevent these incidents. NSW Police gave considered evidence on this point, emphasising that attempting to determine whether such information could have assisted in hindsight necessarily involves a hypothetical, counterfactual exercise:

> [A]s a hypothetical, with the nature of Sydney itself and where law enforcement would benefit from metadata in relation to, say, the Sydney incident, it most likely would not have prevented the Sydney incident. At the time, metadata could have been essential in trying to identify any other persons who may be engaged in a group or involved in that type of offence. Historical metadata could still benefit police down the track to see who that person has associated with in terms of a cell or, if they have been radicalised, where they come from.[58]

2.58 The Attorney-General's Department and a number of agencies noted that long-term changes in the telecommunications industry are impacting a number of key investigative capabilities. These changes are being exacerbated by an increasingly high-risk operational environment.

2.59 This section of the report will consider evidence received regarding:

- the declining ability of agencies to reliably access the content of communications,
- the declining ability of agencies to reliably access telecommunications data about communications, and
- the extent to which the current operational environment is exacerbating these challenges, increasing the urgency of the reform.

---

57 Mr Virgil Hesse, *Submission 15*, p. 1.

58 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, pp. 61–62.

Declining ability to reliably access the content of communications

2.60 The Attorney-General's Department noted that the ability of law enforcement and national security agencies to access the *content* of communications is in long-term decline, as a result of ongoing technological change. The Department claimed that this decline is degrading the ability of agencies to investigate serious threats, such as organised crime and terrorist cells. As a result, agencies are 'increasingly reliant on alternative investigative techniques, including access to telecommunications data'.[59]

2.61 NSW Police provided a valuable explanation of this challenge:

> It is a pretty broad topic but it is also very close to my heart as I have been the [telecommunications interception (TI)] commander for 15 years. I have been doing interceptions for 15 years. I have managed thousands and thousands of intercepts. But, in the last four or five years, the phrase 'going dark' has come about in terms of the strong encryption out there, lots of over-the-top providers providing apps, the online process. The advent of the internet, if I could explain it to you, has actually degraded our interception capability to the point where we are receiving a lot less than we used to receive.
>
> When I went to the [Telecommunications Interception Branch], I used to apply for the warrants. I used to go before Federal Court judges; in those days, we did not have AAT members. I used to go down with a request for the warrant, the same warrant that is served today, and present it before the member, present our case with the affidavit, come back with a warrant and serve it on the carrier. In those days, we had the luxury of one carrier. We would get all communications related to Mal Lanyon, say—everything. It was not a problem. It was easy. Any words spoken were what was said over the phone. The audio was easy to work out. But with the advent of the internet, although it is the same warrant today to the same member, there are about 600 or 700 potential ISPs and carriage service providers out there; and, when we serve the warrant, I am not getting the content, the communications, I used to get, to the point where we have to do other things—I cannot disclose those things in this forum—to complement the TI process.
>
> So we are exploring alternative methods of operational deployment and other forms of electronic surveillance services to fill in the gaps. There is a gap there. Encryption has become

59 Attorney-General's Department, *Submission 27*, p. 13.

> mainstream now, with the Snowden impact; we have over-the-top applications and the smartphones out there: all those things are impacting on us. I am not saying they are bad for the global community. I think there are some good things in there, but for us it is hard just to keep abreast.[60]

2.62 The Attorney-General's Department also noted that the relative value of telecommunications data to investigations is increasing as communications technology plays an increasing role in activities prejudicial to security, including cyber-espionage, and serious criminal activity.[61]

Declining ability to reliably access telecommunications data

2.63 The Attorney-General's Department noted that the ability of agencies to access telecommunications data is in long-term decline, reducing the value of data both as a primary investigative tool, and impairing the ability of agencies to mitigate the loss of capability they are experiencing as a result of the ongoing loss of access to the content of communications. The Committee identified this issue as a key challenge to national security investigations in its 2013 Report.[62]

2.64 The Department confirmed that this trend 'has continued unabated since the Committee's report, with further, significant reductions in the period for which certain service providers retain critical telecommunications data'.[63]

2.65 In its submission, the Attorney-General's Department drew a distinction between the increasing volume of telecommunications data being retained across the telecommunications industry, and retention practices in relation to particular categories of telecommunications data that are of any significant utility for national security and law enforcement purposes:

> It is important to distinguish between industry retaining telecommunications data in general, and retaining the types of telecommunications data that are critical to law enforcement and national security investigations. While it is true that, across the telecommunications industry, more telecommunications data is generated and retained than at any previous point in history,

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

61 Attorney-General's Department, *Submission 27*, pp. 11–12.

62 PJCIS, *Report of the inquiry into potential reforms of Australia's national security legislation*, Canberra, May 2013, p. 190.

63 Attorney-General's Department, *Submission 27*, p. 13.

> much of this data is of limited, if any, investigative value and would not be subject to data retention obligations.[64]

2.66 The evidence received by the Committee over the course of this inquiry outlined two distinct challenges:

- a general decline in the availability of telecommunications data, and
- the inconsistent availability of telecommunications data for similar services provided by different providers, and between different services provided by the same provider.

Declining availability of telecommunications data

2.67 The AFP explained the challenge facing law enforcement agencies as a result of declining retention practices for critical categories of telecommunications data:

> Telecommunications data is a critical component of investigations and has been successfully used to support numerous investigations into serious criminality from many, many years. Industry already captures much of this data, but, as more services become available, providers are keeping fewer records for shorter periods of time.[65]

2.68 In his second reading speech to the House of Representatives following the introduction of the Bill, the Minister for Communications, the Hon Malcolm Turnbull MP, provided an example of the decline in retention practices and their potential to impact on national security investigations:

> Last year, a major Australian ISP reduced the period for which it keeps IP address allocation records from many years to three months. In the 12 months prior to that decision, the Australian Security Intelligence Organisation (ASIO) obtained these records in relation to at least 10 national security investigations, including counter-terrorism and cybersecurity investigations. If those investigations took place today, vital intelligence and evidence simply may not exist.[66]

2.69 In its submission, the Attorney-General's Department provided two specific examples where, since this Committee's 2013 report, major Australian service providers have substantially reduced their holdings of IP address allocation records and other critical data types. The Department advised that the impact of one of these changes is that, '[a]s a

64 Attorney-General's Department, *Submission 27*, p. 13.

65 Commissioner Andrew Colvin, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

66 The Hon Malcom Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12561.

direct result of this action, agencies are unable to reliably identify suspects or execute interception warrants on this carrier's network.'[67]

2.70 Mr Chris Berg, Senior Fellow at the Institute of Public Affairs, summarised the challenge facing agencies in the following terms:

> The existing telecommunications data access regime takes advantage of a practice that telephone providers utilise for business purposes – the recording of data about the time, length, and parties to an individual telephone call. This information is retained in order to accurately bill customers, as telephone services are billed typically on a per-call basis or some variation of that system. From this data large amounts of information can be gleaned, but it is important to note that the data exists independently of its law enforcement uses. The data has been created by telecommunications providers for specific business purposes.
>
> In the internet era, this sort of data is both less important and less accessible. Communication that was once done by phone might be done over email, or in a chat room. Telephone calls which were logged on a per-call basis might be conducted over purely internet telephonic services like Skype. Rather than selling customers per-call access, now telecommunications is sold in large blocks of data. The only information needed for billing purposes with internet access might be download volumes. Even then that might not be necessary, either in the case of unlimited download plans or simply because excess downloads are 'shaped' – that is, offered freely at a reduced speed – rather than charged back to the customer.[68]

2.71 In its submission, ASIO provided a similar assessment of the underlying drivers of the decline in retention practices.[69]

2.72 Agencies provided a large number of case studies addressing situations where the non-retention of telecommunications data hampered law enforcement and national security investigations. For example, NSW Police explained to the Committee how changing industry retention practices are impacting on its investigations:

> There were only about 1 100 requests [for IP data in 2013–14], of which conservatively 80 per cent failed to yield a subscriber from

67 Attorney-General's Department, *Submission 27*, p. 16.

68 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 4.

69 ASIO, *Submission 12.1*, p. 20.

> the other end because, without the legislation, carriers are not required to keep the proposed data sets.
>
> Similarly, on metadata call charge records, investigators get very skilled at knowing which carriers they can get data from and which they cannot. They know very well, so the level of requests that go to carrier A, knowing that they only hold that data for four to six seeks, is obviously reduced. There is no point putting a request in if we know the carrier does not hold the data for that long.[70]

2.73 Similarly, South Australia Police explained how the inability to access 14-month old telecommunications data in a murder investigation hampered efforts to investigate a newly-identified suspect:

> A stalled murder investigation was reviewed about 14 months after the victim's death. Fresh information received during the review identified a suspect who was a known drug dealer. The victim, a regular drug user, had been in contact with the suspect and investigators suspect the victim may have been killed over a drug debt. Historical telecommunications data was sought for the suspect's mobile service for around the time of the murder but it was no longer available. The unavailability of the telecommunications data has been detrimental to the investigation and the case remains unsolved.[71]

2.74 The major service providers each provided the Committee with assurances that they do not currently intend to further reduce their retention practices.[72] For example, in response to a question as to whether there was any imminent proposal to reduce the data that it keeps, Telstra, responded:

> We have no proposals to substantially reduce our data holdings at this point in time. What we have at the moment is sufficient to meet our regulatory obligations and to manage our network and provide services to customers.[73]

2.75 However, these assurances must be viewed in light of the providers' further evidence that services providers are likely to release *new* services,

---

70 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, p. 49.

71 South Australia Police, *Submission 9*, p. 3.

72 Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard*, Canberra, 29 January 2015, pp. 18–19; Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (Vodafone), *Committee Hansard*, Canberra, 29 January 2015, p. 64; Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Singtel-Optus (Optus), *Committee Hansard*, Canberra, 30 January 2015, p. 21.

73 Mr Shaw, *Committee Hansard*, Canberra, 29 January 2015, pp. 18–19.

update the underlying architecture of their existing networks and services, and transition subscribers and communications onto IP-based platforms in the future. This may further reduce the availability of telecommunications data for national security and law enforcement purposes. For example, Telstra also explained that:

> As we change our business, as we introduce new products, or we might phase out an old system and introduce a new system—a new building platform or something, for instance—we would design that in order to meet business needs and whatever regulatory obligations there are. If that meant that we kept less data because we did not need to keep it, then that would be an artefact of that particular process.[74]

2.76 Similarly, Vodafone explained that, while it does not currently intend to reduce its retention practices in relation to its traditional telephony network, it expects that increasingly large volumes of communications will occur via newer, IP-based technologies. For these technologies, less telecommunications data is kept, and such data is kept for significantly shorter periods of time.[75]

2.77 Optus also observed that it is the migration of customers and services to newer platforms, which have shorter retention periods, that is driving down the overall period for which relevant telecommunications data is retained:

> I think the main influence on change and the overall character of the dataset, if you were to look at it in the very broad, is that increasingly communications are moving to mobile services and increasingly—even with what we would regard as voice communications between ourselves—they are in effect data, and that has an influence on how data is kept.[76]

Inconsistent availability of telecommunications data

2.78 The Committee received evidence from law enforcement agencies and ASIO that the *inconsistent* retention of data between providers, and between services offered by the same provider, poses a considerable challenge. That is distinct from the declining retention of critical telecommunications data across the industry.[77]

2.79 For example, Commissioner Colvin explained that:

74 Mr Shaw, *Committee Hansard*, Canberra, 29 January 2015, p. 14.

75 Mr Lobb, *Committee Hansard*, Canberra, 29 January 2015, p. 66.

76 Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Optus-Singtel (Optus), *Committee Hansard*, Canberra, 30 January 2015, p. 21.

77 For example, South Australia Police, *Submission 9*, p. 1.

> When the AFP are dealing with serious threats to national security and other serious crime, we cannot afford to rely on luck to see if the provider that the criminal has chosen to use has retained that data. I also do not think the public would consider that an acceptable outcome for serious criminal investigations.[78]

2.80 The AFP further explained that sophisticated criminals actively exploit the inconsistent retention practices between providers:

> We want standardisation. Also, we do not want the crooks to shop. We do not want them to go to the providers who they know keep the data—and it will not take long to work out who keeps the data and who does not keep the data. We do not want them to sit there and say, 'That's the best network to go if you are a criminal, because we know that they are not going to keep the IP addresses if it is dynamic. They are not going to keep it for any length of time. They might keep it for three months, because that is what their business model says, but beyond that that is fine. Why we do not go to one of the big ones at the moment is because they keep it for—for however long they keep it—a long period of time'. We do not want that to happen. We want a consistent model, so that we have a level playing field and the people we are trying to combat against also have a level playing field.[79]

2.81 The AFP confirmed that the risk of sophisticated criminals actively seeking out providers with more limited retention practices is not hypothetical, and is 'absolutely' occurring at present.[80]

2.82 Mr Chris Dawson, Chief Executive Officer of the Australian Crime Commission (ACC), explained the importance of reliable and consistent access to historic telecommunications data, noting that the ACC investigates 'complex communications webs which are often only able to be discovered through retrospective analysis of criminality which span at times many years.'[81]

2.83 ASIO provided a summary of its assessment of current industry retention practices, demonstrating their wide variability.[82] A copy of this table is included in the detailed discussion on retention periods in Chapter 4 of this report (Table 4.2).

---

78 Commissioner Andrew Colvin, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

79 Deputy Commissioner Michael Phelan APM, Australian Federal Police, *Committee Hansard*, Canberra, 17 December 2014, p. 15.

80 Deputy Commissioner Phelan, *Committee Hansard*, Canberra, 17 December 2014, p. 15.

81 Mr Chris Dawson, Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, Canberra, 17 December 2014, p. 6.

82 Australian Security Intelligence Organisation, *Submission 12.2*, p. 5.

2.84 Optus noted the current inconsistencies and the potential for these disparities to increase over time:

> [T]his regime is bringing everyone to a common set of standards. At the moment, probably the vast bulk of communications pass through the three major carriers in some form or another by means that are captured relatively well for the purpose of a regime like this one that we are discussing, but increasingly there is the potential for that to fragment. Indeed, people are always on the lookout for something. You will have seen media reports, for example, [about] drug syndicates and bikie gangs. There was a reason for that. Whether they can feel entirely confident of what they are up to is another thing, but they have clearly tried it on because they are of the belief that they can evade the protections that apply or the enforcement regime that applies in Australia through mainstream services.[83]

2.85 Optus went on to confirm that the concerns regarding the inconsistent retention of telecommunications data sought by law enforcement agencies did not just relate to the major carriers:

> I think it is a combination of a smaller part of the market, fragmentation in the market, technological alternatives and a broader change to what I would call crudely a data based regime for communications, rather than necessarily a traditional PSTN type voice regime.[84]

2.86 The level of inconsistency was most clearly highlighted by the evidence from Telstra, which confirmed that agencies' ability to access telecommunications data could vary significantly depending on which day of the year the request relates to:

> Some of the data that is being sought on a quiet day might be kept for a couple of weeks but on New Year's Eve is on the network for only a few hours.[85]

Higher risk operational environment

2.87 The Attorney-General's Department explained that the 'increasingly high-risk operational environment',[86] particularly the increased threat of domestic terrorism, has exacerbated the capability gaps experienced by agencies:

---

83 Mr Epstein, *Committee Hansard*, Canberra, 30 January 2015, pp. 21–22.

84 Mr Epstein, *Committee Hansard*, Canberra, 30 January 2015, p. 22.

85 Mr Shaw, *Committee Hansard*, Canberra, 29 January 2015, p. 14.

86 Attorney-General's Department, *Submission 27*, p. 12.

> [I]n an increased threat environment characterised by a higher operational tempo, there is a narrower margin for error in law enforcement and national security investigations. This narrower margin is particularly evident in relation to 'lone wolf' threats: such persons have limited, if any, contact with other known extremists, giving authorities fewer opportunities to detect their activities and intentions. As such, any missed opportunity to identify and prevent these attacks represents a significant risk.[87]

2.88 The Department noted that, where telecommunications data is not retained, it can result in missed opportunities:

> In the best case, agencies may be able to progress investigations by using more resource-intensive methods (limiting their capacity to investigate other matters) or more intrusive investigative techniques.
>
> In the worst case, a crime or threat to security will not be adequately investigated.[88]

2.89 ASIO's submission described the scale of the challenge it is facing to identify, investigate and prevent terrorist attacks in Australia at present:

> Presently, there are over 300 counter-terrorism investigations, of which a third are high threat priority cases. High threat cases are ones in which ASIO holds credible information requiring time critical action to resolve or monitor. The dominant theme across these cases is the conflicts in Syria and Iraq.[89]

2.90 The Attorney-General's Department also noted the increasing risk posed by cyber-espionage, and the importance of telecommunications data to combat that risk:

> Instances of espionage and foreign interference within Australia have continued to increase, both in terms of the number of occurrences and the range of operatives. In particular, the scale and sophistication of cyber-espionage conducted against Australian Government and private sector systems has increased significantly …
>
> … [A]ccess to telecommunications data and the lawful interception of… communications are often both crucial aspects of counter-espionage investigations.[90]

---

87 Attorney-General's Department, *Submission 27*, p. 15.

88 Attorney-General's Department, *Submission 27*, p. 15.

89 ASIO, *Submission 12.1*, p. 15.

90 Attorney-General's Department, *Submission 27*, pp. 11–12.

2.91 The Commissioner of ASIC highlighted the need for reliable access to telecommunications data to combat the increasing global threat of insider trading:

> It is not like terrorism, and I do not make a case that it is exactly the same as terrorism. That would be churlish and, frankly, stupid. But insider trading is an especially pernicious activity. If insider trading is permitted to continue, retail investors and institutional investors will lose confidence in the Australian market. Australia is a net importer of capital—a very major net importer of capital—and if foreign investors in particular, let alone Australian investors, lose confidence in our market, we lose this whole engine and multiplier effect that we have through our capital markets for efficient capital raising. … I am not equating this to a terrorist act, but I am equating this somewhat to other crimes which cause physical harm to people. It is very difficult for a person who has lost their life savings to recover, particularly if your are at that part of your life… where you do not have a lot of time to recover a deadweight loss.[91]

2.92 The Director-General of Security also addressed the question of whether the two-year implementation timeframe following the Bill receiving Royal Assent runs counter to the argument that the passage of the Bill is required to address these urgent operation pressures:

> We had a discussion internally about this. From the time of Royal Assent, there is no … backsliding in terms of the data that is being held by the telecommunication companies at that point.[92]

2.93 Additionally, the Attorney-General's Department's explained that one of the core objectives of the implementation planning arrangements proposed to be established by the Bill is to:[93]

> ensure that service providers achieve substantial compliance with their data retention obligations early in the implementation phase by encouraging interim data retention solutions, for example, by increasing storage capacity for existing databases to approach the two year retention period, or by prioritising the implementation of full data retention capability for some services or kinds of data.

2.94 The implementation arrangements for the proposed data retention scheme are discussed later in the report.

---

91 Mr Greg Tanzer, Commissioner, ASIC, *Committee Hansard*, Canberra, 29 January 2015, pp. 4–5.

92 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 69.

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

Reconciling data retention with privacy and civil liberties concerns

2.95 In May 2013, the previous Committee cautioned that:

> A mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed.[94]

2.96 The Bill's Statement of Compatibility with Human Rights identifies that the proposed data retention regime would engage the right to protection against arbitrary or unlawful interferences with privacy, set out in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) (referred to hereafter as the 'right to privacy'),[95] as well as the right to freedom of expression, set out in Article 19 of the ICCPR. The Australian Human Rights Commission supported this assessment.[96]

2.97 The Attorney-General's Department recently gave evidence to the Senate Legal and Constitutional Affairs References Committee summarising the effect of Australia's obligations under Article 17:

> Article 17 of the International Covenant on Civil and Political Rights sets out the right of persons to be protected against arbitrary or unlawful interference with their privacy. In order to avoid being arbitrary, any interference with privacy must be necessary to achieve the legitimate purpose and proportionate to that purpose.[97]

2.98 The Australian Privacy Commissioner, Mr Timothy Pilgrim PSM, drew the Committee's attention to the test put forward by the Office of the United Nations High Commissioner for Human Rights:

> The 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 a right (an interference with privacy, for example, for the purposes of

94 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, p. 190.

95 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 10.

96 Australian Human Rights Commission, *Submission 42*, p. 4.

97 Ms Katherine Jones, Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 44.

> protecting national security or the right to life of others) must be shown to have some chance of achieving that goal.[98]

2.99 The Law Council of Australia also endorsed this test.[99]

2.100 Mr Vaile and Mr Remati of the University of New South Wales discussed how the Committee should approach the question of whether the scheme is necessary and proportionate:

> Proportionality requires identification and weighting of benefits and costs or risks for the proposal, and for its realistic alternatives. We need to avoid considering benefits or costs in isolation, or overlooking whether an effective alternative with better proportionality exists.
>
> …
>
> 'Necessity' and 'effectiveness' are key factors on the benefits side. Consideration of the effectiveness of alternatives is also a necessary part of consideration of necessity.[100]

2.101 As the Australian Human Rights Commission also noted, the mere fact that a law interferes with privacy or freedom of expression does not make that interference disproportionate, nor does it make that law unjustified. In the Commission's view:

> Human Rights Law provides significant scope for [law enforcement and national security] agencies to have expansive powers, even where they impinge on individual rights and freedoms. Such limitations must, however, be clearly expressed, unambiguous in their terms, and legitimate and proportionate to potential harms.[101]

2.102 Following on from the 2013 report of this Committee, which emphasised the need to address privacy and civil liberties concerns raised by mandatory data retention, the following sections consider the evidence received by the Committee about the necessity, efficacy and proportionality of a data retention scheme as a response to the current risk environment.

---

98 Office of the Australian Information Commissioner, *Submission 92*, p. 4, quoting 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), p. 23.

99 Dr Natasha Molt, Senior Policy Lawyer, Criminal Law, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 32.

100 Mr Vaile and Mr Remati, *Submission 194*, p. 3.

101 Australian Human Rights Commission, *Submission 42*, p. 3.

Can data retention meet the test as being necessary for a legitimate aim?

2.103 The Explanatory Memorandum identifies that the legitimate aim, or aims, of a data retention scheme are:

> the protection of national security, public safety, addressing crime, and protecting the rights and freedoms … by requiring the retention of a basic set of communications data required to support relevant investigations.[102]

2.104 The Parliamentary Joint Committee on Human Rights has reported on the Bill, and concluded that, in relation to the question of necessity:

> the committee considers that the statement of compatibility has generally established why particular categories of data are considered necessary for law enforcement agencies.[103]

2.105 However, the Committee received a number of submissions questioning the necessity of mandatory telecommunications data retention.

2.106 The Law Council of Australia argued that:

> [T]he case for mandatory data retention has not been made out because:
>
> - the ability of access to telecommunications data is not limited to national security or serious crime;
> - there is little evidence from comparable jurisdictions that had previously had mandatory data retention schemes to suggest that such schemes actually assist in reducing the crime rate, for example in Germany, research indicates that a mandatory data retention scheme led to an increase in the number of convictions by only 0.006%;
> - there is a lack of Australian statistical quantitative and qualitative data to indicate:
>   - ⇒ the necessity of telecommunications data in securing convictions; or
>   - ⇒ the cases where requests for telecommunications data could not be met because data had not been retained and its effect on an investigation.[104]

2.107 In evidence, the Law Council acknowledged that the evidence provided by agencies 'definitely have the benefit of showing why agencies such as the AFP consider the value of telecommunications data', but argued that

---

102 Data Retention Bill, *Explanatory Memorandum*, p. 10.

103 Parliamentary Joint Committee on Human Rights, *Fifteenth Report to the 44th Parliament*, p. 12.

104 Law Council of Australia, *Submission 126*, p. 7.

'there seems to be a lack of statistical data that indicates the value of such data'.[105]

2.108 A number of submissions cited the report alluded to by the Law Council, which was prepared by the Legal Services of the German Parliament.[106] Extracts of this report have been translated by the German privacy rights group, AK Vorrat.[107] The report is stated to have addressed Germany's data retention regime, which was in force between 1 January 2008 and 2 March 2010, and concluded that data retention had increased 'crime clearance rates' by 0.006%.

2.109 In a joint submission, the councils for civil liberties across Australia accepted that 'telecommunications data is an important investigative tool that and law enforcement and security agencies should have appropriate access to it'.[108] However, the councils noted that they:

> share the scepticism of many experts, parliamentarians, legal and civil society groups that the mass collection and retention of telecommunications data of non-suspect citizens for retrospective access will significantly increase Australia's (or any nation's) safety from terrorism and serious crime.[109]

2.110 The councils further drew the Committee's attention to the United States' Privacy and Civil Liberties Oversight Board's January 2014 *Report on the Telephone Records Program*. That program involved the collection by the United States Government of large volumes of call-charge records (the time, date, duration and phone numbers) from some US phone companies.[110] The Board's headline conclusion, which was referenced by the councils, was that 'we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.'[111] However, the Board also concluded that the program:

- identified one unknown terrorism suspect, although there was reason to believe that the Federal Bureau of Investigation (FBI) 'may have

105 Dr Natasha Molt, Senior Policy Lawyer, Criminal Law, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 30.

106 See, for example: Law Institute of Victoria, *Submission 117*, p. 8; Mr Vaile and Mr Remati, *Submission 194*, p. 4.

107 Available at: <http://www.vorratsdatenspeicherung.de/content/view/534/55/lang,en/> viewed 26 February 2015.

108 Councils for civil liberties across Australia, *Submission 129*, p. 8.

109 Councils for civil liberties across Australia, *Submission 129*, p. 9.

110 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 8.

111 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 11.

discovered him without the contribution of the National Security Agency's program',

- provided additional leads regarding the contacts of terrorism suspects, and
- demonstrated that foreign terrorist plots did *not* have a US nexus, allowing the US intelligence community to avoid false leads and to channel its limited resources more effectively.[112]

2.111 The Board also indicated that the Telephone Records Program provided little additional value to the FBI's more 'traditional', targeted powers, noting that:

- US service providers are already subject to long-standing data retention obligations under Federal Communications Commission Regulations that cover the telecommunications data collected under the program, ensuring that those records are relatively consistently available to the FBI,[113] and
- the FBI (and other US law enforcement agencies) have the power to access those records under an 'administrative subpoena', similar to data authorisations made under the TIA Act, making it possible to 'streamline this process and eliminate delays' in accessing the telecommunications data retained by service providers.[114]

2.112 The Department drew the Committee's attention to the European Commission's *Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, which concluded that:

- 'The European Union should support and regulate data retention as a security measure',
- 'The evidence… is limited in some respects, but nevertheless attests to the important role of retained data for criminal investigation', and
- 'These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons'.[115]

112 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 11.

113 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 141.

114 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, pp. 140–141.

115 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, p. 31.

2.113 The Commission also criticised the use of 'crime clearance rates' as an appropriate methodology to evaluate the effectiveness of data retention (internal citations omitted):

> [C]rime statistics – including the number of crimes and the number of crimes which are solved ('clearances') - are determined by multiple socio-economic factors, and success in tackling crime cannot be attributed to a specific security measure, such as data retention. Police use different methods for measuring crime clearance rates and, moreover, it may be argued that an undue focus on such statistics can be counterproductive to the effectiveness of law enforcement. In any case, it would not be possible to identify meaningful statistical trends only a few years after the [Data Retention Directive] entered into force.[116]

2.114 While claiming data retention to be a necessary tool, representatives of South Australia Police and Victoria Police highlighted the complexities of assessing its direct impact on investigative outcomes:

> **Assistant Commissioner Dickson:** It is a very difficult question to answer. In jury matters, it is difficult to know why a jury found a person guilty, as an example. Was it because of the metadata provided? Was it because of certain admissions made? Or was it because of the DNA evidence? It is very difficult to say that metadata was the reason that that person was convicted. Most convictions at the end of the day are because of a whole raft of different things and bits of evidence.
>
> **Inspector Segrave:** I will make another point there, if I may. The metadata, quite often, is a step in the process to the investigator to get to the evidentiary footing. Without the metadata, that evidentiary footing may never be achieved. But it is not actually represented or recognised in the brief of evidence that is put before a court. So it can be very hard to drill down into the brief and into the prosecution to have an understanding of the underlying role that metadata actually places. But I think law enforcement consistently says that, with our understanding of the investigative process and the application of metadata within that process routinely, it is critical to us.[117]

2.115 In response to later questioning, NSW Police further emphasised the difficulty in producing meaningful quantitative analysis for the utility of access to retained data:

---

116 European Commission (2013), *Evidence for necessity of data retention in the EU*, p. 8.

117 *Committee Hansard*, Canberra, 30 January 2015, p. 49.

> I do not think there would be a police force in Australia that would keep that sort of data and, as Mr Dickson alluded to before, one of the issues is that it is rarely a single source of data that is responsible. For example, metadata might identify a source for us and might contribute to the way we go with the first steps of an investigation but there would be a number of other contributors. So to say that it was simply purely as a result for metadata would be a very problematic statistic to keep and I do not know of a police force which keeps that sort of information.[118]

2.116 The Committee received a range of evidence and case studies highlighting the impact that the absence of telecommunications data can have on investigative outcomes. This evidence supplements evidence previously received by this Committee in the course of its 2012–13 inquiry, and other publicly-available information on this issue, including evidence received by the Senate Legal and Constitutional Affairs References Committee.

2.117 The Attorney-General's Department drew the Committee's attention to analysis conducted by the German Federal Police of the utility of retained data to their investigations, which demonstrated that:

> [O]f the investigations in which telecommunications data was accessed, that telecommunications data provided the *only* investigative lead in 45.4% of cases. Telecommunications data made an 'important' contribution in 92.7% of the remaining cases.[119]

2.118 In its submission, the AFP provided an unclassified summary of the impact that current, inconsistent data retention practices had on the outcomes achieved by Operation Drakensberg, a major online child exploitation investigation that commenced in November 2013 following a referral from UK authorities. The referral contained 333 IP addresses suspected of accessing child exploitation material hosted on a UK-based website in 2011, as well as a further 219 IP addresses that had not actually performed any transactions. The non-retention of IP address allocation records by Australian service providers meant that the AFP were unable to even commence investigations into more than 45 per cent of the IP addresses identified as being highest-risk—those that had likely accessed the child exploitation material. Of the remaining cases, where service providers had retained IP address allocation records for up to two years,

118 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, p. 61.

119 Bundeskriminalamt, *Statistical analysis of data collection in the BkA*, p. 13, quoted in Attorney-General's Department, *Submission 27*, p. 14.

the AFP were able to positively identify 139 suspects, a success rate of almost 80 per cent.[120]

2.119 In its supplementary submission, the AFP advised the Committee that it received 5 617 reports of online child sexual exploitation relating to Australian IP addresses in 2014, a 54 per cent increase from the previous year. As at 9:00am on 27 January 2015, the AFP had received 709 reports this year. If that rate continues, the AFP would receive approximately 9 585 reports this year, an increase of almost 71 per cent.[121] The AFP drew to the Committee's attention the findings of a 2013 study by the United Kingdom's Child Exploitation and Online Protection Centre, that 'up to 85 per cent of online child sexual exploitation offenders have, or at some point, will contact offend against a child'.[122]

2.120 The AFP also noted the potential for reports from its international counterparts to be delayed, which would require the AFP to access more historic telecommunications data, as was the case in Operations Drakensberg:

> The time taken in respect of the referral of an online child sexual exploitation matter by an international partner of the AFP, and the investigation by the AFP, is dependent on the complexities of the matter, evidence available, technology used, volume of data and the results available from internet service providers.[123]

2.121 The Uniting Church in Australia's Justice and International Mission Unit of the Synod of Victoria and Tasmania (hereafter referred to as the Uniting Church Justice and International Mission Unit) drew the Committee's attention to the recommendations of the Asia-Pacific Financial Coalition Against Child Pornography that 'both for Internet Service Providers and file sharing companies, data retention and preservation are critical functions in the fight against child pornography'.[124]

2.122 The Unit also observed that:

> The Bill does not provide law enforcement agencies with any additional powers, nor does it give them any capacity to access metadata beyond what they already have. However, they cannot

120 AFP, *Submission 7.1*, p. 11.

121 AFP, *Submission 7.2*, p. 2.

122 AFP, *Submission 7.2*, p. 1.

123 AFP, *Submission 7.2*, p. 2.

124 Asia-Pacific Financial Coalition Against Child Pornography, *Confronting New Challenges in the Fight Against Child Pornography: Best Practices to Help File Hosting and File Sharing Companies Fight the Distribution of Child Sexual Exploitation Content*, September 2013, p. 4, quoted in Uniting Church Justice and International Mission Unit, *Submission 76*, p. 5.

> access the information if the company that has it has wiped it before the police are able to request it.[125]

2.123 It was also argued that data retention is necessary to assist in the protection and promotion of human rights.

2.124 For example, the Attorney-General's Department, in evidence to the Senate Legal and Constitutional Affairs References Committee, summarised the Australian Government's obligations under international human rights law to take positive steps to protect and promote fundamental human rights. The Department noted that this obligation is achieved in part through the maintenance of effective law enforcement and national security capabilities:

> International law to which Australia is a party recognises that Australians have a right to security of person, which requires the government to protect a person's physical safety and right to life. That means we must have an effective criminal justice system and the capacity to undertake preventative operational measures to protect people from the worst behaviour of others. The Australian Government also has an obligation to provide the right to an effective remedy for victims of crime. That means agencies need the investigative tools that will enable offenders to be brought to justice.
>
> The government believes that effective access to telecommunications data is critical to the government meeting those responsibilities. In investigating past crimes and deterring and preventing future crimes, Australia's agencies have come to rely heavily on telecommunications data. This should not be surprising, given how heavily the broader Australian population and the criminal element without our broader population have come to rely on communications technology … It is particularly necessary during the early stages of investigating crimes, where telecommunications data availability can often determine whether or not an investigation can succeed and the human rights of the victim can be protected.[126]

2.125 The Uniting Church Justice and International Mission Unit's submission contained a detailed review of Australia's human rights obligations in relation to online child exploitation. In particular, the Unit drew the

125 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 9.

126 Ms Jones, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 43.

Committee's attention to the United Nations Human Rights Council's Resolution A/HRC/8/L.17 of 12 June 2008, calling on governments:

> 2(g) To establish mechanisms, where appropriate, in cooperation with the international community, to combat the use of the Internet to facilitate trafficking in persons and crimes related to sexual or other forms of exploitation and to strengthen international cooperation to investigate and prosecute trafficking facilitated by the use of the Internet.[127]

2.126 The Unit then noted Australia's obligations under Articles 7, 8 and 17 of the ICCPR, Articles 16 and 34-36 of the *Convention on the Rights of the Child*, and Article 9 of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* to protect children from the cruel, degrading and inhuman treatment, sexual servitude, and violations of their privacy, honour and reputation associated with child exploitation, and argued that:

> The demonstrated likelihood that without data retention (as proposed in the Bill) hundreds, if not thousands, of offenders engaged in online child sexual abuse offences will escape detection and prosecution over time, should outweigh any concerns about the impact of data retention on the right to privacy.
>
> …
>
> It needs to be stressed that for the vast majority of Australians, law enforcement will never access the data retained under the requirements of the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, so the Unit rejects the arguments that retaining data is a violation of the privacy rights of all Australians.[128]

2.127 Bravehearts argued that data retention represents a particular opportunity to improve conviction rates in relation to child sex offenders:

> [W]e know that trying to find evidence to prosecute sex offenders is very difficult. This is why we have such a low conviction rate, because it is such a difficult crime to prosecute. And this is an opportunity where there is actually evidence; the police can get evidence. And we would hate to see that squandered, because it is critical in terms of child protection that this metadata is retained

127 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 10.

128 Uniting Church Justice and International Mission Unit, *Submission 76*, pp. 11–12.

> and that police have access to it in order that they can identify children who are at risk.[129]

2.128 Professor George Williams of the Gilbert + Tobin Centre of Public Law acknowledged the need for agencies to be able to intrude on individuals' privacy by accessing telecommunications data, but emphasised the need for appropriate safeguards to ensure that such access occurs only as part of a legitimate investigation.[130]

Can data retention meet the test as being effective for a legitimate aim?

2.129 As noted above, for a measure to be considered 'necessary' for a legitimate aim, it must be shown to have some chance of achieving that goal. That is, even where a measure is properly directed at a legitimate aim, it may not be regarded as 'necessary' if it produces second-order consequences that undermine its likely efficacy.

2.130 Mr Chris Berg, Senior Fellow at the Institute for Public Affairs argued that the existence of relatively easy-to-use counter-surveillance tools, such as Virtual Private Networks (VPNs), would undermine the value of data retention for law enforcement and national security purposes:

> The law enforcement value of data retention will be seriously eroded by the large scale VPN use. Any mildly sophisticated user is capable of setting up a VPN on their computer or mobile phone. Given that data retention is intended for 'serious crime' in the words of the prime minister, it is likely that any serious criminals will deploy VPNs or other data retention countermeasures to prevent law enforcement action. The Institute of Public Affairs has previously identified VPNs as a critical barrier to government internet policy in the domain of copyright infringement. Security and law enforcement agencies – like copyright holders – have to understand how technological adaptation will limit the efficacy of desired new powers.[131]

2.131 Communications Alliance, Mr Ben Johnston, and Mr Bernard Keane also highlighted this issue.[132]

---

129 Mrs Hetty Johnston AM, Chief Executive Officer, Bravehearts, *Committee Hansard*, Canberra, 30 January 2015, p. 1.

130 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 9.

131 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 12.

132 Communications Alliance (CA) and the Australian Mobile Telecommunications Association (AMTA), *Submission 6*, p. 16; Mr Ben Johnston, *Submission 36,* pp. 1–2; Mr Bernard Keane, *Submission 37*, pp. 5–6.

2.132 The Attorney-General's Department addressed this argument, to the extent possible in public testimony, in evidence to the Senate Legal and Constitutional Affairs References Committee:

> I am sure you will appreciate that in this forum I need to be careful about talking about the capabilities of the agencies, but it is fair to say that notwithstanding that there is a variety of means by which those people who are engaged in criminal and security relevant activities might seek to engage and subvert any lawful access to their data or their activities, it remains the case … that data present a critical and unique tool and key lead piece of information in progressing their investigations.[133]

2.133 A number of law enforcement and national security agencies gave evidence that telecommunications data is used most frequently in complex investigations where agencies would be expected to routinely encounter suspects practicing counter-surveillance techniques, indicating that it remains of considerable value in such circumstances. The AFP provided evidence that telecommunications data has been used in all recent cybercrime investigations, which inherently tend to involve highly technologically-sophisticated criminals, as well as virtually all counter-terrorism, child protection and organised crime investigations, where suspects tend to adopt significant more advanced tradecraft than the average criminal.[134]

2.134 Similarly, ASIO gave evidence that it uses telecommunications data in its counter-espionage and cyber-security investigations, and emphasised that:

> the 10 per cent or the two per cent outside, at the longest length of retention, is actually the most crucial information that you are looking for in terms of networks and … in terms of particularly espionage cases and cyber cases.[135]

2.135 The Uniting Church Justice and International Mission Unit strongly opposed the argument that the uptake of counter-surveillance tools undermines the case for a data retention regime, noting that 'the argument… would appear to be that because some offenders may adapt their behaviour… the capacity of law enforcement should be permitted to be eroded.'[136] The Unit provided a detailed rebuttal of the argument, focusing in particular on the case of child exploitation:

---

133 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 45.

134 Commissioner Andrew Colvin, *Committee Hansard*, Canberra, 17 December 2014, p. 3.

135 Ms Hartland, *Committee Hansard*, Canberra, 17 December 2014, p. 21.

136 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 8.

> The argument is deeply flawed. While any improvement in tools for law enforcement to combat online criminal activity is likely to see some offenders adapt and use more sophisticated tools to avoid detection and capture, experience of law enforcement agencies is that many offenders do not adapt their behaviour and are more likely to get caught. The fact that many offenders engaged in extreme forms of online criminal activity do not currently make use of all the online tools available to them that would assist them in avoiding detection and capture is evidence that not all offenders have the knowledge or simply do not behave in a way that maximizes their ability to get away with their online criminal behaviour.
>
> For example, offenders who access child sexual abuse material do not appear as sophisticated as is often assumed. The [United Nations Office on Drugs and Crime] commented only 6% of offenders in one sample used encryption technology. In another sample, 17% used password protection, 3% evidence eliminating software and only 2% used remote storage systems. They note more sophisticated consumers could have evaded detection. However, such statistics serve as a warning that simply because a counter-strategy is technologically available does not mean that all offenders will avail themselves of the strategy.[137]

2.136 The Unit also drew the Committee's attention to the assessment of the Virtual Global Taskforce, which is an international coalition of law enforcement from 11 countries, as well as INTERPOL and Europol, dedicated to protecting children from sexual exploitation:

> [A]wareness is not the same as execution. Very few offenders are 100% secure all of the time or in all respects. The collecting impulse and sexual drive of offenders often prevents them from being as secure as they would like.
>
> Equally, offenders cannot entirely control the behaviour of others. Participating in online forums, while necessary to access newer material, was deemed by some respondents to be something of a risk in itself, even in those environments in which administrators enforce security standards. In this respect, anonymity is never absolutely assured.[138]

2.137 Communications Alliance noted that counter-surveillance tools may not entirely defeat agencies attempting to identify communications as part of a

137 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 7.

138 Uniting Church Justice and International Mission Unit, *Submission 76*, p. 8.

lawful investigation,[139] and that the existence of such tools may in fact represent a further justification for data retention:

> Equally you could make the argument that because there are holes you should make the pieces you can cover as absolutely stringent as possible. That is not an argument we are advancing, but we think it is an issue worthy of considering in the overall picture.[140]

2.138 The European Commission's *Evaluation Report* also noted that, despite concerns expressed by civil society groups that the introduction of data retention could lead to people to change their communications behaviour, 'there is no corroboratory evidence for any change in behaviour having taken place in any Member State concerned or in the EU generally'.[141]

Can data retention meet the test as being proportionate for a legitimate aim?

2.139 The Committee received a number of submissions arguing that mandatory telecommunications data retention would constitute a disproportionate interference with the rights to privacy and freedom of expression. As noted above, the Statement of Compatibility with Human Rights confirms that the retention of telecommunications data constitutes an interference with the rights to privacy and freedom of expression. [142]

2.140 Dr Lesley Lynch, Secretary of the New South Wales Council for Civil Liberties, emphasised the value of privacy to individuals and society:

> [P]rivacy, like security, does matter; it is not a trivial consideration in the balancing equation. Serious intrusions into privacy have real consequences for persons and for societies, and that is what we are grappling with balancing in this context.[143]

2.141 Mr Chris Berg of the Institute of Public Affairs provided a more detailed explanation of the individual value of privacy:

> [W]e all require privacy to function and thrive. Let's start with the mundane. Obviously we desire to keep personal details safe – credit card details, internet passwords - to protect ourselves against identity theft. On top of this, we seek to protect ourselves against the judgment or observation of others. We close the door

139 Mr Stanton, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

140 Mr Stanton, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

141 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, p. 26.

142 Data Retention Bill, *Explanatory Memorandum*, p. 14.

143 Dr Lesley Lynch, Secretary, New South Wales Council for Civil Liberties, *Committee Hansard*, Canberra, 30 January 2015, p. 79.

> to the bathroom. We act differently with intimates than we do with colleagues. We often protect our thoughts, the details of our relationships, our preferences, from prevailing social norms. We compartmentalise. How many people would be uncomfortable with a colleague flipping through their mobile phone – with the window into a life that such access would provide?[144]

2.142 Mr Berg also explained the value of a broad construction of freedom of speech, and the relationship between privacy and freedom of expression, insofar as 'the threat or actuality of government surveillance may psychologically inhibit freedom of speech',[145] arguing that:

> The potential of surveillance – and there is no doubt that the data retention bill threatens to inculcate a culture of being under surveillance, given its possible breadth and future expansion – to limit freedom of speech is significant. Once the government has introduced this legal regime it is, barring future judicial oversight, unlikely to be repealed, and almost certain to be extended. The so-called 'balance between liberty and security' is only ever moved in favour of security.[146]

2.143 The Victorian Commissioner for Privacy and Data Protection argued that 'the wide scale collection of metadata is an unjustified infringement on human rights',[147] and that retained data would:

> reveal patterns of communications that will enable those who have access to it to investigate and understand the private lives of all Australians, such as the habits of everyday life, places of residence, minute by minute movements, activities undertaken, social, professional and commercial arrangements, and relationships and social environments frequented.[148]

2.144 Mr Jon Lawrence, of Electronic Frontiers Australia and the Australian Privacy Foundation, made similar arguments.[149]

2.145 Mr Lawrence also drew the Committee's attention to the conclusion of the Court of Justice of the European Union, in its decision in *Digital Rights Ireland*, that, where telecommunications data is required to be retained:

---

144 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 8.

145 Quoting G.L. White and P.G. Zimbardo, *The chilling effects of surveillance: Deindividuation and reactance*, Office of Naval Research, 1975.

146 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 10.

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

148 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 8.

149 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, Canberra, 29 January 2015, p. 21; Australian Privacy Foundation, *Submission 75*, p. 1.

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary place of residence, daily or other movements, the activities carried out, the social relationships of those persons, and the social environments.[150]

2.146 Dr David Lindsay, Vice Chair of the Australian Privacy Foundation, argued that the Bill is disproportionate, and a 'sledgehammer that unjustifiably breaches the right to privacy who are overwhelmingly neither criminals nor terrorists'. Dr Lindsay cited a report of the Office of the UN High Commissioner for Human Rights, which states that:

> Concerns about whether access to and use of data are tailored to specific legitimate aims… raise questions about the increasing reliance of Governments on privacy sector actors to retain data 'just in case' it is needed for government purposes. Mandatory third-party data retention – a recurring features of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location… - appears neither necessary nor proportionate.[151]

2.147 The Committee noted that the following paragraph of the Office's report went on to list 'factors that must be taken into account in determining proportionality' in relation to 'bulk data' programs, such as data retention.[152] Similarly, the preceding paragraph, which discussed the mass collection of communications or telecommunications data by government agencies (as opposed to third-party data retention) states that:

> Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed.[153]

---

150 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [27].

151 Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), [27], quoted by Dr David Lindsay, Vice-Chair, Australian Privacy Foundation, *Committee Hansard*, 30 January 2015, p. 77; the Law Institute of Victoria also referred the Committee to this paragraph of the report in *Submission 117*, p. 14.

152 Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), [28].

153 Office of the United Nations High Commissioner for Human Rights, *Right to Privacy in the Digital Age*, A/HRC/27/37 (30 June 2014), [26].

2.148 Emeritus Professor Gillian Triggs, President of the Australian Human Rights Commission, drew a distinction between the magnitude of the privacy intrusion associated with *access* to telecommunications data by law enforcement and national security agencies, which she characterised as 'powerful',[154] compared to the mandatory *collection* and *retention* of telecommunications data by a third-party service provider, which she characterised as 'small'.[155]

2.149 Mr Peter Leonard, from the Law Council of Australia, supported this distinction:

> The fact that data is retained about me is not, of itself, pervasive surveillance, but it does enter into the balance between those three rights—that if there is a risk that data may be used to undermine the other rights that I should enjoy, then that should be assessed in determining the proportionality of the data retention. So I think it is necessary to look, firstly, at the data retention, and balance its effect on other rights before we got to the question of proportionality as to how the data is used.[156]

2.150 Mr Leonard went on to argue that whether telecommunications data should be retained and, if so, how much and for how long, are less significant issues than questions about the types of safeguards that should apply to protect that data from being improperly accessed or misused.[157]

2.151 The Statement of Compatibility with Human Rights, which accompanies the Bill, notes that the proportionality of data retention cannot be considered in isolation from the purposes for which retained data can be lawfully used, and the safeguards that exist around the access to and use of such data:

> The Bill permissibly limits an individual's privacy in correspondence (telecommunications) in a way which is reasonable and proportionate by circumscribing the types of telecommunications data that are to be retained by service providers to the essential categories of data required to advance criminal and security investigations, permitting access to telecommunications data only in circumstances prescribed by existing provisions in the TIA Act and moreover reducing the range of agencies who may access data under those provisions.[158]

154 Professor Triggs, *Committee Hansard*, Canberra, 29 January 2015, p. 76.

155 Professor Triggs, *Committee Hansard*, Canberra, 29 January 2015, p. 78.

156 Mr Leonard, *Committee Hansard*, Canberra, 30 January 2015, p. 34.

157 Mr Leonard, *Committee Hansard*, Canberra, 30 January 2015, p. 35.

158 Data Retention Bill, *Explanatory Memorandum*, p. 11.

2.152 The Privacy Impact Assessment for the Bill notes that 'the kind of information that may be prescribed does not go beyond that which service providers are already generating to provide services, albeit that some service providers may not be recording the information or keeping it for very long',[159] and ultimately concludes that:

> we have concluded that the proposed changes set out in the draft Amendment Bill do not appear to have significant privacy implications.[160]

2.153 Dr Roger Clarke, Immediate Past Chair of the Australian Privacy Foundation, disagreed with Professor Triggs' and Dr Leonard's assessment that data retention, of itself, involves a small intrusion on privacy and is not pervasive surveillance:

> [T]his is mass surveillance that is to be imposed by the parliament on the Australian people. We have skirted around that and never used the word. There has been mention of personal surveillance—the collection of data about individuals who come to attention and about whom there is reasonable suspicion et cetera. That has been mentioned in passing. But this moves way, way beyond that, to mass surveillance.[161]

2.154 Professor Williams, while supporting data retention, emphasised that the fact that data retention will potentially apply to all Australians' communications is an important distinguishing factor from other law enforcement and national security measures, and emphasised the need for appropriate safeguards.[162]

2.155 In its submission, ASIO argued that the view that telecommunications data is, or will be, used for 'mass surveillance' is a misconception. In particular, ASIO advised the Committee that:

- ASIO does not engage in 'large-scale mass gathering of communications data', and that it 'does not have the resources, the need, or the inclination' to do so, and

---

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

160 Australian Government Solicitor, *Privacy Impact Assessment: Proposed amendments to the Telecommunications (Interception and Access) Act 1979*, 15 December 2014, p. 25 (appended to Attorney-General's Department, *Submission 27*).

161 Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 30 January 2015, p. 78; see also, Dr Clarke, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, 2 February 2015, p. 20.

162 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 9.

- at most, a few thousand people come to ASIO's attention each year as part of security investigations, inquiries and leads that may require access to telecommunications data.[163]

2.156 In her submission, the Inspector-General of Intelligence and Security (IGIS) advised that the Attorney-General's Guidelines for ASIO require, among other things, that:

- any means used by ASIO for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence, and
- inquiries and investigations into individuals and groups must be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions.[164]

2.157 As noted earlier, the Director-General of Security explained to the Committee how the legal restrictions contained in the Guidelines are applied in practice:

> It is not and will not be the case that ASIO automatically requests the maximum amount of data available. Should this bill become law, ASIO will continue to request access to historical communication data needed only for the purpose of carrying out our function, regardless of the length of time that data may be available for. We abide by the law.[165]

2.158 The IGIS confirmed that her Office inspects ASIO's access to and use of both historic and prospective telecommunications data, that there is a high rate of compliance in this area, and that she had not identified any concerns with ASIO's access to such information.[166]

2.159 Professor Triggs challenged the view that telecommunications data is less privacy sensitive than the content of communications, noting that:

> A great deal can be learned from metadata. Indeed, in many cases, more can be learned from metadata than can be learned from content, especially as many people are extremely cautious about content but forget that it is the metadata that can actually lead law enforcement agencies to a paedophile ring, to a terrorist group or to serious criminals.[167]

163 ASIO, *Submission 12.1*, p. 10.

164 IGIS, *Submission 131*, p. 6.

165 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 65.

166 IGIS, *Submission 131*, p. 5.

167 Professor Triggs, *Committee Hansard*, Canberra, 29 January 2015, p. 71.

2.160 However, the Explanatory Memorandum argues that telecommunications data is less privacy sensitive than the content of communications.[168] The Bill's Statement of Compatibility with Human Rights also identifies that the degree of this interference differs in relation to various elements of the proposed data set. For example, the Statement identifies that

> subscriber data, as the predominant data category which would be generated through the collection of customer information, raises relatively fewer privacy implications than traffic and location data comparators.[169]

2.161 The Attorney-General's Department, in its supplementary submission, drew the Committee's attention to the conclusion of the Court of Justice of the European Union that:

> even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.[170]

2.162 Professor Williams noted that, 'I do think there are different degrees of information… I think there is a clear distinction between the stored communications as to content and metadata.'

2.163 However, Professor Williams also observed that:

> I think the community is sending a pretty strong signal to your committee that they do see this information as sensitive. You only need to look at the public debate and the public reaction about this to see that the community does not see this as ordinary information but is actually very concerned as to the circumstances in which government agencies would access it.[171]

2.164 A number of submissions and witnesses argued that the Government should consider less privacy-intrusive alternatives to data retention.[172]

2.165 Mr Vaile and Mr Remati drew the Committee's attention to a recent report of the US National Research Council, entitled *Bulk Collection of Signals*

---

168 Data Retention Bill, *Explanatory Memorandum*, p. 3.

169 Data Retention Bill, *Explanatory Memorandum*, p. 14.

170 Attorney-General's Department, *Submission 27.2*, p. 9, referring to *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [39].

171 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 8.

172 See, for example: Privacy International, *Submission 80*, p. 11; Mr Lawrence, *Committee Hansard*, Canberra, 29 January 2015, p. 22.

Intelligence: Technical Options.[173] The report, released on 15 January 2015, evaluated whether viable alternatives existed to the bulk collection of signals intelligence by US intelligence agencies, and concludes that:

> there are no technical alternatives that can accomplish the same functions as bulk collection and serve as a complete substitute for it; there is no technological magic.[174]

2.166 Some submitters argued that viable alternatives existed to a mandatory data retention regime, such as the use of the existing preservation notice regime under Part 3-1A of the TIA Act. The Australian Privacy Foundation argued that:

> [I]n proposing a mandatory blanket data retention regime, the government has given insufficient consideration to the potential benefits of a targeted data preservation regime, in which relevant agencies may selectively require the preservation of telecommunications data, provided always that satisfactory procedural safeguards are met … In any case, no consideration appears to have been given to the merits of adapting and extending a regime such as the Chapter 3 preservation notice regime, to appropriately apply to the preservation of non-content telecommunications data.[175]

2.167 Similarly, Mr Keane argued that agencies could currently use these notices to preserve telecommunications data as an alternative to data retention:

> The 'going dark' argument is further undermined by the fact that ASIO simply doesn't use existing tools designed explicitly to enable data retention.
>
> For two years, ASIO, the AFP and state police forces have had the power, under the *Cybercrime Legislation Amendment Act 2012*, to require communications companies to store information that may help in the investigation of a 'serious contravention' — an offence punishable by three years or more in jail — for up to 90 days before getting a warrant to access the data. The only limitation on the requests apart from the seriousness of the offence is that it

173 Mr Vaile and Mr Remati, *Submission 194*, p. 8.

174 United States National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, pp. 4–5; The Committee notes that the report primarily concerns foreign intelligence collection by US Government agencies, as quite distinct from the Government's proposal to require Australian telecommunications companies to keep records at arms-length from Australian agencies. Nevertheless, much of the Council's core analysis around the utility of retaining information and possible alternative approaches is relevant to this Committee's consideration of the Bill.

175 Australian Privacy Foundation, *Submission 75*, p. 30.

> must be targeted at one person, but an agency can issue as many preservation notices as necessary.[176]

2.168 Mr Berg raised the question of whether any inadequacies within the preservation notice regime could be rectified, as an alternative to implementing data retention.[177]

2.169 This Committee previously received evidence from the Attorney-General's Department about whether preservation notices are a viable alternative to data retention as part of its *Inquiry into potential reforms of Australia's national security legislation*:

> Data preservation involves a [carrier or carriage service provider (C/CSP)] preserving specific telecommunications data identified by an agency that it has available on its network in relation to a relevant investigation or intelligence gathering activity on notification by an agency. Given the current authority under the TIA Act for agencies to access telecommunications data from a C/CSP when it has been identified as being relevant to a specific investigation or intelligence gathering activity, agencies already have the ability to access telecommunications data that the C/CSP has on hand at the time of the request or that comes into existence into the future, negating the need for data preservation.[178]

2.170 The Department's submission to this inquiry contained further discussion on this issue.[179] In particular, the Department explained that such notices, which are currently issued under Part 3-1A of the TIA Act ('Preserving stored communications') apply only to 'stored communications', such as emails and SMS messages, and the associated telecommunications data.[180] This is consistent with the Department's previous evidence to the Joint Select Committee on Cyber-Safety that preservation notices apply only to 'stored computer data', as defined in the *Convention on Cybercrime* and which equates to 'stored communications' under the TIA Act.[181]

---

176 Mr Bernard Keane, *Submission 37*, p. 7.

177 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. 13.

178 Attorney-General's Department, *Submission 218 to the Inquiry into potential reforms of Australia's national security legislation*, p. 8, quoted at p. 163 of the *Report of the inquiry into potential reforms of Australia's national security legislation*.

179 Attorney-General's Department, *Submission 27*, pp. 17–18.

180 TIA Act, section 107J.

181 See: Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Joint Select Committee on Cyber-Safety, 1 August 2011, p. 31; Mr David Cramsie, Senior Legal Officer, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Committee Hansard*, Joint Select Committee on Cyber-Safety, 1 August 2011, p. 32.

2.171 The Department acknowledged that the preservation notice regime could be amended or expanded, as suggested by Mr Berg, but argued that while preservation notices could complement data retention, they would not be a substitute for it:

> The purpose of preservation notices is to 'quick freeze' volatile or perishable electronic evidence that a provider possesses for a short period of time, to allow agencies time to apply for and obtain a warrant to access that information. Evidence cannot be preserved if it was never retained, or if it has already been deleted.
>
> …
>
> As such, data retention is in fact a prerequisite to preservation of data, rather than preservation offering an alternative to retention.[182]

2.172 The Director-General of Security provided the Committee with his views about the circumstances in which preservation notices are, and are not, of use to ASIO:

> It is something we use and it is absolutely the case that if we were aware that something was likely to happen that you can in fact put in place a preservation order around that particular set of circumstances to understand it better going forward. But all of that of course is prospective. Your earlier question… is a retrospective issue and retrospectivity is a different set of issues here.[183]

2.173 The Australian Commission for Law Enforcement Integrity (ACLEI) drew the Committee's attention to the fact that preservation notices are of limited value, in particular, as part of anti-corruption investigations:

> ACLEI notes that data retention alternatives, such as preservation notices, are currently available under the TIA Act. However, ACLEI's experience is that these alternatives are most relevant when it is desirable to ensure preservation of future information, such as when a person is under investigation and is likely to commit further crimes. Preservation of past data is entirely limited to the carrier's business practices.
>
> The nature of corruption – particularly in a law enforcement context where officers are more aware of surveillance limitations and able to defeat them – means that relevant conduct is covert and may not come to light for some months or years after the event. It follows that preservation notices cannot assist an

182 Attorney-General's Department, *Submission 27*, p. 17.

183 Mr Lewis, *Committee Hansard*, Canberra, 30 January 2015, p. 69.

> investigation if the data sought has already been deleted by the carrier.[184]

2.174 The AFP also argued that, without data retention, agencies would frequently lack the necessary information to identify a suspect and serve a preservation notice, rendering the preservation notice power 'ineffective' in many situations:

> In many instances, the role that data place in the early stages of investigations is to assist in attribution: that is, data is a crucial tool in identifying the suspect in a criminal act or event, and in clearing other persons from suspected involvement. Where this data is unavailable because it has not been retained, investigations have been unable to progress.[185]

2.175 The US National Research Council's report considered the comparative value of retained data compared to targeted collection or preservation:

> If past events become interesting in the present for understanding new events… historical facts and the context they provide will be available for analysis only if they were previously collected.
>
> …
>
> Targeted collection provides data only on present and future actions of parties of interest at the time of collection, but not their past activities.[186]

2.176 In its submission, the Department drew the Committee's attention to a number of international evaluations of whether preservation notices are a viable substitute for data retention, including the Council of Europe's *Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*,[187] the European Commission's *Evidence of the Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*,[188] and the Netherlands Government's *The Dutch implementation of the Data Retention Directive*.[189] Each of these reports concluded that preservation notices are not a substitute for accessing existing telecommunications data.

184 Australian Commission for Law Enforcement Integrity, *Submission 48*, p. 8.

185 AFP, *Submission 7.1*, p. 13.

186 United States National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, p. 4-1.

187 Council of Europe, *Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime*, 2012, pp. 75-76.

188 European Commission, *Evidence of the Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries,* 2012, pp. 22-23.

189 Netherlands Government, *The Dutch implementation of the Data Retention Directive,* 2014, pp. 110–111.

2.177 As noted above, Mr Leonard of the Law Council argued that the available evidence shows that existing arrangements for the retention of telecommunications data by service providers are adequate for the purposes of national security and law enforcement investigations.[190]

2.178 Similarly, the Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG) argued that:

> law enforcement are not fully utilising the data that is currently available to them, particularly metadata that is publicly available. The DPG members expect that law enforcement should make full use of such information before embarking on a fishing expedition by requiring businesses to retain data for a defined period of time.[191]

2.179 The substance of this issue is largely addressed in the preceding discussion about the necessity of data retention. However, the Attorney-General's Department, in evidence to the Senate Legal and Constitutional Affairs References Committee, observed that:

> [A] number of commentators I think have referred to the existing practices of industry in retaining telecommunications data and that that provides an avenue to avail agencies of the data that they need to conduct investigations. In that regard, the key thing that we would note is that telecommunications industry practices are changing and that they are changing at a rapid rate. A number of providers have indicated in evidence before committees, most recently the PJCIS, the fact that they have significant gaps in their holdings of data, particularly in relation to more modern telecommunications services as opposed to traditional telephony services. And of course the range of service s is constantly changing and their business practices are being driven by the profitability of their particular companies. They are driven by commercial needs rather than the needs of law enforcement and security agencies. So the alignment between what has historically been a coincidence between the business practices of the telecommunications industry and the needs of law enforcement and security agencies is moving apart and that is why there is in part the need to address the retention of telecommunications data.[192]

190 Mr Leonard, *Committee Hansard*, Canberra, 30 January 2015, p. 31.

191 AIMIA Digital Policy Group, *Submission 34,* p. 5.

192 Ms Harmer, *Committee Hansard*, Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, pp. 44–45.

2.180 In evaluating the proportionality of a data retention regime for national security and law enforcement purposes, the Committee received a range of evidence on comparable international regimes. As the Committee has noted above, Australia's human rights obligations at international law derive from, among other instruments, the International Covenant on Civil and Political Rights. Nevertheless, the reasoning of the Court of Justice of the European Union, in its decision in *Digital Rights Ireland*, provides useful guidance for evaluating the proportionality of a proposed data retention scheme:

> [A]ny limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. [193]

2.181 The Court went on to conclude that the form of data retention established by the Data Retention Directive (upon which the Bill is based):

- was provided for by law,
- respected the essence of the right to privacy, as it did not 'permit the acquisition of knowledge of the content of electronic communications', [194]
- respected the essence of the right to the protection of personal data, as Member States were required under separate EU Directives to 'ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alternation of the data', [195] and
- 'genuinely satisfie[d] an objective of general interest', namely being to contribute to public security through the fight against international terrorism, the maintenance of international peace and security, the fight against crime and, in particular, organised crime, and the promotion of the right of any person to security. [196]

---

193 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [38].

194 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [39].

195 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [40].

196 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [41]–[44].

2.182 As summarised in the Australian Human Rights Commission's submission, the Court's decision to strike down the Directive was, therefore, based on 'several characteristics of the Data Retention Directive that rendered the regime disproportionate'.[197]

2.183 The Attorney-General's Department summarised the key issues identified by the Court, being that the Directive:

- 'cover[ed], in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception',
- 'fail[ed] to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions' (such matters were left to each member-State of the EU to determine),
- 'require[ed] that those data be retained for a period of at least six months, without any distinction being made between the categories of data … on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned',
- '[did] not provide for sufficient safeguards… to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data', and
- '[did] not require the data in question to be retained within the European Union'.[198]

2.184 The effect of this decision, in the Australian Human Rights Commission's view, was to 'define the limits of permissible data retention pursuant to human rights law',[199] rather than to prohibit data retention outright. The Committee noted that similar conclusions have been reached by the German Constitutional Court and the Czech Republic's Constitutional Court, striking down domestic laws on particular grounds while confirming that data retention may, in principle, be a necessary and proportionate response.[200] Similarly, courts in Cyprus and Bulgaria have

197 Australian Human Rights Commission, *Submission 42*, p. 5.

198 Attorney-General's Department, *Submission 27*, p. 39.

199 Australian Human Rights Commission, *Submission 42*, p. 5.

200 Judgement of the Bundesverfassungsgericht, 1 BvR 256/08, of 2 March 2010; Official Gazette of 1 April 2011, Judgment of the Constitutional Court of 22 March on the provisions of section 97 paragraph 3 and 4 of Act No. 127/2005 Coll. on electronic communications and amending certain related acts as amended, and Decree No 485/2005 Coll. on the data retention and transmission to competent authorities.

annulled individual elements of their national laws, without affecting the validity of data retention as a whole in those countries.[201]

2.185 The Romanian Constitutional Court held data retention to be unconstitutional in 2009.[202] Additionally, as the Department notes in its submission:

> The invalidation of the Directive has resulted in the annulment of a number of data retention laws in member States where the Directive was implemented, in particular in jurisdictions that had effectively transposed the Directive without incorporating additional, national safeguards.[203]

2.186 The outcomes of these international decisions indicates that the assessment of the proportionality of a mandatory data retention scheme must take into account the existence and extent of safeguards to protect against unlawful or improper access to or use of retained information.

Privacy concerns relating to legal professional privilege and obligations of professional confidence

2.187 The Committee received evidence from a number of submitters and witnesses identifying particular privacy concerns regarding access to telecommunications data about communications that may be subject to legal professional privilege or to obligations of professional confidence, such as a journalist's obligation to protect the confidentiality of their sources.[204]

2.188 The Parliamentary Joint Committee on Human Rights has requested the advice of the Attorney-General as to whether access to telecommunications data under the TIA Act may impact on legal professional privilege and, if so, how this is proportionate with the right to privacy.[205]

2.189 The Attorney-General's Department noted that existing safeguards under the *Public Interest Disclosures Act 2013* immunise Commonwealth officials

---

201 Supreme Court of the Republic of Cyprus, Decision in civil applications 65/2009, 78/2009, 82/2009 and 15/2010-22/2010, 1 February 2011; Supreme Administrative Court of Bulgaria, No. 13627, 11 December 2008.

202 Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court, Romanian Official Monitor No 789, 23 November 2009.

203 Attorney-General's Department, *Submission 27*, p. 39.

204 See, for example, Law Council of Australia, *Submission 126*, p. 22; Media, Entertainment and Arts Alliance, *Submission 90*, p. 4.

205 Parliamentary Joint Committee on Human Rights, *Fifteenth Report to the 44th Parliament*, p. 17.

from any form of criminal, civil or administrative liability for making a legitimate public interest disclosure, and that:

> As such, data access powers will generally not be available to law enforcement agencies in relation to genuine whistleblowers by reason of those disclosures.[206]

2.190 The Department's submission further argued that, where particular conduct has been determined to be criminal in nature, agencies should have access to appropriate tools to investigate that conduct :

> Disclosures of data are available to support the enforcement of the criminal law, administration of pecuniary penalties and the protection of the public revenue. It is not appropriate to afford a special status to particular types of communications as powers of this type should, by their nature, be applied generally.[207]

2.191 The Law Council of Australia acknowledged that there are circumstances in which access to telecommunications data about a lawyer's communications will be justifiable, including where the communications are in furtherance of the commission of a crime.[208] Similar reasoning would apply to communications within other relationships that are subject to obligations of confidence.

2.192 In evidence, the Media, Entertainment & Arts Alliance argued that the Bill should not be passed, but that if it were passed it would be preferable that law enforcement and national security agencies should be precluded from accessing telecommunications data to investigate criminal offences involving the unlawful disclosure of information covered by the official secrecy provisions of the *Crimes Act 1914*:[209]

> The real concern of all this is that the use and the keeping of metadata makes the ability to identify confidential sources and the communication between a confidential source and a journalist transparent to the authorities. We have seen over the past 10 or 15 years an increasing amount of referral to particularly the Australian Federal Police for investigation of breaches under the Crimes Act.
>
> …
>
> There is no doubt under the current legislation, because of the failure of repeated governments to decriminalise the leaking of

206 Attorney-General's Department, *Submission 27*, p. 22.

207 Attorney-General's Department, *Submission 27*, p. 21.

208 Law Council of Australia, *Submission 126*, p. 22.

209 Mr Christopher Warren, Federal Secretary, Media, Entertainment & Arts Alliance, *Committee Hansard*, Canberra, 30 January 2015, p. 38.

> information, that a whistleblower or a confidential source of whatever nature is committing a crime—when they are a government employee—when they release information to a journalist.
>
> …
>
> The problem of having a criminalised approach like that is it acts as a very serious chilling effect. The main impact of this legislation is to have a chilling effect on any potential whistleblower or confidential source releasing information they would not want to release.

2.193 The Committee recognises the heightened public interest in ensuring the confidentiality of certain privileged or confidential communications, as well as in promoting public confidence in the confidentiality of those communications. This issue is considered in greater detail later in the report (see Chapter 6).

The security of retained telecommunications data

2.194 Whether or not telecommunications data retained under a mandatory data retention scheme can be effectively secured is critical to assessing whether such a scheme is a proportionate for national security and law enforcement purposes.

2.195 The Committee received a range of evidence that retained telecommunications data would be vulnerable to unauthorised access.[210] The risk of unauthorised access to or modification of telecommunications data retained by carriers is closely related to privacy and civil liberties concerns. The Australian Privacy Commissioner observed that data retention:

> creates a risk that the data may be misused, such as through inappropriate access or the risk of identity theft and fraud as a result of data breaches.[211]

2.196 Mr Tom Courtney submitted that ISPs would implement inadequate security controls to reduce costs:

---

210 See, for example: Ms Clark, Australian Communications Consumer Action Network, *Committee Hansard*, 29 January 2015, p. 81; Mr Lawrence, Electronic Frontiers Australia, *Committee Hansard*, Canberra, 29 January 2015, p. 21.

211 Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard*, Canberra, 29 January 2015, p. 46.

> As storing the data will have to be implemented by the ISP's it will not necessarily have the appropriate security controls. It is 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.[212]

2.197 Mr Courtney's concerns echo public comments previously made by the then Chief Regulatory Officer of iiNet that 'we'll be looking for the cheapest, lowest-cost option. That means cloud storage and the lowest-cost cloud storage in the world today is in China'.[213]

2.198 Telstra's Chief Information Security Officer explained to the Committee how implementing a data retention scheme may increase, but not fundamentally alter the nature of the information security risks currently faced by service providers:

> We do secure the data we have today. So we do have that problem today. The issue here is that now we are advertising that for a customer of Telstra there is a whole range of data, depending on what services they have, that for two years we can make available upon lawful request. If I were that way inclined as a hacker, you would go for that system, because it would give you the pot of gold as opposed to working your way through our multitude of systems today to try to extract some data. But your fundamental point is that, yes, we face this risk today—absolutely.[214]

2.199 Optus provided an alternative view on how the centralised storage of data may alter the level of information security risk:

> [H]aving a relatively limited, well-defined dataset as opposed to our entire internal commercial dataset … just makes that task a lot easier. Mr Burgess from Telstra did say that yes, there will be a—I think the word he used was 'honeypot'. Clearly just the existence of a database will attract people's interest. But 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 possible encrypt it, if need be. It is a sensible thing to have things like electronic sand traps—

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

213 Mr Steve Dalby, Chief Regulatory Officer, iiNet Ltd, quoted in 'New laws to stop web storage hackers', *Sydney Morning Herald*, 31 October 2014, <http://www.smh.com.au/federal-politics/political-news/new-laws-to-stop-web-storage-hackers-20141031-11f3qz.html> viewed 26 February 2015.

214 Mr Mike Burgess, Chief Information Security Officer, Telstra, *Committee Hansard*, Canberra, p. 9.

> all of the access protocols that we apply to the most sensitive information already.[215]

2.200 Optus further observed that, because information retained in accordance with data retention obligations may only need to be accessed by a provider's law enforcement liaison unit, providers may actually have options to secure such information to a greater extent than is possible for most telecommunications data currently held by industry:

> One of the options that may be considered is putting all of this data onto its own system, its own separate database, so that the only people who can access that system are the law enforcement liaison unit staff and it is not available for other people in the business and so, therefore, it is not linked out into the wide world where people can attack it from. That is one of the options that providers could give very serious consideration to.[216]

2.201 The telecommunications industry is currently subject to a range of information security obligations. Most service providers, with the exception of those with an annual turnover of less than $3 million, are required to comply with the information security provisions of the *Privacy Act 1988*. The Attorney-General's Department noted that these obligations require service providers to 'adopt a risk-based approach to protecting personal information in their possession from misuse, interference or loss, as well as from unauthorised access, modification or disclosure'.[217]

2.202 The Department also drew the Committee's attention to the guidelines issued by the Australian Information Commissioner, which explain that entities must consider a range of factors when determining how to protect information they hold, including the amount and sensitivity of the personal information, and the possible adverse consequences for an individual. In particular, the guidelines state that '[m]ore rigorous steps may be required as the quantity of personal information increases'.[218]

2.203 Communications Alliance also confirmed that service providers are currently required to comply with the Australian Government Protective Security Policy Framework (PSPF), which sets out mandatory requirements for physical, personnel and information security, and the Information Security Manual (ISM), which is developed by the Australian

---

215 Mr Epstein, *Committee Hansard*, Canberra, 30 January 2015, p. 22.

216 Mr Michael Elsegood, Member of Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, p. 40.

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

218 Australian Information Commissioner, *Australian Privacy Principles guidelines* (2014), [11.7].

Signals Directorate and sets out executive guidance, principles and technical security controls to mitigate risks to information and systems.[219]

2.204 The Committee notes that it is not common for private sector organisations to be required to comply with the PSPF and ISM.

2.205 The Government has also undertaken to implement further, industry-wide telecommunications sector security reforms (TSSR), recommended by this Committee in May 2013, before data retention is fully implemented.[220] In its submission, the Department explained that:

> TSSR is designed to ensure the security and integrity of Australia's telecommunication infrastructure by encouraging ongoing awareness and responsibility for network security by the telecommunications industry, and will extend to provide better protection of information held by industry in accordance with data retention obligations.
>
> TSSR will impose an obligation on service providers to do their best to prevent unauthorised access and unauthorised interference to telecommunications networks and facilities, including where the provider outsources functions.[221]

2.206 The Bill does not introduce new information security obligations for retained telecommunications data. However, the Department argued:

> it is preferable to implement a holistic security framework for the telecommunications sector, rather than imposing specific, stand-alone and potentially duplicative security obligations that apply only to a relatively narrow subsection of the information held by industry.[222]

2.207 Mr Peter Froelich, appearing as an industry member of the Communications Alliance, stressed that, beyond their legal obligations, providers have commercial and ethical incentives, as well as a range of tools, to secure customer information:

> [A]s 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,

219 Mr Stanton, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

220 The Hon Malcolm Turnbull MP, Minister for Communications, *House of Representatives Hansard*, 30 October 2014, p. 12562; Ms Jones, Attorney-General's Department, *Committee Hansard*, Canberra, 17 December 2014, p. 2.

221 Attorney-General's Department, *Submission 27*, p. 38.

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

> 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.[223]

Committee comment

2.208 The Committee received a great deal of evidence on the question of whether mandatory data retention is a necessary and proportionate measure for national security and law enforcement purposes. Much of this evidence was received in public. The Committee has also received classified and commercially confidential evidence. The Committee has carefully weighed the totality of the evidence before it when considering this issue.

2.209 The value of telecommunications data to national security and law enforcement investigations is indisputable. Its value is rising as criminals and persons engaged in activities prejudicial to security increasingly rely on communications technology to plan, facilitate and carry out their activities, while the ability of agencies to lawfully intercept the content of those communications declines.

2.210 Several submissions and witnesses argued that this Bill is not urgent, due to the long-term nature of the challenges facing agencies and the fact that, should this Bill be passed, it would take up to two years following Royal Assent for data retention to be fully implemented.[224] This is an argument which the Committee has carefully considered.

2.211 Nearly two years ago, the previous Committee concluded that the ability of national security and law enforcement agencies to safeguard national security and public safety, and to combat serious crime, had already been degraded as a result of service providers keeping fewer records about the services they provide. This degradation has continued.

2.212 This Committee has been briefed on numerous, major investigations into serious criminal activity that have failed as a result of these changes. For example, the AFP have been unable to identify nearly half of all suspects in a current child exploitation investigation, because a number of Australian service providers do not retain basic IP address allocation

223 Mr Peter Froelich, Industry Member, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, pp. 39–40.

224 See, for example, Mr Lawrence, *Committee Hansard*, Canberra, 29 January 2015, p. 25.

records—which are akin to a person's phone number—for any length of time.[225] In South Australia, service providers not retaining telecommunications data for mobile phones has stalled murder investigations.[226] In New South Wales, more than 80 per cent of requests for internet-related data for police investigations have been unsuccessful.[227] In Queensland, the unavailability of critical telecommunications data prevented police from identifying an offender in a child exploitation investigation; that offender continued to sexually abuse a young girl for more than four years until his identity was discovered as part of a separate investigation.[228]

2.213 The Committee has also received detailed, classified evidence on the impact that the inconsistent retention of telecommunications data has had on national security investigations, including counter-terrorism, counter-espionage and cyber-security investigations. This long-term decline in the availability of telecommunications data has undermined ASIO's ability to detect and prevent threats to national security and public safety. ASIO has confirmed that these changes in commercial retention practices have prevented it from replicating previous, specific successes in safeguarding national security.[229]

2.214 Accordingly, the Committee accepts that introducing a mandatory data retention regime is necessary to support our national security and law enforcement agencies' capabilities.

2.215 In the Committee's view, the appropriate balance is to implement a data retention scheme that is strictly limited to what is necessary and proportionate, while ensuring that appropriate limits, safeguards and oversight mechanisms are in place to address privacy and civil liberties concerns. In examining the Bill, the committee has given careful consideration to the appropriate safeguards and oversight mechanisms that can be implemented to ensure the integrity of a data retention regime, and to protect and promote fundamental human rights and civil liberties, as the Australian public expects.

225 AFP, *Submission No. 76*, p. 11.

226 South Australia Police, *Submission No. 9*, p. 3; Assistant Commissioner Dickson, *Committee Hansard*, Canberra, 30 January 2015, p. 48.

227 Assistant Commissioner Lanyon, *Committee Hansard*, Canberra, 30 January 2015, p. 43.

228 Bravehearts, *Submission No. 33*, pp. 5-6.

229 ASIO, *Submission 12.1*, p. 30.

3

The data set

Introduction

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

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

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

(Chapter 3)

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

(Chapter 4)

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

(Chapter 5)

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

Should the data set be contained in primary legislation?

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

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

3.5 The Explanatory Memorandum states:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Committee comment

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

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

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

Recommendation 2

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

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

Recommendation 3

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

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

The data set as proposed and Industry Working Group recommendations

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

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

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

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

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

26 Paragraph 187A(4)(a).

27 Paragraph 187A(4)(b).

28 Paragraph 187A(4)(c).

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

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

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

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

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

---

29 Paragraph 187A(4)(d).

30 Paragraph 187A(4)(e).

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Committee Comment

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

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

Recommendation 4

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

Is the proposed data set sufficiently clear?

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

3.44 Optus assured the Committee that it had:

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

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

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

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

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

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

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

Passwords and PINs

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

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

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

Data that is not readily available to service providers

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

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

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

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

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

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

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

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

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

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

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

Committee Comment

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

---

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

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

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

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

Recommendation 5

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

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

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

Recommendation 6

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) any name or address information;

(ii) any other information for identification purposes;

---

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

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

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

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

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

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

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

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

(i) billing or payment information;

(ii) contact information;

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

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

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

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

3.61 The Law Institute of Victoria posed the question:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.69 The IWG has acknowledged that:

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

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

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

Location information—Item 6

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> suspect makes a phone call immediately after the time a crime was committed, that phone call may appear suspicious. However, location records showing the phone call was made several suburbs from the scene of the crime would tend to remove that person from suspicion.[70]

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

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

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

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

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

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

---

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

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

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

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

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

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

3.83 As the Explanatory Memorandum notes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Committee comment

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

---

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

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

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

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

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

Types of data excluded from the data set

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

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

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

Contents or substance of a communication

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

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

Defining 'contents or substance' of a communication

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Can content be reliably separated from telecommunications data?

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

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

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

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

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

Web-browsing histories

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

> information that:

---

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

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

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

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

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

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

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

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

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

3.110 The IWG report provides greater detail on this exclusion:

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

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

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

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

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

3.112 The Explanatory Memorandum states:

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

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

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

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

Impact on national security and law enforcement investigations

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

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

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

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

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

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

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

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

Concerns about the drafting of this exclusion

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

Definition of the term 'session'

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.130 The Explanatory Memorandum states:

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

3.131 Similarly, the IWG report states that:

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

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

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

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

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

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

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

Committee comment

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

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

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

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

Recommendation 7

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

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

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

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

Recommendation 8

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

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

4

Data retention period

The retention period

4.1 Subsection 187C(1) of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) provides that service providers must retain most telecommunications data covered by the data set for two years after it comes into existence.

4.1 The exception to this general rule is 'subscriber data', being data covered by paragraph 187A(2)(a), which must be retained from when it is created until two years after the closure of the relevant account. However, subsection 187C(2) provides that regulations may still prescribe the shorter, two-year retention period for specified subscriber data. The Government's proposed data set, included at Appendix A to this report, states that:

> The regulations will also limit the retention of subscriber information described in item 1 (c)-(f) to two years from creation of that data.

4.2 Accordingly, name, address and contractual information would be required to be kept for the life of the account plus two years, and all other telecommunications data covered by the data set would be required to be kept for the shorter, two-year period.

4.3 The Explanatory Memorandum explains why a longer retention period has been included for subscriber data:

> Subscriber records are typically generated when an account or service is opened, and may not be updated for many years. The purpose of this provision is to ensure that subscriber records associated with an account are available throughout the life of the account, and for as long as records relating to communications sent using that account are retained. This is intended to ensure

> that the necessary information is available to establish a connection between a particular communication and the subscriber.[1]

4.4 The Explanatory Memorandum also states that:

> A retention requirement of two years is consistent with the aim of the legislation and is necessary having regard to the reasonable requirements of national security and law enforcement agencies to have telecommunications data available for investigations and the privacy of users of the Australian telecommunications system.[2]

4.5 The Statement of Compatibility with Human Rights further explains the necessity and proportionality of a two-year retention period:

> The retention period reflects international experience that, while the majority of requests for access to telecommunications data are for data that is less than 6 months old, certain types of investigations are characterised by a requirement to access to data up to 2 years old. These include complex investigations such as terrorism, financial crimes and organised criminal activity, serious sexual assaults, premeditated offences and transnational investigations. Against the particular context of the critical importance of telecommunications data in very serious crime types and security threats, the two year retention period provides a proportionate response to that environment.[3]

General discussion

4.6 The Australian Privacy Commissioner provided extensive evidence on this issue, covering the privacy implications of various retention periods, how the Committee should approach assessing the necessity and proportionality of particular retention periods, and his assessment of what retention period is supported by the publicly-available information. As a starting principle, the Commissioner stressed the need to ensure that the retention period is set at the minimum necessary for law enforcement and national security purposes:

> To minimise any impact, I would suggest that the committee should satisfy itself, firstly, that each item of the dataset that service providers would be required to collect and retain under the scheme is necessary and proportionate; and secondly, that the

1 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 48.

2 Data Retention Bill, *Explanatory Memorandum*, p. 48.

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

> retention period imposed in relation to each item of the dataset is also necessary and proportionate.[4]

4.7 The Commissioner's view was also supported by the Law Council of Australia.[5]

4.8 A number of submissions cited various figures published by the European Commission showing the age breakdown for requests for access to telecommunications data by EU member-States.[6] There was some variability between the figures cited, however, as different submitters selected different date ranges. The Attorney-General's Department produced a table summarising figures released by the European Commission in its report, *Statistics on requests for data under the directive for 2008-2012*, which appear to be the most comprehensive figures available. These figures are set out at Table 4.1 below.

Table 4.1 Summary of age of telecommunications data requested under the EU Data Retention Directive in countries with two-year data retention periods, 2008-12

	Age of telecommunications data requested (months)							
	0–3	*3–6*	*6–9*	*9–12*	*12–15*	*15–18*	*18–21*	*21–24*
Percentage of requests	57.81%	19.59%	8.03%	5.03%	2.80%	2.00%	1.51%	3.24%
Cumulative percentage of requests	57.81%	77.40%	85.43%	90.46%	93.25%	95.25%	96.76%	100.00%

Source *Attorney-General's Department, Submission 27, p. 30.*

4.9 In its submission, the Department provided a detailed justification for a two-year retention period, based on its assessment of the European Commission's review:

> It is essential to distinguish between the frequency with which agencies access older data, and the importance of that data to investigations when it is accessed: where agencies require access to telecommunications data, its value does not decrease with age. While the review found that approximately 90% of requests for access relate to telecommunications data less than twelve months old, this number is skewed heavily by the use of telecommunications data in more straight-forward 'volume crime' investigations that, despite being serious in nature, can frequently

4 Mr Timothy Pilgrim PSM, Australian Privacy Commissioner, *Committee Hansard,* Canberra, 29 January 2015, p. 46.

5 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard,* Canberra, 30 January 2015, p. 33.

6 See, for example: Australian Human Rights Commission, *Submission 42*, p. 8; Muslim Legal Network (NSW), *Submission 198*, p. 11.

be resolved in a shorter period of time. As such, the above summary obscures the fact that certain types of law enforcement investigations frequently involve longer investigatory periods and therefore require a disproportionate level of access to older telecommunications data.

4.10 The Department explained that these types of investigations included:

- counter-terrorism and organised crime investigations, which are often characterised by long periods of preparation. These investigations often require time to establish a clear pattern of relationships between multiple events to expose not just individual suspects, but entire criminal networks, especially where suspects are practicing sophisticated counter-surveillance techniques
- series of related crimes, where agencies are required to piece together evidence from a wide range of sources, not all of which may be immediately evident
- cyber-crimes and other crimes where access to IP-based telecommunications data is required, due to the greater complexity of these investigations—the EU statistics show agencies are up to 7 times more likely to access IP-based data that is more than 12 months old than mobile telephony data
- trafficking in human beings and drug trafficking, where there is often a complex division of labour between accomplices
- serious corruption of public officials, financial crime and tax fraud, where offences are often only detected following audits, or are only reported to law enforcement agencies following internal investigations, requiring agencies to often access data that is already considerably dated
- repeated extortion, where victims are in a relationship with the offender and often only seek help months or even years after the exploitation commenced
- serious sexual offences, where victims may not report the offence for a considerable period of time after the event—for example, the United Kingdom Government has provided advice that over half of the telecommunications data used by its agencies in the investigation of serious sexual offences is more than six months old
- serious criminal offences, particularly in relation to murder investigations, where extensive historical evidence must be assembled to prove intent or premeditation, and
- transnational investigations, which involve significant challenges for agencies attempting to coordinate investigations across multiple jurisdictions, frequently resulting in delays

> while preliminary information is obtained from foreign agencies.[7]

4.11 The Department added that:

> More broadly, many crimes are not brought to the attention of the relevant authorities until well after the fact, and the normal variability in criminal investigations means that some investigations will continue for considerably longer than average. In such cases, reliable access to telecommunications data can be particularly important, as physical and forensic evidence will frequently degrade with the passage of time.[8]

4.12 The Committee received a number of submissions and heard evidence from a number of witnesses calling for a shorter retention period, either for all or part of the data set.

4.13 Blueprint for Free Speech recommended that, if the Committee recommended passing the Bill, the retention period should be capped at six months to limit the privacy and regulatory impacts. It noted that, for countries subject to the former EU Data Retention Directive:

> the period of storage is typically between 6-12 months. This is well short of the 2-year period proposed by this legislation. In fact, these periods are likely too long. A report on the UK experience demonstrated that in approximately 75% of cases over a 4-year period, the data sought to be accessed was less than 3 months old.[9]

4.14 Similarly, the Law Institute of Victoria argued that the retention period should be reduced to what is 'strictly necessary and proportionate' and argued for a six month period.[10]

4.15 The Australian Privacy Commissioner provided a detailed assessment of what retention period he believed is supported by the publicly-available information:

> Statistical evidence, both international and domestic, seems to suggest that a large proportion of investigations use telecommunications data that is up to or less than one-year old. Acknowledging that there are differing views on what this evidence shows, it could nevertheless support a case for a shorter one-year data retention period. However, the case for a two-year data retention scheme is less clear. It may rest on information that is being made available to the committee but which is not being

7 Attorney-General's Department, *Submission 27*, p. 31.

8 Attorney-General's Department, *Submission 27*, p. 31.

9 Blueprint for Free Speech, *Submission 54*, p. 13.

10 Law Institute of Victoria, *Submission 117.1*, p. 10.

> released publicly—I assume to ensure that it does not prejudice the activities of law enforcement and security agencies. It is therefore important that close consideration be given to whether the evidence provided to the committee establishes that it is necessary to retain each item of telecommunications data for a minimum period of two years or, alternatively, whether a shorter retention period would meet the needs of law enforcement and security agencies.[11]

4.16 However, the Commissioner confirmed that he does not rule out a two-year retention period being justified as necessary and proportionate,[12] and cautioned that the Committee should have regard to the gravity of the matters that require access to older telecommunications data, and not place undue weight on the raw figures showing that such data is accessed in only a minority of cases:

> We should not just limit it to the number of cases because, as we start looking at some of these matters—I am feeling a bit odd here because it seems like I am starting to defend the position of the law enforcement and security agencies—it is about how large an impact they could have on the community. A particular investigation could be one that prevents an attack which could impact on hundreds or thousands of people.[13]

4.17 The Commissioner also observed that, given that the proposed data set makes clear the Government's intention to limit the retention period for items 1(c) to 1(f) of the data set to two years, rather than the life of the account plus two years, 'there does not appear to be a compelling reason for that limitation not to be contained in the Bill.'[14]

4.18 The Australian Human Rights Commission noted the EU Court of Justice's conclusion that retention periods should be limited to that which is 'strictly necessary',[15] and that the proposed two-year retention period is 'at the upper end of retention periods implemented in comparable jurisdictions'.[16] In its submission, the Commission argued that the Bill should be amended to incorporate a one-year retention period on a trial basis, subject to the statutory review by this Committee.[17] However, at a

11 Mr Pilgrim, *Committee Hansard,* Canberra, 29 January 2015, p. 46.

12 Mr Pilgrim, *Committee Hansard,* Canberra, 29 January 2015, p. 55.

13 Mr Pilgrim, *Committee Hansard,* Canberra, 29 January 2015, p. 48.

14 Office of the Australian Information Commissioner, *Submission 92*, p. 15.

15 *Digital Rights Ireland v Ireland*; *Kärtner Landesregierung, Seitlinger and Tschohl* (joined cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014), [64].

16 Australian Human Rights Commission, *Submission 42*, p. 9.

17 Australian Human Rights Commission, *Submission 42*, pp. 8-9.

public hearing, the Commission's President, Professor Gillian Triggs, noted that international comparison are 'relevant evidence; it is not determinative',[18] and that she 'would not argue too strongly for a year'.[19]

4.19 Professor Triggs went on to argue that 'the debate about the period is missing the core point',[20] and that, as the objective of data retention is to facilitate the better investigation of persons involved in serious crime and threats to security, uniform data retention is a 'crude instrument to deal with a problem that is a very sophisticated one and one where considerably greater lengths of time may be necessary.'[21] In this vein, Professor Triggs proposed that the uniform data retention period be coupled with an independent administrative mechanism to allow the retention period to be extended—potentially by many years—in relation to specific matters, such as the investigation of a serious risk to security or a child exploitation network.[22] The Committee discussed this proposal with Professor Triggs in significant detail.

4.20 The Committee also received evidence from organisations and members of the community in favour of the proposed two-year retention period. For example, Bravehearts noted the importance of a longer retention period for serious criminal investigations and recommended that the retention period be further assessed as part of the mandatory review established by the Bill:

> While the European Union's period and statements from police demonstrate that many investigations are completed within months, serious crimes often necessitate access to older records as the criminal behaviour may span a number of years. This is particularly true for investigations of child sexual exploitation.
>
> We note that the data retention period set in the Bill is at a minimum of two years and support this proposal. In addition, Bravehearts would recommend that after a three year period, as part of a review of the legislation, an assessment be made as to whether the 2 year retention period is the most appropriate length of time.[23]

4.21 Professor George Williams and Dr Keiran Hardy, in their capacity as members of the Gilbert + Tobin Centre of Public Law at the University of

18 Emeritus Professor Gillian Triggs, President, Australian Human Rights Commission, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

19 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

20 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

21 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 71.

22 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, pp. 71-75.

23 Bravehearts, *Submission 33*, p. 4.

New South Wales, expressed the view that, as of 9 December 2014, the Government had not yet justified a two-year retention period:

> The government has reasoned that data less than six months old is the most frequently accessed, but data up to two years old can be necessary for investigations into terrorism and other complex criminal offences. Given that this timeframe is central to the operation of the regime, we believe that a stronger case needs to be made as to why it is necessary. … In particular, a stronger justification for the two-year timeframe could help to reduce public perceptions that the Bill is designed to allow mass surveillance of the population.[24]

4.22 However, in evidence to the Committee on 30 January 2015, Professor Williams advised that he had revised his position, based on the submissions and evidence provided by the Attorney-General's Department and government agencies:

> The first thing I will say is that that statement was made on 9 December, when we did not have access to other submissions that have now provided a much higher degree of detail about this. Indeed, I would say that I am very pleased to see that those agencies are now strongly making the case as to why that two-year period is necessary. One thing I have looked at carefully is the table on page 30 of the Attorney-General's Department's submission, where, based on European data, they have also given an indication as to when certain data is accessed. I do not have a strong view on this issue, because I think it is one that depends very much on operational issues. I think it gets outside of my expertise.
>
> But I suppose the threshold question for me is that, based on the European data, over 90 per cent of all requests are made within the first 12 months. Is the case compelling enough to extend it for another 12 months, given the cost and the extension of the scheme? As the submission indicates, it perhaps might be justified if it can be shown that in fact terrorism investigations, particularly, tend to take place in that second 12-month period. If that is the case then perhaps that threshold I have indicated can be met.[25]

4.23 As discussed in Chapter 6, a joint submission from a number of media organisations argued that the introduction of a data retention regime would increase the difficulty faced by journalists in gathering information

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

25 Professor Williams, *Committee Hansard,* Canberra, 30 January 2015, pp. 7-8.

from confidential sources.[26] However, in evidence, Ms Georgia-Kate Schubert, Head of Policy and Government Affairs for News Corp. Australia, confirmed that the actual retention period is of significantly less concern to journalists than is the underlying ability of law enforcement and national security agencies to be able to identify confidential sources.[27]

Industry interests

4.24 Following a public hearing with the Communications Alliance and the Australian Mobile Telecommunications Association (AMTA), the Committee requested that Telstra, Optus, Vodafone, iiNet, TPG, Next Telecom, M2 Group, and the Inabox Group provide submissions setting out their existing retention practices. These companies represent a broad cross-section of the telecommunications industry, including the major, vertically integrated carriers, large ISPs, enterprise providers, and companies providing dedicated services to small and medium ISPs. The Committee received commercially confidential submissions from Telstra, Optus and Vodafone,[28] as well as an item of correspondence from the Inabox Group.

4.25 The Director-General of Security also provided the Committee with an unclassified summary of ASIO's assessment of existing industry practices in relation to critical categories of telecommunications data (Table 4.2),[29] as well as a more granular, classified assessment.[30]

4.26 The Committee has carefully reviewed the submissions provided by service providers and ASIO, and considers that ASIO's unclassified assessment, reproduced in Table 4.2 below, provides a useful summary of existing retention practices across the telecommunications industry.

---

26 Joint media organisations, *Submission 125*, p. 1. The joint submission was made on behalf of Australian Associated Press, the Australian Broadcasting Corporation, APN News and Media, the Australian Subscription Television and Radio Association, Bauer Media, Commercial Radio Australia, Fairfax Media, FreeTV, the Media, Entertainment and Arts Alliance, News Corp. Australia, the Special Broadcasting Service, The Newspaper Works, and the West Australian.

27 Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp. Australia, *Committee Hansard,* Canberra, 29 January 2015, p. 93.

28 Telstra, *Submission 112.1*; Optus, *Submission 86.1*; Vodafone, *Submission 130.1.*

29 ASIO, *Submission 12.2*, p. 5.

30 ASIO, *Submission 12.2*, Appendix B; and *Submission 12.3*.

Table 4.2 Comparative ranges of retention by main service providers of historical communications data

Matters to which information must relate	Telephony	Internet
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Up to 7 years (and longer)	90 days to 5 years
2. The source of a communication	6 weeks to 7 years 62 days to 7 years (for SMS)	0 days to 5 years
3. The destination of a communication		
4. The date, time and duration of a communication, or of its connection to a relevant service		
5. The type of communication or relevant service used in connection with a communication	Up to 7 years	90 days to 5 years

Source *Australian Security Intelligence Organisation, Submission 12.2, p. 5.*

4.27 The Attorney-General's Department and Communications Alliance separately drew the Committee's attention to the Telecommunications Consumer Protection Code, which requires all carriage service providers who supply telecommunications products to consumers in Australia to retain 'Billing Information' for at least six years.[31] Billing information includes any information necessary for the purposes of:

- calculating and assembling charges incurred by a customer during a billing period,
- applying any debits or credits outstanding or discounts due against the charges, and calculating the net amount payable by the customer,
- issuing and delivering bills to the billing address,
- handling billing enquiries, and
- receiving and receipting payments made by the customer.[32]

4.28 Optus confirmed that, for its networks and services, the general requirement to keep the proposed data set for two years 'is a workable time period for most data types'.[33] Optus also confirmed that, while the extended retention period for subscriber records 'has the potential to create some additional record keeping complexity depending on the compliance approach adopted', this requirement would overall not 'create

31 Telecommunications Consumer Protection Code, p. 47.

32 Telecommunications Consumer Protection Code, p. 12.

33 Optus, *Submission 86*, p. 10.

any significant retention burden as most of this type of information is already kept by Optus for longer than these periods for other legal reasons'.[34]

4.29 A number of industry representatives also noted that, given the significant variation between service providers' commercial retention practices, many service providers do not currently retain some of the types of telecommunications data covered by the proposed data set. For example, Mr Michael Elsegood, appearing as a member of the Communications Alliance and AMTA, explained that:

> On the usage side is where I think there is probably a greater discrepancy. Some service providers might be billing on a fairly bulk basis and would not be collecting fine-detail information about the customer's services. In that sense, they may not have the detailed usage records that might be required out of a data retention regime. On the mobile side, any information about mobile location may not be being stored in systems at all because there is simply no business reason to keep track of where your customers are. From an operational point of view, you may keep that for a very short period of time to deal with customer complaints or technical complaints about the operation of your network. So you might keep some short-term records about how your network has been performing. But in the long term you would not be keeping that sort of stuff.[35]

4.30 The Communications Alliance summarised this issue in the following terms:

> It is a data creation regime as well as a data retention regime, for all of those providers who do not presently retain everything in the dataset.[36]

4.31 This statement was consistent with ASIO's assessment of current retention practices across the telecommunications industry, which notes that some service providers currently retain some categories of telecommunications data for '0 days'.[37] The Attorney-General's Department noted that while all of the categories of telecommunications data contained in the proposed data set 'exist' on providers' networks, as they are 'typically required in the provision of the communications service itself', some types of data

34 Optus, *Submission 86*, p. 10.

35 Mr Michael Elsegood, Member of Communications Alliance and Manager of Regulatory Compliance and Safeguards, Optus, *Committee Hansard,* Canberra, 17 December 2014, p. 37.

36 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard,* Canberra, 17 December 2014, p. 31.

37 See Table 4.2 above.

may exist only 'fleetingly'.[38] In such situations, service providers would be required to begin collecting and retaining such telecommunications data.

4.32 Proposed new subsection 187A(6) of the Bill makes clear that service providers would be required to create any relevant information that was not currently retained. The Explanatory Memorandum states that:

> Subsection 187A(6) will clarify that if the information or documents that service providers are required to keep under subsection 187A(1) are not created by the operation of the relevant service, or if they are only created in a transient fashion, then the service provider is required to use other means to create this information or document.
>
> Mandatory data retention is the creation of a consistent minimum standard across the telecommunications industry for what data is to be collected and how long it is to be retained. Subsection 187A(6) will ensure that all service providers must meet this minimum standard, whether or not that data is currently being collected or retained by the relevant service provider.[39]

4.33 Optus also noted that there are likely to be a small number of cases in which the retention of certain categories of telecommunications data for particular services would be more difficult, and recommended amending the Bill to allow the regulations to prescribe a shorter retention period for 'specific or "special case" data or service types' would enhance the flexibility of the overall data retention arrangements.[40]

4.34 In its supplementary submission, the Attorney-General's Department has advised that :

> The Department has sought to estimate the cost of implementing the proposed data retention obligation, including seeking to assess the variation in capital costs of implementation if data were to be retained for 12, 24 and 36 months respectively. Extending the data retention period for industry participants will increase the capital costs of implementation; however a preliminary assessment indicates that the costs impacts are modest, and are substantially less than the percentage change in the retention period.[41]

---

38 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard,* Canberra, 17 December 2014, p. 11.

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

40 Optus, *Submission 86*, p. 10.

41 Attorney-General's Department, *Submission 27.2*, pp. 4-5.

4.35 The Committee also received a confidential briefing on the preliminary findings of the PricewaterhouseCoopers report on the costs of implementing data retention.

4.36 The Committee has considered the implications of a two-year retention period across a range of different data types below.

Law enforcement and security interests

4.37 Law enforcement and national security agencies supported a two-year retention period. A number of law enforcement agencies and ASIO noted that, from an investigative perspective, a retention period of greater than two years would be beneficial. However, there was recognition within the law enforcement and national security communities that mandatory data retention obligations should be used only to establish a minimum, legally-binding standard for record-keeping.

4.38 The Director-General of Security confirmed that ASIO supports a two-year retention period,[42] but emphasised that due to ASIO's unique investigative requirements, particularly in relation to counter-espionage investigations, this two-year period was the 'minimum' viable retention period from his perspective.[43] ASIO's submission stated:

> A two year retention period is a compromise from ASIO's perspective – we would prefer a longer retention period due to the long-term nature of some security threats, the sophistication of foreign intelligence actors, and that intelligence lead information can surface many months or years after an event has occurred. For example, leads to individuals who have recruited spies or facilitated individuals to terrorist training camps require ASIO to examine historical connections to understand those they may have influenced to engage in activities prejudicial to Australia's security.[44]

4.39 ASIO and the Attorney-General's Department advised the Committee that the proposed two year retention period is the result of 'extensive' engagement between the Attorney-General's Department, and law enforcement and national security agencies. In the course of these consultations, ASIO had advocated for a retention period of up to five years, however the Department concluded that the shorter, two-year retention period would be proportionate to the legitimate ends of

42 Mr Duncan Lewis AO DSC CSC, Director-General of Security, ASIO, *Committee Hansard,* Canberra, 30 January 2015, p. 64.

43 Mr Lewis, *Committee Hansard,* Canberra, 30 January 2015, p. 66.

44 ASIO, *Submission 12.1*, p. 9.

safeguarding national security and public safety, and the enforcement of the criminal law.[45]

4.40 ASIO addressed the Australian Privacy Commissioner's comments in relation to the potential distinction between the number of authorisations made for access to telecommunications data more than two years old, and the relative gravity of the subject matter of the investigations to which those authorisations relate:

> A point that was made by one of the previous witnesses here was that the data we pull from deeper into the time period is quite often the most important because it will be some critical piece of a major inquiry. I would also—and this is a particular and peculiar requirement for ASIO—reinforce the point that counterintelligence investigations have a very long sine wave.[46]

4.41 The Australian Federal Police (AFP) emphasised that, while the majority of criminal investigations relate to relatively recent conduct, complex and serious investigations often require access to telecommunications data from a considerable time ago:

> The nature of criminal investigations means that the bulk of matters subject to investigation relate to relatively recent conduct. However, where those investigations relate to historical events, the investigation will likely be more complex, relate to more serious conduct, or both. While the volume of requests for telecommunications data beyond 12 months old is likely to be lower than for more recent data, the relative value of that data is likely to be more significant.
>
> An example of historical events that may be the subject of investigation are international child protection operations, where information on Australian IP addresses are identified. This process may take a significant amount of time, meaning that data could be more than a year old before it becomes available to Australian authorities. Delays in the provision of information may relate to:
>
> - Lack of control over prioritisation or legal processes in foreign partner agencies;
> - Administrative processes associated with international cooperative
> - arrangements;
> - Establishment of coordinated international operational activity;
> - Technical difficulties in analysis of source data.[47]

45 *Committee Hansard,* Canberra, 30 January 2015, p. 68.

46 Mr Lewis, *Committee Hansard,* Canberra, 30 January 2015, p. 66.

47 AFP, *Submission 7*, p. 3.

4.42 The AFP stressed that the value of telecommunications data does not diminish with age, and that in many cases its value will increase as other sources of evidence are lost:

> [T]here is no clear correlation between the age of the information and its intrinsic value. Depending on the type of investigation, telecommunications data could be as important five years after an event as it is in the immediate aftermath. Moreover, in complex cases the value of older data may increase, particularly where physical evidence has eroded or (as is the case [in] cyber investigations) it is non-existent, making telecommunications data the key piece of information and evidence available.[48]

4.43 Deputy Commissioner Michael Phelan noted that agencies are often not in a position to even begin investigations for some time after a crime has been committed, due to delays in criminal activity being brought to their attention:

> You are actually beholden to when the originating information comes to you not from when the offence occurred. So an offence occurred last year, three years ago, two years ago, 10 years ago but you can only start the investigation when you know about it. That has sometimes been lost on some of our commentators, that they think the offence occurred and straightaway we have access to the information. That is not true.[49]

4.44 The Australian Commission for Law Enforcement Integrity (ACLEI) explained the particular importance of older data to anti-corruption investigations:

> The sophistication of corrupt networks (and organised criminals generally) develops over time. If left undisturbed, it is likely that they will become competent at counter-surveillance and increase their ability to defeat law enforcement efforts.
>
> …
>
> The means and frequency of contact with each individual varies over time, making it difficult to know how wide a corrupt network is, or how deep the compromise may be. Older data can be more useful, since it increases the chances of hidden relationships being discovered.[50]

---

48 AFP, *Submission 7.1*, p. 5.

49 Deputy Commissioner Michael Phelan APM, Australian Federal Police, *Committee Hansard,* Canberra, 30 January 2015, p. 75.

50 Australian Commission for Law Enforcement Integrity, *Submission 48*, p. 5.

4.45 ACLEI also provided the Committee with a detailed case study analysing the role that 18-month old telecommunications data played in Operation Heritage/Marca. The investigation, which began in 2011, uncovered a drug importation ring involving corrupt Customs and Department of Agriculture officials that had been operating since at least 2007. Initial investigations considered a particular associate as being benign. However, subsequent analysis of telecommunications data up to 18 months old demonstrated that this associate did, in fact, have corrupt connections, had been involved in criminal conduct, and was in fact a central figure in the conspiracy. The associate had, however, become more cautious over time and had adopted more sophisticated tradecraft that enabled him to avoid other forms of detection, including in the initial stages of Operation Heritage/Marca.[51]

4.46 From the perspective of a state police force, the New South Wales Police Force (NSW Police) argued that a longer retention period would be preferable:

> Whilst two years may be appropriate for the majority of offences investigated by the Commonwealth, such as national security, drug and online sexual offences, states are also responsible for investigating a range of criminal offences, including murders, sexual assaults and robberies, which are often historical or take years to investigate prior to a suspect being identified.
>
> …
>
> The need for data retention for extended periods is even more important at the moment, as DNA, trace evidence and other forensic science becomes more sophisticated and it is possible to test against older crime exhibits, resulting in the identification of suspects years after offences being committed.[52]

4.47 NSW Police provided the Committee with a detailed account of the types of matters currently under investigation dating back more than five years:

> [T]o perhaps clarify that this is not just rhetoric, we have some records on our books at the moment that justify data in excess of five years. Whilst they are minimal, as Mr Lanyon has alluded to—minimal in terms of the volume of requests that are handled up-front in the first six to 12 months—we have nearly 1,000 cases involving most-serious fraud, unsolved homicides, historical

51 Australian Commission for Law Enforcement Integrity, *Submission 48*, pp. 7-8.

52 Assistant Commissioner Mal Lanyon APM, Commander, Special Services Group, New South Wales Police Force, *Committee Hansard,* Canberra, 30 January 2015, p. 43.

> sexual assaults, and a lot of clear-up armed robberies. They are fairly complex crimes in that batch.[53]

4.48 Victoria Police similarly advised the Committee that:

> If we are looking at an investigation that may be afoot three, four, five or six years after a communication, almost invariably it is going to be an investigation of great significance. Law enforcement is not going to take on an incident that occurred that long ago, unless it is a homicide, a sex crime, a crime of significant personal violence, a counterterrorism inquiry or something of that nature.
>
> The other point I would make, and I think it has already been borne out in other evidence before you, is that the reality is that the bulk of these types of inquiries are made when this data is relatively new. Minimal inquiries are made father out. But again, they are ones that pertain to investigations that are probably of greater import.[54]

4.49 NSW Police also highlighted to the Committee that law enforcement agencies are not only required to access telecommunications data as part of criminal investigations, but are also required to access such information at the request of prosecutors and defendants in the course of proceedings, which can occur months or even years after the investigation itself concludes:

> [W]hen a court proceeding comes up, whether it is a trial, a hearing or a committal, somewhere down the track, whether it is two, three, four or five years, we get requests from the DPP and from the defence in terms of alibis, in terms of checking out a particular witness's statement, a particular location or a particular subscriber. So we get after the fact type requests for metadata.[55]

4.50 South Australia Police further argued that the importance of telecommunications data aged more than two years' old is likely to increase into the future, rather than decrease:

> If we got to two years, from an investigative perspective that is a retrograde step, especially when you are dealing with more and more historical offences, be they murders or historical sex offences, which do require that information. All of us around the table here

---

53 Detective Superintendent Arthur Kopsias APM, Commander, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard,* Canberra, 30 January 2015, p. 52.

54 Inspector Gavan Segrave, Intelligence and Covert Support Command, Victoria Police, *Committee Hansard,* Canberra, 30 January 2015, p. 51.

55 Detective Superintendent Kopsias, *Committee Hansard,* Canberra, 30 January 2015, p. 52.

> would understand that the reliance on and use of electronic devices such as those we are talking about is not going to go away. It is increasing. So we will become more and more reliant on this sort of technology in the future.
>
> From a law enforcement perspective and, I would imagine, also from a security perspective, the longer the data is kept the better because there will be investigations where we would ordinarily have sought information that goes back beyond two years. This is about trying to create a minimum standard that is level across the industry. As the department has already said, there are internet providers now who routinely hold this information for up to seven years and perhaps longer, depending on the way their systems are configured. From a policing perspective, that would be beneficial to us. But this is about creating a minimum standard. … Two years is a time frame that law enforcement and security agencies have accepted. That is appropriate in the circumstances, but I can see instances where we will still claw back further than two years if the data is held. If data is not held under this regime then it is not available to us.[56]

4.51 NSW Police expressed concern that the proposed two year retention period would not prevent service providers from reducing their current retention practices to a two-year minimum, which would significantly reduce the period of time for which certain types of telecommunications data are retained:

> The reason that New South Wales has asked for that period of two years, particularly with call charge records and reverse call charge records and subscriber checks to be longer than that period is that there is nothing to stop a service provider keeping for commercial purposes what are only billing records, after two years.[57]

4.52 On 4 December 2014, the Committee wrote to the heads of the ACC, AFP, ASIO and State and Territory police forces to request information about their agencies' access to and use of both stored communications and telecommunications data. In particular, the Committee sought information about the age breakdown of historical telecommunications data for which access was sought in each of the past five years.

---

56 Assistant Commissioner Paul Dickson, Crime Service, South Australia Police, *Committee Hansard,* Canberra, 30 January 2015, p. 52.

57 Assistant Commissioner Lanyon, *Committee Hansard,* Canberra, 30 January 2015, p. 51.

4.53 Some were unable to provide the Committee with information about the age breakdown of historical telecommunications data for which access was sought. For example, the Western Australia Police stated that:

> the systems used do not permit interrogation to identify the age of the data requested. Each request would have to be manually checked to identify the date range, and WA Police is unable to allocate resources required to provide the information without affecting core policing services.[58]

4.54 South Australia Police was able to provide the Committee with an age breakdown for the historic telecommunications data for which access was sought. Between 1 July 2010 and 31 June 2014:

- data less than three months old was sought in between 36.9 per cent and 38.9 per cent of authorisations,
- data between three months old and 12 months old was sought in between 0.1 per cent and 1.2 per cent of authorisations, and
- data more than 12 months old was sought in between 61 per cent and 62.1 per cent of authorisations.[59]

4.55 Queensland Police advised that, while its record keeping systems were not designed to specifically record the requested information, it had attempted to manually analyse the available information for the 2013 and 2014 calendar years:

> Although the data showed a strong tendency towards recent information this is attributable to the fact [that] most offences are reported soon after occurring and investigations that use a high volume of telecommunications information, such as drug matters, are focused on current real time events.
>
> The sample set did show at least 10% of authorisations were for information over 12 months old; however the sample set is considered to be too small to provide a reliable indication of the true requirement for and value of information more than 12 months old. Anecdotally, it is offences such as cold case homicide, historical sex offences and other serious offences where new suspects are identified that require older telecommunications data.[60]

4.56 In public evidence, Ms Kerri Hartland, Acting Director-General of Security, explained that:

---

58 Western Australia Police, *Submission 11*, p. 2.

59 South Australia Police, *Submission 9*, pp. 2-3.

60 Queensland Police, *Submission 19*, pp. 2-3.

> Around 10 per cent of the requests are for periods of 12 months or more, leading into periods of up to two years and beyond. Those cases relate to—10 per cent may seem small number—our most serious and complex cases. Typically, these relate to activities of hostile foreign nationals or nations engaged in spying and influence operations against Australia.[61]

4.57 The Committee also received a classified submission from ASIO containing the number of data authorisations made by ASIO over the past five years, as well as a breakdown of the age of data requested. The information contained in that classified submission is consistent with Ms Hartland's evidence. It is also consistent with the previous evidence of the former Director-General of Security, Mr David Irvine, to the Senate Legal and Constitutional Affairs References Committee that the number of authorisations made by ASIO for access to telecommunications data each year is 'proportionate… with other individual agencies.'[62]

4.58 The New South Wales Ministry for Police and Emergency Services provided the Committee with a confidential submission containing detailed statistics on its use of telecommunications data.[63] NSW Police also provided some information on its use of telecommunications data in at a public hearing:

> Of the 122,000 requests for telecommunications data New South Wales submitted in the previous year, 4,358 of those requests related to a period greater than two years for retention. Whilst as a percentage this may not appear large, it represents a significant number of offences which may be solved with the access to the information after two years. It is worth pointing out that, of those requests for greater than two years' data, the most common offence was murder, followed by sexual assault and then robbery.[64]

4.59 Communications Alliance and the AMTA confirmed that the majority of requests received by service providers from agencies 'relate to data that is 6 months old or younger'.[65]

4.60 The Committee also received supplementary submissions from Telstra, Optus and Vodafone setting out the age-breakdown of requests for

---

61 Ms Kerri Hartland, Acting Director of Security, ASIO, *Committee Hansard,* Canberra, 17 December 2014, p. 5.

62 Mr David Irvine AO, *Committee Hansard,* Canberra, 21 July 2014, p. 10.

63 New South Wales Ministry for Police and Emergency Services, *Submission 199*.

64 Assistant Commissioner Lanyon, *Committee Hansard,* Canberra, 30 January 2015, p. 43.

65 Communications Alliance and AMTA, *Submission 6*, p. 8.

telecommunications data each service provider had received. Telstra's submission showed that, in the 2014 calendar year:

- 79% of requests related to data less than six months old,
- 11% of requests related to data more than 12 months old, and
- 4% of requests related to data more than 24 months old.[66]

4.61 Vodafone's and Optus' submissions contained a higher level of detail and were provided to the Committee on a confidential basis.

4.62 However, at a public hearing Vodafone noted that its experience in relation to telephony data is that approximately three quarters of all requests relate to data less than six months old, while approximately 15 per cent of requests relate to data more than 12 months old.[67] The figures contained in Vodafone's confidential submission are consistent with this evidence, [68] and the figures provided by Optus were broadly consistent with those provided by Telstra and Vodafone.[69]

4.63 A number of witnesses, from both Government and industry, cautioned that the age breakdowns for access to historic telecommunications data are limited by industry's current retention practices and so reflect the age of data that agencies are able to access, rather than the age of data that may be of benefit to law enforcement and national security investigations.[70]

4.64 Optus also noted that the statistical information available about the age breakdown of requests may be misleading due to a number of factors that would tend to understate the importance of access to older telecommunications data to investigations, and in particular for investigations into suspects using particular counter-surveillance techniques:

> The one thing I would say is to exercise some caution in drawing immediate conclusions about where the volume of requests lies in terms of the age of the information, because I think you always have to apply a matrix about the seriousness of the request and the preservation regimes which might operate in tandem.
>
> …
>
> There is one other thing that perhaps I would say. This is particularly Optus specific, and it is not necessarily drawn out in

66 Telstra, *Submission 112.2*, p. 2.

67 Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (Vodafone), *Committee Hansard,* Canberra, 29 January 2015, p. 60.

68 Vodafone, *Submission 130.2*.

69 Optus, *Submission 86.2*.

70 See, for example, Queensland Police, *Submission 19*, p. 3; Mr Elsegood, Optus, *Committee Hansard,* Canberra, 17 December 2014, p. 34.

> the table that we have provided to the committee in confidence, but it is worth noting. We have a large, prepaid mobile base of customers and, indeed, are suppliers to resellers, who also do that. And there a number of reasons why people might prefer prepaid phones. The turnover of prepaid accounts can sometimes be greater. That does tend to explain a little bit why there is disproportionate interest in that particular cohort of customers. I think that does influence some of the timing and the age of the data that has been looked at to date.[71]

Retention periods for particular data types

4.65 While the above discussion focused on the overall retention period, the Committee also received more granular evidence on the necessity and proportionality of retaining particular types of telecommunications data.

4.66 The following pages discuss this evidence with regard to five semi-distinct classes of information:

- subscriber or account-holder records,
- IP address allocation records;
- telecommunications data relating to telephony services, other than location records,
- telecommunications data relating to internet-based communications services, such as email, VoIP and messaging applications, and
- location records.

Subscriber records

4.67 ASIO's unclassified assessment of industry retention practices indicated that there is some considerable variation in the periods for which service providers retain the range of subscriber records that are covered by item 1 of the Government's proposed data set, however, this variability relates primarily to subscriber records for internet-based services.[72]

4.68 Communications Alliance described subscriber records as being 'more static' than usage information, and advised that providers 'keep most of that sort of information for two years or so'.[73] As noted earlier, Communications Alliance also drew the Committee's attention to the requirements under the Telecommunications Consumer Protection Code

71 Mr David Epstein, Vice-President, Corporate and Regulatory Affairs, Optus, *Committee Hansard,* Canberra, 30 January 2015, pp. 20-21.

72 ASIO, *Submission 12.2*, p. 5.

73 Mr Elsegood, *Committee Hansard,* Canberra, 17 December 2014, p. 37.

to retain 'billing information', which includes many subscriber records, for at least six years.[74]

4.69 Similarly, Vodafone advised the Committee that it had 'always held the traditional telephony metadata—billing records, account holders—for certainly longer than two years'.[75]

IP address allocation records

4.70 Vodafone argued that IP address allocation records should be retained for no more than six months. Vodafone based this argument on the relative privacy sensitivity of this information, evidence about access rates from European jurisdictions, and the relative utility of historic IP address allocation records. In relation to the privacy sensitivity of this category of telecommunications data, Vodafone expressed the view, informed by customer feedback, that IP address allocation records are more sensitive than other categories of telecommunications data, and should therefore be retained for no more than six months:

> Traditional metadata is generally account information and phone numbers, and often that information is in the *White Pages* and so on. The feedback we are getting from consumers is that that kind of information is less sensitive than IP identifier information.[76]

4.71 However, Vodafone also explained that an IP address allocation record 'is essentially analogous to a telephone phone number, where a customer, when they access the internet, gets assigned an IP identifier so that they can carry out access to the internet'.[77]

4.72 The Committee also notes Vodafone's previous evidence to the Senate Legal and Constitutional Affairs References Committee, referred to above, that it intends to implement capability to collect these records for its own business purposes.[78]

4.73 The Attorney-General's Department's submission took an opposing view to Vodafone, arguing that:

> For internet access services, the types of telecommunications data that service providers would be required to retain (subscriber records and IP address allocation records) are less privacy

74 Mr Stanton, *Committee Hansard,* Canberra, 17 December 2014, p. 39.

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

76 Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia, *Committee Hansard,* Canberra, 29 January 2015, p. 60.

77 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 60.

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

> sensitive than the records they would be required to retain for 'traditional' telephony services (including call-charge and limited location records).[79]

4.74 Vodafone also highlighted the European Commission's *Evaluation Report*, which concluded that the majority of law enforcement requests for access to telecommunications data are for data less than six months old. However, Vodafone confirmed that it had only very limited experience with law enforcement requests for IP address allocation records.[80]

4.75 Vodafone further advanced the argument that law enforcement agencies would be relatively less interested in IP address allocation records aged more than six months old, compared to traditional telephony records aged more than six months old:

> Certainly our view is that IP identifier metadata would be of most use more immediately than telephony metadata. That is because it is ever-changing. I think it is going to be potentially useful in regard to IP telephony. I think there are other ways of overseeing that. But when you are talking about an 'under surveillance' website, an agency will be looking at a dodgy website, and IP identifier accesses that website and the agency wants to find out who that person is, it is unlikely that that will be in two years hence. It is much more likely to be an immediate offence.[81]

4.76 In evidence, Optus advised the Committee that it did retain IP address allocation records, albeit with some variability between different services.[82]

4.77 The Committee received confidential evidence from ASIO, Optus and other service providers on this issue about their current retention practices for IP address allocation records.[83] This evidence showed a great deal of variability between service providers, and even between services provided by the same provider, ranging from negligible through to well in excess of two years.

4.78 In its submission, the Attorney-General's Department noted that agencies are actually significantly more likely to need access to IP-based telecommunications data aged more than 12 months old compared to other types of telecommunications data, due to the more complex nature of cybercrime investigations. Additionally, the Committee notes that the

79 Attorney-General's Department, *Submission 27*, p. 32.

80 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, pp. 68-69.

81 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 64.

82 Mr Elsegood, *Committee Hansard,* Canberra, 30 January 2015, p. 21.

83 Optus, *Submission 86.1*; ASIO, *Submission 12.2*, Appendix B.

inherently global nature of internet-based communications means that the assistance of foreign law enforcement agencies is a more common requirement in investigations where such communications are involved. The Department stated:

> certain types of law enforcement investigations frequently involve longer investigatory periods and therefore require a disproportionate level of access to older telecommunications data. These types of investigations include, but are not limited to:
>
> …
>
> - cyber-crimes and other crimes where access to IP-based telecommunications data is required, due to the greater complexity of these investigations
>
> …
>
> - transnational investigations, which involve significant challenges for agencies attempting to coordinate investigations across multiple jurisdictions, frequently resulting in delays while preliminary information is obtained from foreign agencies.[84]

4.79 The Department also drew the Committee's attention to the findings of the European Commission in its *Evaluation Report*, and in particular that, for a range of operational reasons, law enforcement agencies were seven times more likely to require access to IP-based telecommunications data aged more than six months old, compared to telecommunications data relating to mobile telephone services aged more than six months old.[85]

4.80 The Committee also received a supplementary confidential submission from Optus which confirmed that the age-profile of requests for IP-based data is significantly older than for other data types, despite the significant variation in retention practices between Optus services.[86]

4.81 The Uniting Church Justice and International Mission Unit drew the Committee's attention to the Australian Institute of Criminology's findings in a 2009 research paper on the grooming of children online for future sexual exploitation, which highlights the critical importance of access to IP address allocation records for the investigation of this particularly pernicious crime:

> The modern criminal, using the same devices as today's teenagers, communications with Voice over Internet Protocol, video instant messaging, cellular camera phone, and text messaging in

84 Attorney-General's Department, *Submission 27*, p. 31.

85 European Commission, *Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)*, p. 22, referred to in Attorney-General's Department, *Submission 27*, p. 31.

86 Optus, *Submission 86.2*.

> computer slang that is foreign to most police officers and parents. The trail to uncover this valuable investigation resource often starts with a forensic examination, but this trail quickly grows cold as Internet Service Providers overwrite logs and data retention periods expire. All police agencies are facing the same challenge when dealing with computer forensics. Police managers must find a way to examine an increasing number of digital devices, each containing an immense volume of data, in a timely manner and with limited resources.[87]

4.82 The case study of Operation Drakensberg, provided by the AFP, exemplifies the above points. In November 2013, the UK police referred 552 IP addresses suspected of accessing child exploitation material on a UK-based website that was compromised for a short period of time in late 2011 to the AFP for further investigation. The AFP received more than 5 500 referrals for online child exploitation matters from international law enforcement agencies for in 2014,[88]and confirmed to the Committee during a private briefing that the two-year delay in the referral in Operations Drakensberg was the result of ordinary and proper investigative procedures conducted in the UK, and is not uncommon for such international referrals.

4.83 Bravehearts noted that '[f]or child sex offenders advances in on-line technologies are continuing to provide increased opportunities; including for grooming victims, accessing child exploitation material and networking',[89] and supported a two-year retention period 'as a critical tool for supporting the investigation of child sexual exploitation matters'.[90]

Telecommunications data relating to telephony services

4.84 Communications Alliance and the AMTA confirmed that, for telephony services, the Government's proposed data set and two-year retention period would not significantly alter existing industry practice:

> Industry notes that an appropriately defined data set relating to the standard telephone service and a requirement to retain such

87 Kim-Kwang Raymond Choo, *Online child grooming: a literature review of the misuse of social networking sites for growing children for sexual offences*, Australian Institute of Criminology Research and Public Policy Series 103, 2009, p. 82, quoted in Uniting Church in Australia, Justice and International Mission Unit, Synod of Victoria and Tasmania, *Submission 76*, p. 5.

88 AFP, *Submission 7.2*, p. 2.

89 Bravehearts, *Submission 33*, p. 2.

90 Bravehearts, *Submission 33*, p. 4.

> for a period of two years, as requested by agencies and proposed by Government, would be close to current industry practice.[91]

4.85 In evidence to the Committee, Communications Alliance further confirmed that the proposed data retention scheme for the Public Switched Telephone Network (PSTN) (which includes fixed, mobile and satellite telephony networks) 'has zero impact. You have the data anyway'.[92]

4.86 Vodafone also confirmed that it would continue to hold telecommunications data for its telephony services for in excess of two years, irrespective of any new data retention obligations imposed by this Bill.[93]

4.87 NSW Police argued for the retention period for subscriber and telephony data to be extended to six years, to match the existing industry standard set out in the Telecommunications Consumer Protection Code:

> My concern is that, regarding some of the data which I feel is least intrusive, if I can put it that way, and would be of concern, we have the potential to have it for a lesser period of time than we currently do. My submission to the Committee was that we could consider expanding that period or keeping that persion as it was for that data, which would be an extension of what the Bill is currently proposing.[94]

Telecommunications data related to internet-based services

4.88 Communications Alliance and the AMTA submitted that:

> Industry is… far from convinced that a two year retention period for IP-related data is either necessary, justifiable, cost-effective, or in the public interest.[95]

4.89 Communications Alliance gave further evidence on these issues:

> There are storage, maintenance and other costs associated with IP data, which is typically growing at a much faster rate than telephony data; the longer you need to store it the more it is going to cost. Also, there is a general recognition in many of those [EU] jurisdictions that it is the younger data, overwhelmingly, that is

91 Communications Alliance and the AMTA, *Submission 6*, p. 7.

92 Mr Peter Froelich, Industry Member, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2014, p. 39.

93 Mr Lobb, *Committee Hansard,* Canberra, 29 January 2015, p. 64.

94 Assistant Commissioner Lanyon, *Committee Hansard,* Canberra, 30 January 2015, p. 58.

95 Communications Alliance and the AMTA, *Submission 6*, p. 7.

> useful to the pursuit of serious crime and national-security issues.[96]

4.90 However, Communications Alliance and the AMTA also noted that there is a diversity of views within the telecommunications industry about whether a uniform retention period would result in a simpler and cheaper system:

> That said, there is some debate among our members as to whether the potential greater simplicity of having a uniform retention period for all services is outweighed by the expense of and complexities of building to a longer than necessary retention period for non-telephone data.[97]

4.91 Accordingly, Communications Alliance and the AMTA recommended that the Bill be amended to require service providers to retain data for a period 'in the order of 6 months' in conjunction with a provision that 'make[s] it clear that such data can be retained for up to two years without exposing the CSP to a potential breach of the Privacy Act'.[98]

4.92 The Australian Interactive Media Industry Association (AIMIA) Digital Policy Group (DPG), which represents the Australian digital industry and therefore has interests relating primarily to internet-based services, supported Communications Alliance's position,[99] and suggested that the two-year retention period goes 'well beyond what international experience suggests is necessary for effective law enforcement'.[100]

4.93 Communications Alliance argued that the cost to industry of retaining telecommunications data relating to internet-based services is likely to increase exponentially, rather than linearly, beyond a two-year retention period:

> I guess the costs are not strictly incremental but more exponential. In terms of the way that data growth is in the industry at the moment, as you start to blow out the time period from two years to three years, four years, five years or whatever you propose, the volume of data usage on an internet-type service is growing at a factor of 10 times. So you will have those exponential growths on

96 Mr Stanton, *Committee Hansard,* Canberra, 17 December 2014, p. 38.

97 Communications Alliance and the AMTA, *Submission 6*, p. 7.

98 Communications Alliance and the AMTA, *Submission 6*, p. 8.

99 Australian Interactive Media Industry Association (AIMIA) Digital Policy Group, *Submission 34*, p. 3.

100 AIMIA Digital Policy Group, *Submission 34*, p. 3.

> top of the basic incremental growth of the length of time you want to store the data.[101]

4.94 However, Telstra disagreed with the proposition that the retention period would have either a 'significant' or 'exponential' impact on the capital or operational cost of any data retention scheme:

> The costs will change if the prescribed period changes. We have costed to two years. If that were to change, then our costings would change. Will we get substantially different costs? Probably not, because a lot of the capital cost is setting up the systems to extract this data.
>
> …
>
> I am not sure that we necessarily agree on the use of the word 'significant'. It certainly has an impact on cost, because the more data there is then the greater the task to continue to maintain that database, make it accessible and then to interrogate when required. With changes it becomes more complex. So there is a relationship between the retention period and the cost of the scheme. I am not sure that we would go as far as saying it is significant, but it is certainly a factor.[102]

4.95 Mr Chris Berg, Senior Fellow at the Institute for Public affairs, argued that there is a fundamental distinction between the types of telecommunications data associated with traditional telephony services, such as voice calls or SMS, and the internet-based communications covered by the proposed data set, such as VoIP and email:

> [I]nternet activity and telephone activity are not parallels. They operate under substantially different technological paradigms, and they have vastly different social profiles. Where telephone conversations are an adjunct to our lives, internet access is central to it – an enormous amount of interaction with the world is done through the internet. What we do on the internet is part of our private domain to a degree that telephone conversations are not. We live our lives online – to a great degree our work, private lives, our leisure, and our personal and professional relationships are mediated by digital technologies.[103]

4.96 Telstra's submission argued in favour of a single fixed retention period across all technologies and data types. In part, Telstra's position was based

---

101 Mr Froelich, *Committee Hansard,* Canberra, 17 December 2014, p. 35.

102 Mr James Shaw, Director, Government Relations, Telstra, *Committee Hansard,* Canberra, 29 January 2015, pp. 14, 20.

103 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, pp. 4-5.

on the size and complexity of Telstra's own network and service offerings.[104] Telstra also argued strongly that a single retention period would prevent criminals from migrating to alternative services to evade lawful surveillance, and would promote competitive neutrality in a rapidly evolving technological environment:

> [O]bligations should be technologically agnostic to the greatest extent possible. For example, one set of retention obligations should not apply to traditional technologies, such as PSTN or mobile voice and SMS services, while different obligations apply to competing technologies, such as Voice over IP or instant messaging. Not only would asymmetric regulatory obligations put providers of the traditional services at a competitive disadvantage, it would create a perverse incentive from criminals to circumvent scrutiny by the agencies by using the alternative services.[105]

4.97 The Committee notes the findings of the European Commission's Evaluation Report on the Data Retention Directive, that 'internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations',[106] and that EU law enforcement agencies are significantly *more* likely to access internet-related data that is aged more than 12 months compared to other types of telecommunications data.[107]

4.98 The Attorney-General's Department argued that internet-based communications services are similar in functionality, from a user's perspective, to traditional telephony services, and so should be required to retain analogous records.[108]

4.99 The Data Retention Implementation Working Group (IWG) noted that the data set adopts a technologically-neutral approach, and that 'some European nations encountered challenges with the EU Data Retention Directive's technically specific approach, which has inhibited its application to new technologies.'[109] The Attorney-General's Department similarly highlighted the importance of a technologically neutral approach and the importance of drawing on international experience.[110] The

104 Telstra, *Submission 112*, p. 3.

105 Telstra, *Submission 112*, p. 3.

106 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 2011, p. 22.

107 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 2011, p. 22.

108 Attorney-General's Department, *Submission 27*, p. 32.

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

110 Attorney-General's Department, *Submission 27*, p. 25.

Department cited the Netherlands Government's review of its data retention laws, which concluded that:

> It is not quite clear on the basis of which arguments the retention periods for telephone and internet traffic data vary. It is possible that arguments pertaining to privacy issues (in part) underlie this distinction. However, the nature of the internet data stored, effectively doesn't pose a greater infringement on individual privacy when compared to the nature of telephony data.
>
> …
>
> The retention period of six months for internet data is considered unanimously to be too short by the criminal investigations professionals and experts. This is particularly so for complex cases where such data can be useful.[111]

4.100 The IWG industry members noted that 'significant technological change is likely to occur within the Australian telecommunications industry, with potential for significant technological evolution even in the short term.'[112]

Location records

4.101 The Committee received a range of evidence about the privacy sensitivity and utility of location records, which has been discussed above.

4.102 Communications Alliance provided evidence to the Senate Legal and Constitutional Affairs References Committee that location data 'is typically not kept for long periods of time today but would need to be'.[113] The confidential submissions received from service providers indicated that retention practices for location records vary considerably, both between providers and between individual services offered by the same provider, with records not being kept for some services, and being kept for well in excess of two years for others.

4.103 The Attorney-General's Department acknowledged that, 'Arguably, location records are less intimately linked to the remainder of the data set', but that the contextual information that could be provided to other telecommunications data by knowing the location from which a communication was made was particularly important, including to exculpate individuals from suspicion:

---

111 Netherlands Government, *The Dutch Implementation of the Data Retention Directive*, p. 139. The Netherlands Government had implemented laws requiring telephony data to be retained for 12 months, and internet-related data to be retained for six months.

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

113 Mr Stanton, *Committee Hansard,* Senate Legal and Constitutional Affairs References Committee, Canberra, 2 February 2015, p. 9.

> For example, where a suspect makes a phone call immediately after the time a crime was committed, that phone call may appear suspicious. However, location records showing the phone call was made several suburbs from the scene of the crime would tend to remove that person from suspicion.[114]

International comparisons

4.104 The Department provided the Committee with a summary of past and present retention practices across 35 Western countries.[115] Communications Alliance and the AMTA also provided the Committee with a summary of past and present retention practices across 25 Western countries.[116]

4.105 There were a limited number of inconsistencies between the two summaries. In summary, 26 countries previously required or currently require a uniform retention period for both 'traditional' telephony data and internet-based data. Of those countries:

- South Africa specified a 3-year retention period,
- Poland specified a 2-year retention period,
- Latvia specified an eighteen-month retention period,
- twelve specified a twelve-month retention period,[117] and
- eleven specified a 6-month retention period, [118] although the Swiss Government has introduced new laws into its Parliament to increase its retention period to 12 months.

4.106 The remaining nine countries specified different retention periods for different types of telecommunications data:

- two specified a two-year period for fixed and mobile telephony data, and a one-year period for internet access, email and telephony data,[119]
- the United States specified an 18-month period for telephony data, and does not require the retention of internet-based data,

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

115 Attorney-General's Department, *Submission 27*, pp. 38–40.

116 Communications Alliance

117 Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Greece, Spain, France, Portugal, Finland and the United Kingdom.

118 Austria, Cyprus, Germany, Iceland, Liechtenstein, Lithuania, Luxembourg, Romania, Sweden and Switzerland.

119 Ireland and Italy.

- Slovenia specified a 14-month period for fixed and mobile telephony data, and an eight-month period for internet access, email and telephony data,
- Brazil specified a 12-month period for IP connection logs, such as IP address allocation records, a 6-month period for IP access logs, such as web-browsing history, and does not require the retention of telephony data,
- Hungary specified a 12-month period for all telecommunications data, except for unsuccessful call attempts, which are retained for six months,
- two specified a 12-month period for fixed and mobile telephony data, and a six-month period for internet access, email and telephony data,[120] and
- Malta specified a 12-month period for fixed, mobile and internet telephony data, and a six-month period for internet access and email data.

4.107 In summary, 19 out of 34 countries have passed laws requiring the retention of internet-related data for at least 12 months,[121] and six out of 33 countries have implemented different retention periods for telephony and internet-related data.[122]

4.108 The Australian Human Rights Commission argued that the retention periods selected by other countries are 'relevant evidence' for this Committee, but are 'not determinative'.[123]

4.109 The Attorney-General's Department similarly indicated that the proposed data retention regime had drawn on international experience, rather than being identical to regimes in place in Europe.[124]

4.110 As noted above, the Department and Vodafone each drew the Committee's attention to the European Commission's *Evaluation Report*, which discussed the experience of EU nations under the former Data Retention Directive. The Report acknowledges that access to telecommunications data more than six months old is 'less frequent', but argues that access to older data can be 'crucial':

> Firstly, internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations. Analysis

120 The Netherlands and Slovakia.

121 The United States does not require the retention of internet-based data and so has not been counted.

122 The United States does not require the retention of internet-based data, and Brazil does not require the retention of telephony data. As such, these countries have not been counted.

123 Professor Triggs, *Committee Hansard,* Canberra, 29 January 2015, p. 72.

124 Attorney-General's Department, *Submission 27*, p. 25.

> of fixed network and mobile telephony data often generates potential leads which result in further requests for older data. For example, if during an investigation a name has been found on the basis of fixed network or mobile telephony data, investigators may want to identify the Internet Protocol (IP) address this person has been using and may want to identify with whom that person has been in contact over a given period of time using this IP address. In such a scenario, investigators are likely to request data allowing the tracing also of communications with other IP addresses and the identity of the persons who have used those IP addresses.
>
> Secondly, investigations of particularly serious crimes, a series of crimes, organised crime and terrorist incidents tend to rely on older retained data reflecting the length of time taken to plan these offences, to identify patterns of criminal behaviour and relations between accomplices to a crime and to establish criminal intent. Activities connected with complex financial crimes are often only detected after several months. Thirdly, and exceptionally, Member States have requested traffic data held in another Member State, which can usually only release these data with judicial authorisation in response to a letter rogatory issued by a judge in the requesting Member State. This type of mutual legal assistance can be a lengthy process, which explains why some of the requested data was in these cases over six months old.[125]

4.111 The European Commission also identified that, while the majority of requests for access to telecommunications data in the EU were made within a few months or even weeks of the communication taking place, there were four types of criminal investigation for which older data tended to be required, being:

- terrorism and organised crime,
- serious sexual offences,
- substantiating previous intent to commit illegal activities, and
- large cross-border cases.[126]

4.112 The Commission further noted that, the adoption of flat-rate, unlimited use contracts and services had, prior to the introduction of mandatory data retention obligations, significantly impacted the availability of telecommunications data for investigative purposes. The Commission cited the examples of Germany, where the proportion of users with such

125 European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 2011, p. 22.

126 European Commission, *Evidence for necessity of data retention in the EU*, 2013, pp. 4-5.

plans 'rose from 18% in 2005 to 87% in 2009' and noted that it had received advice from both data protection authorities and service providers that data about such services was of 'minimal business value and are only stored in a retrievable form because of mandatory data retention.'[127]

4.113 The Committee notes that major providers have begun offering such unlimited use plans in Australia, but not at the rates observed in Germany.

4.114 As noted above, the Committee's attention was also drawn to the Netherlands Government's review of its data retention laws. The review concluded *inter alia* that a six month retention regime was 'considered unanimously to be too short by the criminal investigations professionals and experts. This is particularly so for complex cases where such data can be useful.'[128] The review also noted that a 12 month retention period was adequate for the majority of cases, but that 'there are cases where for longer term investigations it is insufficient.'[129]

Committee comment

4.115 The length of time for which telecommunications data is retained has direct implications for both the necessity and the proportionality of the scheme.

4.116 Evidence received from ASIO, law enforcement agencies and service providers consistently showed that between 10 and 15 per cent of data authorisations made by Australian agencies are for data which is in excess of one year old. However, these requests disproportionately relate to investigations into serious and complex criminal activity, serious matters of national security (particularly counter-espionage investigations), and other complex cases. Despite constituting only a minority of all access requests, the public interest in the effective resolution of these matters is particularly strong.

4.117 The Committee notes that agencies consider a two year retention period to be a compromise and the minimum amount of time that would be acceptable from a national security and law enforcement perspective.

4.118 The Committee also notes that current retention practices are not uniform across the industry. Some service providers will be required to begin collecting telecommunications data that they do not currently hold for their business purposes. Other providers that do currently collect and retain the data will need to retain it for longer periods. In many cases,

127 European Commission, *Evidence for necessity of data retention in the EU*, 2013, p. 5.

128 Netherlands Government, *The Dutch Implementation of the Data Retention Directive*, p. 139.

129 Netherlands Government, *The Dutch Implementation of the Data Retention Directive*, p. 89.

however, service providers currently collect and retain telecommunications data covered by the proposed data set for well in excess of two years.

4.119 On the basis of the evidence provided, the Committee considers that a two-year retention period is necessary and proportionate. This two-year period would run from the time a particular communication is made, in the case of communications-related data, or from the time an account is closed, in the case of account-holder data.

4.120 The Committee acknowledges that a two-year retention period would place Australia at the upper end of retention periods adopted in other jurisdictions. Of the 35 Western countries identified as having implemented mandatory data retention obligations, only Italy, Ireland, Poland and South Africa require service providers to retain some or all telecommunications data for two years or more. However, the Committee accepts the unequivocal evidence of the national security and law enforcement agencies, which is supported by the international evidence, that a retention period of up to two years is necessary and proportionate for a range of investigations into particularly serious types of criminal and security-relevant activity.

4.121 The Committee received a confidential briefing on the costings from the Attorney-General's Department, which is discussed in greater detail later in this report. The analysis presented to the Committee as part of that briefing showed that reducing the retention period to 12 months would decrease the cost of the scheme by only five to six per cent.[130] Further, varied retention periods for different elements of the data set would risk undermining the efficacy of the scheme as a whole.

4.122 The Committee notes that longer retention periods may aid particular investigations. However, the effective conduct of serious national security and criminal investigations must be balanced against the degree to which a two-year retention period could interfere with the privacy, freedom of expression and other rights of ordinary Australians. For many service providers, a two-year retention period will not represent a substantial change to existing retention practices.

4.123 The Committee notes that the proposed two-year retention period would not impact the ability of service providers to retain telecommunications data for longer than two years for their legitimate business purposes.

130 Attorney-General's Department, *Submission 27.4*, p. 2.

Recommendation 9

The Committee recommends that the two-year retention period specified in section 187C of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be maintained.

4.124 The Committee notes that as a consequence of its earlier recommendation that the data set be contained in primary legislation, there may be some consequential amendments required to section 187C of the Bill that will need to be addressed. These may include consequential amendments to specify the appropriate retention period for different kinds of subscriber data that are covered by proposed new paragraph 187A(2)(a).

Should providers be required to destroy data at the end of the retention period?

4.125 Subsection 187C(3) of the Bill provides that service providers are not precluded from retaining telecommunications data covered by their data retention obligations for longer than two years. The Explanatory Memorandum notes that:

> This means, for example, that service providers will not be prevented by new section 187C from retaining telecommunications data for longer than two years for their own lawful business purposes.
>
> However, the Australian Privacy Principles (APPs), as set out in Schedule 1 of the *Privacy Act 1988* (the Privacy Act), will still apply to service providers and their dealings with the telecommunications data that is personal information and that is required to be retained under the new Part 5-1A of the TIA Act. For example, APP 11.2 requires entities to take reasonable steps to destroy personal information or to ensure that the information is de-identified where the entity no longer needs the information for a reason set out in the APPs. Where the required retention period for telecommunications data under the new Part 5-1A of the TIA Act expires, entities may be required to destroy or de-identify such information if it constitutes personal information.[131]

4.126 The Victorian Commissioner for Privacy and Data Protection noted that the Bill does not require the destruction of telecommunications data at the

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

end of the retention period.[132] This issue was also highlighted by the EU Court of Justice in its decision.[133]

4.127 In its submission, Electronic Frontiers Australia argued that s. 187C(3) of the Bill, which provides that service providers are not precluded from retaining data for longer than the prescribed period, should be removed from the Bill, and that service providers should instead be prohibited from retaining any telecommunications data for longer than two years.[134] However, in evidence to the Committee, Mr Lawrence conceded that 'it may not be of significant harm for [s. 187C(3)] to remain there', after it was pointed out that carriers routinely retain data for longer periods for their business purposes, and that the *Privacy Act 1988* continues to prohibit service providers from retaining data for any longer than required for those business purposes.[135]

Committee comment

4.128 The Committee understands that proposed new subsection 187C(3) is intended to operate as an avoidance of doubt provision. It is not intended to override the existing requirement under APP 11.2 that service providers destroy or de-identify information when it is no longer required for a legitimate purpose.

4.129 The Committee received a range of public and classified evidence from service providers, which is outlined in greater detail above, showing that service providers currently retain a wide range of telecommunications data for longer than the proposed two-year retention period, for their own business purposes and in compliance with other regulatory obligations, such as the Telecommunications Consumer Protection Code. The Committee considers that it is entirely appropriate for service providers to continue retaining such telecommunications data for longer than two years where they have a legitimate business purpose to do so, or in accordance with another regulatory obligation.

4.130 However, the proposed new data retention obligations will require service providers to retain some types of telecommunications data for longer than they otherwise would for their business purposes, or even to begin collecting and retaining particular types of telecommunications data for the first time. In these situations, the Committee is concerned that service providers should not retain such telecommunications data for longer than

132 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 11.

133 *Digital Rights Ireland v Ireland* and *Kärntner Landesregierung* (joined cases C-293/12 and C-594/12), [67].

134 Electronic Frontiers Australia, *Submission 97*, pp. 4-5.

135 Mr Lawrence, *Committee Hansard,* Canberra, 29 January 2015, p. 28.

the proposed two-year retention period without a legitimate business or regulatory purpose.

Recommendation 10

The Committee recommends that the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 clarify the requirements for service providers with regard to the retention, de-identification or destruction of data once the two year retention period has expired

5

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

Application to certain service providers

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

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

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

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

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

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

(b) it is a service:

(i) operated by a carrier; or

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

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

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

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

Application to 'offshore' providers

5.4 The Explanatory Memorandum confirms that data retention obligations:

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition of 'infrastructure'

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Committee comment

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

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

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

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

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

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

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

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

Recommendation 11

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

Committee comment

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

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

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

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

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

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

Recommendation 12

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

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

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

Recommendation 13

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

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

Prescription of additional kinds of service providers in regulations

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

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

> The telecommunications industry is highly innovative and increasingly converged. Sophisticated criminals and persons engaged in activities prejudicial to security are frequently early adopters of communications technologies that they perceive will assist them to evade lawful investigations. As such, a regulation-making power is required to ensure the data retention regime is able to remain up-to-date with rapidly changes to communications technologies, business practices, and law enforcement and national security threat environments.[30]

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

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

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

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

Committee comment

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

Recommendation 14

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

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

Implementation plans, exemptions and variations

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

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

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

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

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

Implementation plans

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

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

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

5.47 The Department added that the process aims to:

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

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

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

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

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

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

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

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

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

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

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

5.52 Optus did, however, put forward the view that

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

Committee Comment

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

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

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

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

Exemptions and variations

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

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

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

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

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

5.71 The Department added that:

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Committee Comment

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

5.85 As noted in the Explanatory Memorandum:

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

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

Recommendation 15

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

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

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

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

Cost of data retention

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

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.105 The Department also advised the Committee that:

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

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

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

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

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

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

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

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

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

Impact on small and medium-sized enterprises

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

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

5.107 Similarly, ACCAN stated that:

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

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

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

---

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

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

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

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

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

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

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

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

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

Government funding for service providers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

112 *Telecommunications Act 1997*, section 314.

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

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

Committee comment

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recommendation 16

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

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

6

Authority to access stored communications and telecommunications data

Introduction

6.1 This chapter addresses Schedule 2 of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill), which contains amendments in respect of restrictions on access to stored communications and telecommunications data.

6.2 The Committee is mindful that a range of other significant issues concerning the adequacy of the existing regime for access to telecommunications data contained in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) were raised in evidence. Given the interdependent nature of the data retention regime and the telecommunications data access regime the Committee also considers those issues in this chapter.

6.3 In its simplest form, the Bill aims to restrict access to data required to be retained under the regime. It proposes to separate the access to different types of information that is authorised for different types of agencies. Namely the Bill proposes that those agencies considered 'criminal law-enforcement agencies' under the provisions set out in the Bill are authorised to access stored communications under warrant.

6.4 Other agencies, which are considered to be 'enforcement agencies' under the provisions set out in the Bill, are to be authorised to access telecommunications data. Criminal law-enforcement agencies would also be considered to be enforcement agencies, and so would have access to telecommunications data.

6.5 This chapter contains the following sections:

- Access to stored communications under warrant for criminal law enforcement agencies
  - ⇒ Which agencies should be able to access stored communications?
  - ⇒ Authorisation process for accessing stored content
- Access to historical telecommunications data for enforcement agencies
  - ⇒ The basis for a telecommunications data access regime
  - ⇒ Which agencies should be able to access historical telecommunications data?
  - ⇒ Authorisation process for accessing historical telecommunications data
  - ⇒ Destruction of accessed telecommunications data.

Access to stored communications

6.6 The following section examines the proposed access and authorisation processes of agencies which are considered criminal law enforcement agencies under the provisions set out in the Bill.

Which agencies should be able to access stored communications?

The current position

6.7 The TIA Act currently provides that stored communications may be accessed by enforcement agencies under a stored communications warrant to investigate a 'serious contravention' of the law.[1]

6.8 Stored communications are distinct from the telecommunications data being considered in respect of the data retention regime. A stored communication is defined in section 5 of the TIA Act:

> stored communication means a communication that:
>
> (a) is not passing over a telecommunications system; and
>
> (b) is held on equipment that is operated by, and is in the possession of, a carrier; and
>
> (c) cannot be accessed on that equipment, by a person who is not a party to the communications, without the assistance of an employee of the carrier.

1 *Telecommunications (Interception and Access) Act 1979* (Cth), Part 3-3.

6.9 Examples of stored communications include emails or SMS messages held by a carrier.[2] Significantly, access to a stored communication will provide access to the content of the communication.

6.10 'Enforcement agency' is defined in section 5 of the TIA Act as:

> (a) the Australian Federal Police; or
>
> (b) a Police Force of a State; or
>
> (c) the Australian Commission for Law Enforcement Integrity; or
>
> (d) the ACC; or
>
> (e) the Crime Commission; or the Independent Commission Against Corruption; or
>
> (f) the Police Integrity Commission; or
>
> (g) the IBAC; or
>
> (h) the Crime and Misconduct Commission; or
>
> (i) the Corruption and Crime Commission; or
>
> (j) the Independent Commissioner Against Corruption; or
>
> (k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph; or
>
> (l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management – Police; or
>
> (m) the CrimTrac Agency; or
>
> (n) any body whose functions include:
>
> (i) administering a law imposing a pecuniary penalty; or
>
> (ii) administering a law relating to the protection of the public revenue.

6.11 In its submission the Attorney-General's Department explains that, for the purposes of paragraph (k), the only authority named in the regulations is the Australian Customs and Border Protection Service.[3] It goes on to state:

> Paragraph (n) of the definition of enforcement agency is broad and includes a wide range of Commonwealth, State, Territory and local government agencies. Examples of agencies that have accessed telecommunications data can be found in Chapter 3 of the TIA Act Annual Report 2012-13.[4]

---

2 Attorney-General's Department, *Submission 27*, p. 43.

3 Attorney-General's Department, *Submission 27*, p. 43.

4 Attorney-General's Department, *Submission 27*, p. 44.

6.12 Australian Security Intelligence Organisation (ASIO) interception warrants also authorise access to stored communications.[5]

Proposed amendment to authority to access stored communications

6.13 The Statement of Compatibility with Human Rights in the Bill's Explanatory Memorandum states:

> The Bill will amend the TIA Act to provide that only criminal law-enforcement agencies are able to access stored communications (and to require the preservation of stored communications). Criminal law-enforcement agencies will be defined to mean:
>
> - interception agencies (Commonwealth , State and Territory police and anti-corruption agencies) that are able to obtain warrants to intercept communications under the TIA Act;
> - the Australian Customs and Border Protection Service (Customs);
> - authorities or bodies declared by the Minister as criminal law-enforcement agencies.[6]

6.14 In its submission, the Attorney-General's Department explained the rationale for the proposed amendment:

> Only agencies that have a demonstrated need to access the content of stored communications, and are subject to appropriate privacy and oversight arrangements, should be eligible to do so. In addition, it should be clear either on the face of the TIA Act or in secondary legislation (such as declarations) which agencies are eligible to apply for stored communications warrants or issue preservation notices.
>
> These amendments also recognise the greater privacy sensitivity of stored communications as compared to telecommunications data. Unlike telecommunications data, stored communications reveal the content and the substance of a person's communications with others. The Bill therefore continues the current division in the TIA Act between criminal-law enforcement agencies and enforcement agencies, with the difference being that under the amendments proposed in the Bill only criminal-law enforcement agencies will be able to access stored communications content.[7]

6.15 In respect of the particular agencies listed as criminal law enforcement agencies the Attorney-General's Department noted that:

5 *Telecommunications (Interception and Access) Act 1979* (Cth), section 109.

6 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 [Data Retention Bill], *Explanatory Memorandum*, p. 9.

7 Attorney-General's Department, *Submission 27*, p. 48.

> in practice only the interception agencies, Customs, the Australian Competition and Consumer Commission (ACCC) and ASIC have obtained stored communications warrants in recent years. The reason for the lower number of agencies obtaining stored communications warrants is that an agency must be investigating a serious contravention (which generally excludes offences punishable by less than three years' imprisonment) in order to apply for a stored communications warrant. This high threshold for obtaining a warrant excludes most enforcement agencies from such access in practice.[8]

Attorney-General's discretion in declaring a criminal law enforcement agency

6.16 A number of submitters endorsed the aim of reducing the range of agencies able to access stored communications but did not agree that the Bill satisfactorily achieved this objective. For example, Professor George Williams and Dr Keiran Hardy of the Gilbert + Tobin Centre of Public Law submitted that:

> as the Bill would allow the Attorney-General to declare other authorities and bodies as criminal law enforcement agencies, uncertainty will remain over who will be able to apply for stored communications warrants. In making such a declaration, the Attorney-General must consider a range of factors, including whether the authority is involved in 'investigating serious contraventions'. This wording suggests that only organisations involved in investigating serious breaches of the criminal law will be declared under the provision. However, it is not a limiting factor. The Attorney-General could declare *any* authority or body as a criminal law enforcement agency, so long as he or she considers the specified range of factors in doing so. In particular, the Attorney-General may consider 'any other matter' that he or she considers relevant. It is therefore possible that agencies involved in enforcing fines and protecting the public revenue – including the Australian Taxation Office, local councils, or bodies responsible for enforcing copyright infringements – could be reinstated with the power to apply for warrants to access stored communications.[9]

6.17 In their submission, Professor Williams and Dr Hardy went on to recommend that:

---

8 Attorney-General's Department, *Submission 27*, p. 47.

9 Professor George Williams AO and Dr Keiran Hardy, Gilbert + Tobin Centre of Public Law, University of New South Wales, *Submission 5*, p. 4.

> To achieve greater clarity in the definition of 'criminal law enforcement agency', and to appropriately limit access to stored communications in line with the government's intended purposes, we believe that the matter listed in the proposed s 110(4)(a) should limit the Attorney-General's declaration-making power. That is, the Attorney-General should only be able to declare an authority or body as a criminal law enforcement agency if he or she is satisfied that the agency is involved in 'investigating serious contraventions'.[10]

6.18 The Australian Privacy Foundation made a similar recommendation in relation to the Attorney-General's declaration making power, though recommended the threshold be raised to 'authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security'. The Foundation added:

> Moreover, in exercising the determination-making power, the APF recommends that the Attorney-General be specifically required to take into account the effect of a determination on the right to privacy.[11]

6.19 The Australian Communications Consumer Action Network (ACCAN) also held the view that agencies added to the list of criminal law enforcement agencies should 'meet the definition of a body investigating serious offences, as defined in the TIA Act'.[12]

6.20 Other submitters were of the view that the Attorney-General's power to make a declaration avoided the proper Parliamentary scrutiny, and that the power should be removed in its entirety. For example the Internet Society of Australia stated:

> Defining such organisations in regulations instead of the primary legislation means additions to the list will not receive parliamentary scrutiny that should be afforded to the granting of these powers.[13]

6.21 The Internet Society went on to propose the following recommendation:

> Amend the Bill to remove the power of the Attorney-General to expand the Bill's existing list of 'enforcement agencies' and 'criminal law-enforcement agencies'. Alternatively, if recommendations are adopted to limit grounds on which access is given, confine the declaration power of the Attorney-General to

10 Professor Williams and Dr Hardy, *Submission 5*, p. 4.

11 Australian Privacy Foundation, *Submission 75*, p. 24.

12 Australian Communications Consumer Action Network (ACCAN), *Submission 120*, p. 10.

13 Internet Society of Australia, *Submission 122*, p. 6.

> those bodies or agencies that are involved in the prevention and/or detection of a 'serious offence' as defined in the [TIA Act].[14]

6.22 The Law Council of Australia expressed the view that

> the Attorney-General's ability to further expand the agencies which can access stored communications or telecommunications data by way of regulation, unacceptably reduces the level of Parliamentary scrutiny of fundamental elements of the Bill,

and recommended:

> The Bill should be amended so that the agencies that may have access to: …
>
> - Stored communications are by way of a list scheduled to the legislation – not via regulation or other legislative or executive instrument.[15]

6.23 The Senate Standing Committee for the Scrutiny of Bills expressed similar concerns with the declaration power, and added:

> If the proposed approach is to be retained, the committee seeks the Attorney-General's advice as to whether the disallowance process can be amended to provide for increased Parliamentary oversight. This committee notes that this could be achieved by:
>
> - requiring the approval of each House of the Parliament before new regulations come into effect (see, for example, s 10B of the Health Insurance Act 1973); or
> - requiring that regulations be tabled in each House of the Parliament for five sitting days before they come into effect (see, for example, s 79 of the Public Governance, Performance and Accountability Act 2013).[16]

6.24 In response to the proposal for limitation of criminal law enforcement agencies to those in the Bill, the Attorney-General's Department stated in its submission:

> The Attorney-General, as First Law Officer, is well placed to consider whether an authority or body should be an enforcement agency (or a criminal law-enforcement agency) …
>
> The ministerial declaration process is the most appropriate method to determine which of the wide range of agencies across Australia should be able to exercise the non-interception TIA Act powers. This is because ministerial declarations afford flexibility to

14 Internet Society of Australia, *Submission 122*, p. 6.

15 Law Council of Australia, Submission 126, pp. 14-15.

16 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 16 of 2014*, p. 6.

> take into account changes made to agency structures and functions. Commonwealth, State and Territory governments regularly change the law enforcement responsibilities of agencies through amendments to administrative arrangements orders and Acts of Parliaments. The speed at which such responsibilities can shift means that the availability of TIA Act powers to a particular body also needs to be both responsive and transparent.[17]

6.25 In response to a question on whether this Committee should be empowered to oversight the Attorney General's declaration making power, Professor George Williams stated:

> It would be a welcome safeguard because it would provide a level of scrutiny that is not otherwise there. Of course, your committee already fulfils similar roles with regard to proscription and other forms of Attorney's decisions. So that would not be inappropriate, but still I think it does not get to the heart of the concern that many people are expressing: that there should be greater clarity about the point of not only which organisations but, as you have indicated, the self-serve nature once declared that they can access the information.[18]

Committee comment

6.26 Given the intrusive nature of warrants that authorise access to stored communications, the Committee considers that the range of agencies able to obtain such warrants needs to be carefully circumscribed to ensure that access to stored communications is limited to agencies with appropriate functions and which are subject to appropriate safeguards.

6.27 The Committee notes the concerns of submitters in respect of the Attorney-General's broad discretion to declare an agency as a criminal law enforcement agency, including agencies which may not have functions in respect of serious contraventions.

6.28 The Committee considers it appropriate for criminal law-enforcement agencies to be listed in the primary legislation. However the Committee accepts that there may be emergency circumstances where a more rapid response is required, and that there is merit in the Attorney-General being able to declare an agency as a criminal law-enforcement agency in such circumstances.

6.29 These declarations should only be made in regard to agencies whose functions include investigating serious contraventions, and such a

17 Attorney-General's Department, *Submission 27*, pp. 48-49.

18 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p.6.

declaration should only be in effect for 40 sittings days of either House of the Parliament. This timeframe enables legislative amendment to be brought before the Parliament and for this Committee to review any proposed amendment to list an agency as a criminal law enforcement agency.

6.30 In regard to the threshold that is to apply for eligibility to be declared a criminal law enforcement agency, the Committee notes the distinction between investigation of a serious offence defined in section 5D of the TIA Act and which applies to interception warrants (broadly, offences punishable by seven years imprisonment or more); and the investigation of a serious contravention, defined in section 5E of the TIA Act, which includes additional offences punishable by 3 years imprisonment or significant fine, and which applies to stored communications warrants. The Committee recognises that there is merit in the view that threshold for agencies which can access telecommunications content under warrant, whether interception or stored communications, should be consistent.

6.31 This Committee previously considered the distinction between the two thresholds in its 2013 report of the *Inquiry into Potential Reforms of Australia's National Security Legislation*. In that inquiry the Committee was not able, upon the evidence before it, to reach a final position about the appropriate threshold for access to telecommunications and stored communication, and recommended the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The Committee reiterates this comment in the context of this inquiry.

6.32 The Committee accepts that, for the purposes of the Bill, the Attorney-General's declaration power should be limited to agencies investigating serious contraventions as defined in section 5E of the TIA Act. The Committee is of the view that the amendments will result in a more appropriate and transparent limitation of agencies than is currently the case. However, the Committee is also of the view that the standardisation of thresholds for agencies to access content of communications should be examined as part of the Government's holistic review of the TIA Act.

6.33 In respect of whether an additional obligation to consider privacy should be included, the Committee notes that the Attorney-General is required under s.110A(4) of the Bill to have regard to whether the declaration would be in the public interest, and also whether the body or authority is required to comply with the Australian Privacy Principles (APPs) or a binding scheme that provides a level of protection of personal information comparable to that provided by the APPs ('a binding scheme'). The Committee also notes Recommendation 8 ii. of the Australian Privacy

Commissioner's submission in which he recommended some additional characteristics which ought to apply to a binding scheme in respect of the declaration of an enforcement agency.[19] The Committee considers those additional characteristics are also appropriate to be applied to consideration of a binding scheme in the context of the Attorney-General's declaration of a criminal law enforcement agency.

Recommendation 17

The Committee recommends that criminal law-enforcement agencies, which are agencies that can obtain a stored communications warrant, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*.

To provide for emergency circumstances, the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as a criminal law-enforcement agency subject to the following conditions:

- **the declaration ceases to have effect after 40 sitting days of either House;**
- **an amendment to specify the authority or body as a criminal law-enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days; and**
- **the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sittings days for review and report.**

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 110A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include investigating serious contraventions.

19 Office of the Australian Information Commissioner, *Submission 92*, p. 7.

Recommendation 18

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or its Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 110A(4)(c)(ii) of the *Telecommunications (Interception and Access) Act 1979* include 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.**

The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements.

Recommendation 19

The Committee recommends that the Attorney-General's Department review whether:

- **the agencies which may access the content of communications (either by way of interception warrants or stored communications warrants) under the *Telecommunications (Interception and Access) Act 1979* should be standardised, and**
- **the Attorney-General's declaration power contained in proposed section 110A of the *Telecommunications (Interception and Access) Act 1979* in respect of criminal law-enforcement agencies should be adjusted accordingly.**

The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by the end of the implementation phase of the data retention regime.

Listing of the Australian Securities & Investments Commission as a criminal law enforcement agency

6.34 The proposed definitions of law enforcement agency and criminal law enforcement agency in the Bill do not include the Australian Securities and Investments Commission (ASIC).

6.35 In its submission ASIC stated:

> ASIC, which currently has the ability to access both types of material for certain law enforcement purposes, is excluded from the proposed definition of 'criminal law enforcement agency', even though it has major criminal law enforcement functions and obligations. Accordingly, ASIC's existing powers in this field will be removed if the TIA Bill is enacted in its current form.[20]

6.36 ASIC explained its role as a major criminal law enforcement agency, its current use of stored communications in proving serious offences, and the accountability requirements that apply:

> ASIC is, among other things, a major criminal law enforcement agency. The types of white collar crime investigated and prosecuted by ASIC are both notoriously difficult to prove and capable of causing immense harm to Australia's financial system. This harm includes damage to the integrity of Australia's financial markets, and devastation to individual victims who risk losing their houses and life savings …
>
> ASIC's express criminal law enforcement functions and obligations extend to the investigation and prosecution of "prescribed offences" and "serious offences", as defined in sections 5(1) and 5D of the TIA Act …
>
> Stored communications are a proven valuable source of intelligence to ASIC and constitute crucial evidence for proving serious offences which ASIC is primarily responsible for investigating and prosecuting. Between 1 July 2008 and 30 June 2013 ASIC sought and obtained 19 such warrants …
>
> Any use of telecommunications data or stored communications obtained by ASIC is strictly restricted by:
>
> - obligations imposed on ASIC under the TIA Act;
> - ASIC's obligation to comply with the *Australian Privacy Principles*, which arises because ASIC is an "APP entity" within the meaning of s 6(1) of the *Privacy Act 1988* (Cth) [the Privacy Act]; and

20 Australian Securities and Investments Commission (ASIC), *Submission 24*, p. 2.

- section 127 of the ASIC Act, which imposes an additional obligation upon ASIC to protect the confidentiality of such information.

ASIC also maintains strict internal procedures to protect privacy and ensure we meet all of our obligations when exercising our powers.[21]

6.37 In response to a question from the Committee on this issue, the Attorney-General's Department stated:

> The list of agencies that are included on the face of the legislation are ones that the parliament has already recognised explicitly has those that should have access to data. They are already included either in the Telecommunications (Interception and Access) Act as it currently stands or in regulations made under it as ones who should have access to telecommunications data. The bill reflects the parliament's existing intention that those agencies have access. All other agencies have the ability to seek a declaration, to the extent that they are agencies involved in the enforcement of the criminal law, protection of public revenue et cetera—those categories that I have mentioned—to enable them to access data. You have given one example, ASIC, but there are a number of agencies that do have functions in the enforcement of the criminal law and protection of public revenue and have used data in the past and consider it to be an important part of the tools that they would use.[22]

6.38 In its submission, ASIC argued that making its power contingent on a ministerial declaration introduced legal uncertainty that is not justified:

> It is possible that if ASIC applied to the Minister to be included in such a declaration it would meet the criteria set out in the TIA Bill. However, there is no certainty that the Minister would make a declaration. If a declaration were made, ASIC considers that it would be a sub-optimal outcome because:
>
> - as the making of a declaration would be a challengeable decision, it would result in some legal uncertainty about the nature and extent of ASIC's powers in this field, which would reduce the efficiency of ASIC's investigations and prosecutions and may encourage legal challenges by alleged offenders;
> - such a declaration may be limited by subject matter or be subject to a sunset provision, or be otherwise subject to

21 ASIC, *Submission 24*, pp. 3, 12, 14.

22 Ms Anna Harmer, Acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 17 December 2014, p. 23.

restrictive or onerous conditions not applicable to analogous agencies included within the statutory definition; and

- even if a declaration were made by the current Minister at the time the Bill became operational that was not limited by subject matter or time, such a declaration would not bind a future Minister and might be revoked or otherwise varied (the Minister could revoke the declaration at any time under proposed subsection 110A(8)).[23]

6.39 In response to this submission, the Attorney-General's Department stated:

> In terms of the specific issue that ASIC raised this morning, as I understand it, they reflected that perhaps a declaration as an agency would put them on a weaker footing than they might currently be at the moment. With respect to ASIC -- and we have had discussions with them on this point—I do not agree that that is the case. In actual fact, a declaration puts them on a stronger footing than is currently the case. ASIC's ability to access data at the moment relies on their ability to fall within that very broadly and non-specifically cast definition of 'enforcement agency', which does not identify them by name; it relies on them falling within that broad class of agencies who are involved in enforcement of the criminal law and related functions. A declaration as an agency would actually give very specific certainty that ASIC is prescribed for the purposes of accessing data. And I think if anything it puts them on a stronger footing rather making them more susceptible to challenge on the basis on which they can access the data.[24]

6.40 Professor George Williams, in response to a question from the Committee about ASIC's submission, stated:

> I will say that personally I was surprised that ASIC was not on that list given its role in investigating quite serious crimes involving what can be significant criminal penalties. It would be much better for the list to be exhaustive and to include the appropriate bodies in the first place. As to adding bodies in the future: certainly challenges could be possible. The minister makes a decision that could be the subject of a variety of legal challenges, and that ultimately might be quite significant in proceedings because, if you can undermine the ability of the body to get the information, perhaps you might even be able to prevent the admission of that information in court proceedings and so prevent a prosecution.

23 ASIC, *Submission 24*, pp. 16-17.

24 Ms Harmer, *Committee Hansard*, Canberra, 30 January 2015, p. 70.

> That said, I think it is actually going to be quite difficult, if all the procedures are followed, to stop appropriate bodies being declared, and that is because, as I indicated in my opening remarks, the key clause is three, and it actually does not set down any criteria.[25]

6.41 The Uniting Church Justice and International Mission Unit submitted that the definition of criminal law enforcement agency should be expanded to include the Australian Taxation Office (ATO) and ASIC:

> The new law will limit access to the information to be kept to criminal law enforcement agencies … and we believe it should be expanded to include the ATO and ASIC so that these agencies do not suffer a reduction in their capacity to fight tax evasion and corporate fraud respectively.[26]

Committee comment

6.42 The Committee recognises the importance of carefully circumscribing the agencies which are designated as 'criminal law enforcement agencies' to ensure that only agencies involved in investigating serious contraventions of the law and subject to appropriate safeguards may seek warrants to access stored communications.

6.43 On the evidence provided, the Committee considers that ASIC is an appropriate agency to be a 'criminal law enforcement agency'. In particular, the Committee notes that ASIC's functions include investigating serious offences; that access to stored communications is, and will continue to be, of assistance in its investigations of serious offences; and that ASIC is subject to appropriate accountability requirements and safeguards including the Australian Privacy Principles.

6.44 The Committee notes from the Telecommunications (Interception and Access) Act 1979 – Annual Report for the year ending 30 June 2013 that the Australian Competition and Consumer Commission (ACCC) has also previously lawfully accessed stored communications. The Committee has received private correspondence from the ACCC noting the importance of the ability to access telecommunications data and stored communications to the performance of its functions and foreshadowing that, if it is not named in the legislation, it will likely seek a declaration as a criminal law-enforcement agency. The Committee considers that the ACCC is also an appropriate agency to be a 'criminal law-enforcement agency'.

---

25 Professor Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 6.

26 Uniting Church in Australia, Justice & International Mission Unit, Synod of Victoria and Tasmania, *Submission 76*, p. 9.

Recommendation 20

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to list the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) as criminal law-enforcement agencies under proposed section 110A of the *Telecommunications (Interception and Access) Act 1979*.

Authorisation process for accessing stored communications

6.45 The Attorney-General's Department explained the current process for accessing stored communications, including the requirement to obtain a stored communications warrant:

> Section 108 of the TIA Act prohibits persons from accessing a stored communication held by a C/CSP, except as provided for in that section (such as access under a warrant).
>
> Section 110 of the TIA Act permits an enforcement agency to apply to an issuing authority (an appointed judicial officer or member of the Administrative Appeals Tribunal) for a stored communications warrant to access stored communications content.
>
> The application can be made in relation to the investigation of a 'serious contravention', which is defined in section 5E of the TIA Act to include (amongst other things) offences punishable by imprisonment by three years or more or contraventions rendering an individual liable to pay a pecuniary penalty of 180 penalty units (currently equivalent to $30,600, on the basis of $170 per penalty unit) or more.
>
> Under section 116 of the TIA Act, an issuing authority may issue a stored communications warrant if the issuing authority is satisfied, amongst other matters, that information likely to be obtained would be likely assist in the investigation of a serious contravention. The issuing authority must also have regard to:
>
> - the impact on any person's privacy;
> - the gravity of the conduct;
> - how much the information would assist in the investigation;
> - whether other methods of investigation would be available or effective.[27]

27 Attorney-General's Department, *Submission 27*, p. 43.

6.46 In its submission, the Australian Privacy Foundation noted that the Bill does not change the threshold for the obtaining of stored communications warrants. The Foundation recommended that the higher 'threshold that applies to real time interceptions – which requires that an investigation should relate to a "serious offence"'[28], should apply to access to stored communications:

> [T}he higher threshold should apply to access to both real-time communications and stored content, and require that such access relate to investigations of serious criminal offences (i.e. offences punishable by imprisonment for at least 7 years, as opposed to the current 3 years applying to stored communications), serious allegations of public corruption, or serious threats to national security. Given the extremely serious privacy implications of access to telecommunications data, the APF further submits that access to such data should be subject to the same thresholds as apply to communications content.[29]

Committee comment

6.47 The Committee notes the distinction between the threshold for an interception warrant being, amongst other things, the investigation of a 'serious offence'; and the threshold for a stored communications warrant being, amongst other things, the investigation of a 'serious contravention'.

6.48 Additionally, the Committee acknowledges the significance of this issue in the context of the current Bill and recognises that there may be some merit in greater consistency in the thresholds for warrants for access to telecommunications content. However, there has been insufficient evidence received to come to a conclusion as to whether, and how, the threshold for a stored communications warrant should be amended.

6.49 Accordingly, the Committee reiterates the recommendation made in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* for an examination of the standardisation of thresholds for accessing the content of communications.[30]

28 Australian Privacy Foundation, *Submission 75*, p. 25.

29 Australian Privacy Foundation, *Submission 75*, p. 25.

30 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, Recommendation 6, p. 30.

Access to historical telecommunications data

6.50 As indicated earlier, the Bill aims to restrict access to data required to be retained under the regime. It proposes to separate the access to different types of information that is authorised for different types of agencies. The previous section has examined the proposed access and authorisation process for agencies that are considered to be criminal law-enforcement agencies under the provisions set out in the Bill. Criminal law-enforcement agencies are authorised to access stored communications under warrant. Criminal law enforcement agencies are also considered to be enforcement agencies.

6.51 The following section examines the proposed access and authorisations processes for agencies which are considered to be 'enforcement agencies' under the provisions set out in the Bill. The Bill proposes that enforcement agencies be authorised to access historical telecommunications data.

The basis for a telecommunications data access regime

6.52 In recognition of the personal and sensitive nature of the information that telecommunications carriers, carriage service providers and related bodies or persons may hold, the *Telecommunications Act 1997* (Telecommunications Act) protects certain information associated with telecommunications.

6.53 The Telecommunications Act provides that carriers, carriage service providers, and certain other persons must protect the confidentiality of information that relates to:

> (a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and
>
> (b) carriage services supplied by carriers and carriage service providers; and
>
> (c) the affairs or personal particulars of other persons.[31]

6.54 The penalty for contravening the relevant confidentiality provisions contained in the Telecommunications Act is imprisonment for up to two years.[32]

6.55 The disclosure or use of protected information is authorised in limited circumstances. Chapter 4 of the TIA Act sets out a regime by which certain agencies can authorise the disclosure of such information or documents—with the important exception that it does not permit the disclosure of the

31 *Telecommunications Act 1997*, section 270 (simplified outline).

32 *Telecommunications Act 1997*, Part 13, Division 2.

contents or substance of a communication.[33] In practice this allows the specified agencies to authorise the disclosure of telecommunications data. Significantly, access is not restricted to the categories of telecommunications data proposed to be retained under the Bill.

6.56 The regime in Chapter 4 of the TIA Act distinguishes between access to existing information or documents (referred to as historical telecommunications data) and access to prospective information or documents that will come into existence during the period for which the relevant authorisation is in force (referred to as prospective telecommunications data).

6.57 Law enforcement and security agency evidence consistently highlighted the critical importance of this access regime to their operations. The Australian Federal Police (AFP) stated in its submission:

> Chapter 4 of the TIA Act currently allows a range of agencies to lawfully access telecommunications data by way of authorised request to domestic communications providers. This telecommunications data has provided information fundamental in enabling the AFP to effectively investigate and prevent crime across the full suite of the AFP's functions including counter terrorism, serious and organised crime, firearm and drug trafficking, child protection operations, cybercrime, crimes against humanity such as slavery, people smuggling and human trafficking, as well as community policing in the ACT and airports …
>
> Access to historical telecommunications data is an elementary building block across the vast majority of AFP investigations into serious crimes. Analysis of AFP investigations commenced in the first quarter of 2014-15 confirms that telecommunications data was used in 92% of Counter Terrorism investigations, 100% of Cybercrime investigations, 87% of Child Protection investigations, and 79% of Serious Organised Crime investigations.[34]

6.58 The Police Federation of Australia stated:

> Access to metadata is an essential policing tool. On one hand it is frequently used to eliminate people from ongoing investigations because the data demonstrates that the person concerned was not, at the relevant time, in the relevant place or did not communicate with the suspect. Thus it narrows the field of suspects.

---

33 *Telecommunications (Interception and Access) Act 1979*, section 172.

34 Australian Federal Police (AFP), *Submission 7.1*, pp. 3, 5.

> On the other hand it assists police to establish people involved in a particular incident, relevant connections between individuals involved, the movement of people at particular times, and the incidence of communications between such people.[35]

6.59 South Australia Police stated at a public hearing:

> Access to metadata plays a central role in almost every criminal investigation, including investigations into murder, sexual assault, drug trafficking and kidnapping. In the offence of murder, the ability to actually identify people who have contacted each other is quite critical. It is the same in cases of child exploitation and, obviously, serious and organised crime matters, where you may have people involved in illicit drug-taking or dealing in drugs.[36]

Which agencies should be able to access telecommunications data?

The current position

6.60 The TIA Act currently provides that ASIO or an 'enforcement agency' may authorise the disclosure of historical telecommunications data. The term 'enforcement agency' is defined in section 5 of the TIA Act.[37]

6.61 The Explanatory Memorandum explains the regime in the following terms:

> Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an 'enforcement agency' to authorise a carrier to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue … There are separate provisions enabling access by ASIO for purposes relevant to security.
>
> Currently under the TIA Act, an enforcement agency is broadly defined as all agencies empowered to intercept telecommunications content as well as bodies whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. The range of agencies that are enforcement agencies and which are capable of authorising the disclosure of telecommunications data is broad and includes Commonwealth,

35 Police Federation of Australia, *Submission 72*, p. 2.

36 Mr Paul Dickson, Assistant Commissioner, South Australia Police, *Committee Hansard*, Canberra, 30 January 2015, p. 42.

37 See also paragraphs 6.7 and 6.8 which set out the definition of 'enforcement agency'.

> State, Territory and local government agencies as well as non-government or quasi-government bodies that carry out relevant functions.[38]

6.62 In the *Telecommunications (Interception and Access) Act 1979* – Annual Report for the year ending 30 June 2013, over 70 agencies were identified as having issued authorisations to historic telecommunications data. In its submission the Attorney-General's Department stated:

> The range of agencies that are enforcement agencies and which authorise the disclosure of telecommunications data is broad and includes local councils, State and Commonwealth government departments, agencies such as Centrelink and bodies as the Royal Society for the Prevention of Cruelty to Animals.[39]

Proposed amendment to 'enforcement agency'

6.63 Schedule 2 of the Bill contains an amendment to the definition of enforcement agency.

> Schedule 2 will amend the existing definition of 'enforcement agency' to limit access to telecommunications data to criminal law-enforcement agencies and authorities or bodies that have been declared by the Minister to be an 'enforcement agency'.[40]

6.64 The Explanatory Memorandum notes these amendments are consistent with Recommendation 5 of the previous Committee's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* that the number of agencies able to access telecommunications data be reduced.[41] That recommendation stated:

> The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.[42]

6.65 In its submission, the Attorney-General's Department explained the effect of the proposed amendment as follows:

---

38 Data Retention Bill, *Explanatory Memorandum*, p. 19.

39 Attorney-General's Department, *Submission 27*, p. 45.

40 Data Retention Bill, *Explanatory Memorandum*, p. 66.

41 Data Retention Bill, *Explanatory Memorandum*, p. 66.

42 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, p. 46.

> New section 176A will create a new definition of 'enforcement agency' to replace the definition of 'enforcement agency' currently found in section 5 of the TIA Act. The new definition of enforcement agency in section 176A will include criminal law-enforcement agencies (as set out in new section 110A) and any authority or body declared by the Attorney-General to be an enforcement agency …
>
> The new definition of enforcement agency replaces the existing open-ended approach of permitting any agency with functions relating to the enforcement of laws administering a pecuniary penalty or protection of the public revenue from automatically having access to the power to authorise the disclosure of telecommunications and seek stored communication warrants …
>
> Agencies that would no longer be 'enforcement agencies' on the face of the legislation include the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO), the Department of Defence (in particular, the Australian Defence Force Investigative Service), the Department of Foreign Affairs and Trade (in particular, the Passports Office), the Department of Immigration and Border Protection, Racing NSW, the Victorian Department of Environment and Primary Industries, the Wyndham City Council, and RSPCA South Australia. [43]

6.66 The Department notes that when making a declaration the Attorney-General is required to consider a number of factors:

> When considering whether to declare an authority or body to be an enforcement agency the Attorney-General will be required to consider:
>
> - whether the authority or body has relevant law enforcement functions;
> - whether the obtaining of historic telecommunications data would assist the authority or body in performing those functions;
> - whether the authority or body is governed by an appropriate privacy regime;
> - whether the authority or body will have processes to comply with its obligations under the TIA Act;
> - whether the declaration would be in the public interest.[44]

6.67 In its submission the Department explained the rationale for the amendment:

43 Attorney-General's Department, *Submission 27*, p. 46.

44 Attorney-General's Department, *Submission 27*, p. 46.

> The principle behind the reduction in the number of agencies that can access telecommunications data is that only agencies that have a demonstrated need to access such information, and are subject to appropriate privacy and oversight arrangements, should be permitted to do so. In addition, it should be clear on the face of either the TIA Act or in delegated instruments (such as declarations) which authorities or bodies are enforcement agencies.[45]

6.68 The Department noted that, in principle, all agencies charged to enforce laws should have access to the necessary tools to carry out their functions, but acknowledged the risk of undermining public confidence in the regime if access is too broad or granted to agencies without appropriate controls in place:

> In principle, any agency or organisation charged by an Australian parliament to enforce laws should have access to the necessary tools to carry out their statutory functions. However, the emerging trend of a wider range of smaller, non-traditional agencies and bodies accessing data without external oversight risks undermining public confidence in the integrity of the regime. In particular, these authorities do not always have internal processes, controls and oversight in place to the same degree as traditional law enforcement agencies.[46]

Attorney-General's discretion in declaring an enforcement agency

6.69 A number of submissions expressed support for the Government's aim of reducing the number of agencies able to access telecommunications data. For example the Australian Human Rights Commission stated in its submission:

> The Commission supports the Bill's proposal to confine the number of agencies that may access retained telecommunications data. The Commission notes that this is consistent with the Court of Justice of the European Union's decision, which states that the number of persons authorised to access and subsequently use the communications data should be limited to that which is strictly necessary.[47]

45 Attorney-General's Department, *Submission 27*, p. 45.

46 Attorney-General's Department, *Submission 27*, p. 42.

47 Australian Human Rights Commission, *Submission 42*, p. 10.

6.70 However, a number of submissions also expressed a concern that the change to the definition of enforcement agency does not satisfactorily limit the range of agencies covered by the definition.

6.71 The Law Institute of Victoria stated in its submission:

> Even more concerning is that the Bill leaves wide open the critical question of what authorities or bodies will be listed as an 'enforcement agency' and therefore be able to access the retained data.
>
> This clause gives the Attorney-General the power to list by legislative instrument any authority or body with functions to enforce criminal law or administer a law imposing a pecuniary penalty or relating to the protection of the public revenue. These functions are incredibly broad and reflect the existing and problematic situation where an unknown number of diverse federal, state and even local government entities currently access telecommunications data.
>
> In this context, it seems unlikely that the Bill will significantly limit the range of agencies permitted to access telecommunications data.[48]

6.72 The Institute recommended that 'the agencies which can access telecommunications data must be exhaustively set out in the legislation'.[49]

6.73 Mr Scott Millwood identified a number of risks with the breadth of the declaration regime:

> Further agencies can be added by Regulation at the discretion of the Government, leaving the data retention regime susceptible to scope and purpose creep …
>
> The wider the scope of access, the greater the risk of a breach – 20 agencies with thousands of personnel with access to highly sensitive data on a massive scale, would send a chill through most Chief Security Officers.
>
> A prudent data system would ensure restricted access to the data pool, by limiting both agencies and personnel who have authorised access.[50]

6.74 The Law Council of Australia noted the range of agencies that could potentially be declared, and stated:

---

48 Law Institute of Victoria, *Submission 117*, pp. 11-12.

49 Law Institute of Victoria, *Submission 117*, p. 11.

50 Mr S Millwood, *Submission 121*, pp. 9-10.

> Vesting such a power in the Minister, notwithstanding disallowance procedures available to parliament, may significantly increase the ambit of the legislation and frustrate the intention of the Parliament. Even if a regulation was in force for a short period of time, this would be sufficient for any number of agencies, not previously authorised by the Parliament, to obtain stored communications data or telecommunications data.…
>
> The Bill should be amended so that the agencies that have access to:
>
> … telecommunications data under the scheme are the agencies:
>
> - that may have access to telecommunications data warrants; and
> - listed in a schedule to the legislation – not in regulation or other legislative or executive instrument.[51]

6.75 The Australian Privacy Commissioner expressed a similar view:

> 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 …[52]

6.76 As noted earlier, in respect to the definition of 'criminal law enforcement agency' the Senate Standing Committee for the Scrutiny of Bills also expressed concerns that the power to include additional enforcement agencies should be in primary legislation rather than by ministerial declaration, and added:

> If the proposed approach is to be retained, the committee seeks the Attorney-General's advice as to whether the disallowance process can be amended to provide for increased Parliamentary oversight. This committee notes that this could be achieved by:
>
> - requiring the approval of each House of the Parliament before new regulations come into effect (see, for example, s 10B of the Health Insurance Act 1973); or
> - requiring that regulations be tabled in each House of the Parliament for five sitting days before they come into effect (see, for example, s 79 of the Public Governance, Performance and Accountability Act 2013).[53]

6.77 The Australian Privacy Commissioner noted the Senate Standing Committee's view, and stated:

---

51 Law Council of Australia, *Submission 126*, p.15.

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

53 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 16 of 2014*, p. 6.

> As an alternative, the 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 be made by an amendment to the TIA Act, I consider that this could offer an alternative approach.[54]

6.78 The Commissioner further expressed the view that, if the declaration power is to be retained, the Minister, when having regard to the matters set out in subsection 176A(4), should also have regard to:

> whether such a binding scheme provide 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.[55]

6.79 In addition, the Commissioner recommended that subsection 176A(5) of the Bill be amended to require the Commissioner to be consulted before making a declaration under subsection 176A(3).[56]

6.80 In response to concerns about the declaration process, the Attorney-General's Department stated in its submission:

> The Attorney-General, as First Law Officer, is well placed to consider whether an authority or body should be an enforcement agency (or a criminal law-enforcement agency) …
>
> The ministerial declaration process is the most appropriate method to determine which of the wide range of agencies across Australia should be able to exercise the non-interception TIA Act powers. This is because ministerial declarations afford flexibility to take into account changes made to agency structures and functions. Commonwealth, State and Territory governments regularly change the law enforcement responsibilities of agencies through amendments to administrative arrangements orders and Acts of Parliaments. The speed at which such responsibilities can shift means that the availability of TIA Act powers to a particular body also needs to be both responsive and transparent.[57]

6.81 The Department also noted that the Attorney-General will have the ability to revoke a declaration and will have the ability to impose conditions, providing 'a further ability to restrict access to telecommunications data in

54 Office of the Australian Information Commissioner, *Submission 92*, p. 23.
55 Office of the Australian Information Commissioner, *Submission 92*, p. 23.
56 Office of the Australian Information Commissioner, *Submission 92*, p. 24.
57 Attorney-General's Department, *Submission 27*, pp. 48-49.

a manner consistent with and proportionate to the functions of the agency'.[58]

6.82 Professor George Williams and Dr Keiran Hardy of the Gilbert + Tobin Centre of Public Law proposed that enforcement agencies should be defined with greater specificity, but identified an alternative in the event that it is not practicable to list all relevant agencies in the legislation:

> If it is not practicable to list all relevant authorities that will have access to metadata, the legislation should at least specify the types of authorities that will have access (such as local council, and authorities responsible for taxation). These categories should be appropriately considered by Parliament as part of the primary legislation. In addition, the power to declare authorities or bodies as enforcement agencies should be limited to those organisations that enforce the criminal law, impose pecuniary penalties or protect the public revenue.[59]

6.83 A number of submitters identified similar concerns with the potential breadth of the range of enforcement agencies, and proposed instead that the Attorney-General's declaration making power should be limited to agencies investigating serious offences or threats to national security. For example, Open Knowledge Australia stated that:

> the range of agencies that could gain access to telecommunications data if the Bill is passed in its current form is, in fact, broader then under the present regime.
>
> Given the extent and sensitive nature of the data likely to be retained, OKFNau urges that the range of enforcement agencies given access to telecommunications data retained under the Bill be limited to those investigating serious criminal offences and activities threatening national security.[60]

6.84 The councils for civil liberties across Australia also expressed their concerns with the breadth of the declaration power, and that some additional clear criteria should be added to the declaration power:

> The issue of who will have access to stored telecommunications data of every internet provider customer in Australia is of great significance in the determination of the proportionality of this intrusion into the privacy rights of persons who are not suspected of any involvement in unlawful activity …

---

58 Attorney-General's Department, *Submission 27*, p. 48.

59 Professor Williams and Dr Hardy, *Submission 5*, p. 5.

60 Open Knowledge Australia, *Submission 110*, p. 4.

> The CCLS recommend that a clearer and tighter definition of types of organisation which can be declared as enforcement agencies be specified in the bill and these be limited to those whose functions include:
>
> - i) enforcement of the criminal law; or administering a law imposing a pecuniary penalty; or administering a law relating to the protection of the public revenue; and
> - ii) some additional clear criteria which would ensure that only agencies dealing with serious crime or serious unlawful actions are included.[61]

6.85 The Australian Privacy Foundation was of the view that a declaration power should be limited to those agencies able to access content:

> [A]ccess to telecommunications data (or metadata) now poses equivalent risks to privacy, and in some instances manifestly greater risks, than access to communications content. Consequently, the APF recommends that there should be no distinction between authorities and bodies entitled to apply for a stored communications warrant and those entitled to access telecommunications data, such that the ability to access such data should be confined to authorities or bodies responsible for investigating serious criminal offences, serious allegations of public corruption, or serious threats to national security.[62]

6.86 In response to a query as to whether any thought had been given to a practical way to put some 'hard markers' in the declaration power to exclude some groups and some functions that are clearly outside the scope of what is intended, the Attorney-General's Department stated:

> The bill, I think, in some respects is intended to do precisely that. It identifies the class of agencies that may have a legitimate need to access data in the performance of their functions. So agencies that are involved in the enforcement of the criminal law, the administration of pecuniary penalties and the protection of public revenue are ones that the parliament has already envisaged through the legislation as it currently stands may be have a need to access data. The bill imposes an additional limitation upon that and says that, rather than your membership of that broad class creating an ability to access data, in addition there should be a requirement that the Attorney-General explicitly consider the extent to which data is required in support of those particular functions, the particular oversight arrangements that apply for an

61 Councils for civil liberties across Australia, *Submission 129*, p. 20.

62 Australian Privacy Foundation, *Submission 75*, p. 24.

> agency that wishes to access data and the extent to which that agency is the subject of binding privacy obligations. So the bill does insert a new mechanism to ensure that it is very clear which agencies are included and to provide key thresholds around that. There will be a clear list of agencies that have access to data, and for those that are not in there it will be clear that they do not.[63]

6.87 When asked by the Committee if there was a situation where a non-government organisation, body, or group, could ever be declared, the Department stated:

> The threshold around who can be declared is one that is defined by reference to the function—so, as I have said, enforcement of the criminal law and/or laws protecting public revenue or imposing a pecuniary penalty. It is typically the case that governments confer those functions upon government agencies however they might be described. We have seen over the operation of the current arrangements that a number of bodies have functions in that regard and, therefore, have had access to the data arrangements. So the precise constitution of a body that would be the subject of a declaration is naturally determined by the extent to which governments confer upon agencies or bodies functions in relation to the enforcement of criminal law. Enforcement of the criminal law is typically regarded as a function of the state, and so, as a general observation, I would say that those functions are conferred on government bodies, but the precise definition that is used in the legislation is around the characterisation of functions of those bodies.[64]

Committee comment

6.88 The Committee welcomes the Attorney-General's reform of the scope of agencies which may access telecommunications data. This measure implements the previous Committee's Recommendation 5 in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

6.89 The Committee recognises that the degree of intrusion into privacy resulting from access to telecommunications data will depend significantly on the type and amount of telecommunications data accessed. The Committee considers that in the context of the modern telecommunications environment, and in particular the proposed data

63 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 23.

64 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 29.

retention regime, there is potential for access to telecommunications data to amount to a very significant intrusion into privacy by an agency.

6.90 The Committee notes the concerns of submitters in respect of the Attorney-General's broad discretion to declare an agency as an 'enforcement agency', including agencies which may not have functions in respect of serious contraventions of the law. In particular, while the Attorney-General is required to have regard to certain matters, his or her discretion to declare an agency an enforcement agency is not otherwise fettered on the face of the legislation.

6.91 For this reason, consistent with proposed measures to safeguard access to stored communications, the Committee considers that those agencies able to access telecommunications data should be listed in the legislation.

6.92 The Committee notes that excluded agencies may be able to access telecommunications data as part of a joint investigation with a listed enforcement agency.[65]

6.93 However the Committee also accepts that there may be emergency circumstances where a more rapid response is required, and that there is merit in the Attorney-General being able to declare an agency as an enforcement agency. In these circumstances, the Committee considers it appropriate to direct the Attorney-General's declaration power to those agencies whose functions include enforcement of the criminal law, administering a law imposing a pecuniary penalty, or administering a law relating to the protection of the public revenue.

6.94 Further, such a declaration should only be in effect for 40 sittings day of either House of the Parliament. This timeframe enables legislative amendment to be brought before the Parliament and for this Committee to review any proposed amendment to list an agency as an enforcement agency.

6.95 While the Committee considers it would be a matter of good practice for the Attorney-General to consult with the Australian Privacy Commissioner and Ombudsman before making a declaration, it is not considered necessary to insert a mandatory consultation requirement for this in the legislation.

6.96 When considering whether an authority or body is required to comply with a binding scheme that provides a level of protection of personal information that is comparable to the level provided by the Australian Privacy Principles, for the purposes of proposed subparagraph 176A(4)(c)(ii), the Committee agrees with the Australian Privacy Commissioner's proposal that regard should also be had to whether such

65 Attorney-General's Department, *Submission 27*, p. 45.

a binding scheme provides mechanisms for monitoring an agency's compliance with the scheme, and enabling individuals to see recourse if personal information is mishandled.

Recommendation 21

The Committee recommends that enforcement agencies, which are agencies authorised to access telecommunications data under internal authorisation, be specifically listed in the *Telecommunications (Interception and Access) Act 1979*.

To provide for emergency circumstances the Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended so that the Attorney-General can declare an authority or body as an enforcement agency subject to the following conditions:

- **the declaration ceases to have effect after 40 sitting days of either House;**
- **an amendment to specify the authority or body as an enforcement agency in legislation should be brought before the Parliament before the expiry of the 40 sitting days; and**
- **the amendment should be referred to the Parliamentary Joint Committee on Intelligence and Security with a minimum of 15 sitting days for review and report.**

Further, consistent with the existing provisions of the Bill, the Attorney-General must have regard to the factors listed in proposed paragraphs 176A(4)(b)-(f), and must also be satisfied on reasonable grounds that the functions of the agency include enforcement of the criminal law, administering a law imposing a pecuniary penalty, or administering a law relating to the protection of the public revenue.

Recommendation 22

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, or the Explanatory Memorandum, or both, be amended to provide that the characteristics of a binding scheme referred to in proposed subparagraph 176A(4)(c)(ii) of the *Telecommunications (Interception and Access) Act 1979* include 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.**

The Committee notes that the Australian Privacy Commissioner currently has these functions in relation to Commonwealth agencies, and some States have privacy commissions which would be well placed to perform these functions within these jurisdictions. Other jurisdictions may need to expand the functions of their existing oversight bodies, or establish new oversight arrangements to meet these requirements.

Access for civil litigation purposes

6.97 Currently, access to telecommunications data is not restricted solely to ASIO and enforcement agencies. Telecommunications data may be lawfully disclosed by telecommunications carriers and carriage service providers to other bodies and persons in specific circumstances as set out in Division 3 of Part 13 of the Telecommunications Act. That Division, amongst other things, makes provision for disclosure where required or authorised by or under law, and by witnesses summoned to give evidence or produce documents.[66]

6.98 A number of submitters expressed concerns, in the context of the data retention scheme, that telecommunications data will be able to be accessed for civil litigation or other purposes not related to law enforcement. For example, the Communications Alliance and Australian Mobile Telecommunications Association (AMTA) raised concerns in respect of the implications of the availability of retained metadata for use in civil proceedings:

> There has been understandable public concern expressed that, once it is clear that increased volumes of metadata are being

66 *Telecommunications Act 1997* (Cth), s.280.

> retained by CSPs for a specified period, these data will become a 'honey-pot' for civil litigants, who may seek court orders to obtain access to metadata for use in civil proceedings. Such actions could stem from Family Law cases and all manner of commercial disputes.
>
> If such a practice were to become commonplace there are serious financial implications to CSPs. Moreover, such a practice would be manifestly outside the intended objectives of a data retention regime, and therefore should be guarded against.[67]

6.99 Communications Alliance elaborated further at a public hearing:

> At the outset, we recognise this may be a difficult issue to tackle, given that civil litigants do have rights to seek discovery for those sorts of data. I guess our concern is that, once it is known—through the requirements of the data set—exactly what data is being retained by each service provider and for how long, that may generate a tsunami of action in commercial disputes, in marital disputes and in many other cases where the data is being mined in circumstances where we may not be able to recover costs for all sorts of purposes that the data retention bill was not designed to facilitate …
>
> Our concern, I guess, is that this is a high-profile exercise and it will put it very clearly in the public consciousness that a defined set of data is available from every service provider, and we think it may start an industry, if you like …[68]

6.100 Mr Alexander Lynch expressed the view that access to telecommunications data without warrant should be limited to national security and serious criminal investigations, and should not be available for civil litigation:

> Metadata should be available without a warrant only for national security investigations and the investigation of serious crimes. Data retention legislation should specify that the metadata being retained is only available to named intelligence, police, border and biosecurity agencies only for those specific purposes, and that it is not legal nor is it the Government's intent that the records be available for other purposes, such as civil litigation.[69]

---

67 Communications Alliance Ltd and Australian Mobile Telecommunications Association (AMTA), *Submission 6*, pp. 14-15.

68 Mr John Stanton, CEO, Communications Alliance, *Committee Hansard*, Canberra, 17 December 2015, p. , Canberra, 17 December 2015, p. 5.

69 Mr Alexander Lynch, *Submission 1*, p. 1.

6.101 Mr Chris Berg of the Institute of Public Affairs also expressed concerns with the availability of telecommunications data for civil proceedings :

> It is also deeply concerning that mandatory data retention will inevitably be a feature of civil litigation. Any information that is created can be accessed by a subpoena with the permission of a court. While many citizens may believe that democratic governments act in their own best interest most of the time, they might not believe the same about their fellow citizens, who they may have to face in future litigation. This has been the experience of other nations with data retention laws. One investigation of Polish data retention laws found that 'more and more often traffic and location data is requested by the parties in civil disputes such as divorce and alimentary disputes.' The prospect of a semi-permanent record of travel data being available for personal litigation is unlikely to be welcomed by Australian voters.[70]

6.102 Mr Iain Muir foreshadowed access of telecommunications data by copyright holders for the purposes of pursuing those in breach of their rights:

> Copyright holders will demand access to these stores of metadata likely pressing down on service providers via threats of litigation. These will be used in turn to self police their intellectual property. Typically done via threats of legal action with pressure to settle out of court for whatever they see fit, mostly from those who can least afford it. Furthermore the victims of such unfair litigation may not have even downloaded the offending file as theft of wi-fi is depressingly common.[71]

6.103 The Australian Privacy Foundation also noted a risk of scope creep in use of the data in both civil and criminal litigation:

> Given the volume of data that will be retained by carriers and ISPs, there will be considerable pressure for such data to be accessed and used for purposes other than law enforcement and national security. In particular, there will be immense pressure for the data to be accessed and used in both civil and criminal legal proceedings by parties who are not authorised to access the data under the TIA Act. In terms of criminal law proceedings, prosecutors will have clear incentives to seek to access data on the basis of speculation alone; while defence lawyers will have incentives to request access to potentially exculpate their clients.

---

70 Mr Chris Berg, Senior Fellow, Institute of Public Affairs, *Submission 94*, p. [6].

71 Mr Iain Muir, *Submission 28*, p. 1.

> And further, Courts may clearly order the disclosure of records wherever relevant across a broad range of cases. In terms of civil litigation, the data exists as a 'honey-pot' for a broad range of actors. Parties to disputes in family law, and in all manner of commercial disputes (involving, for example, trade secrets, intellectual property, and defamation) will likely seek disclosure of retained metadata. For instance, Communications Minister Turnbull and the AFP have announced that data records could be made available for copyright litigation purposes. Claims that the data will not be used by agencies for purposes other than those permitted under the TIA Act are simply disingenuous, as the Bill does not impose any limitations on access to the data by means of other legal avenues, including conventional litigation processes.[72]

6.104 The Law Institute of Victoria, in its supplementary submission, proposed that access should be prohibited otherwise than in accordance with the provisions of the TIA Act:

> The LIV strongly recommends access to telecommunications data should be limited to the purposes of the Bill, i.e. preventing, detecting and prosecuting crime and terrorist activities. As such, access should be prohibited otherwise than in accordance with the provisions of the TIA Act. Such a prohibition should apply to the courts, as well as other persons. Such a provision could be modelled on s 57 of the *Meat Industry Act 1993 (Vic)*.
>
> To ensure that telecommunications providers can still use the data to deliver services, there should also be an exception to the prohibition, which permits telecommunications providers to use and disclose the telecommunications data for business purposes necessary to deliver the telecommunications or internet services.[73]

6.105 Mr Scott Millwood included a similar recommendation in his submission:

> An appropriate amendment would prohibit Service Providers from providing metadata about communications to any third party, except as required to provide their services or as mandated by the Telecommunications (Interception and Access) Act or permitted under the Privacy Act.
>
> This would limit scope and ensure that the concern that metadata might be accessed for other legal processes, including civil litigation, is addressed.

---

72 Australian Privacy Foundation, *Submission 75*, pp. 15–16.

73 Law Institute of Victoria, *Submission 117.1*, p. [9].

> It is also recommended in the interests of transparency, accountability and good governance.[74]

6.106 Telstra noted that it expected to receive an increase in court orders to make customer data available, and recommended that industry be given the ability to recover costs:

> If enacted, the Data Retention Bill would increase the volume of data we are required to retain and is likely to also raise public awareness of this fact. As a result, we expect to receive an increase in the number of court orders we receive to make customer data available to the courts as part of civil litigation proceedings that otherwise does not involve Telstra. These court orders can already be quite resource intensive to comply with today as they often require telecommunications company to interpret data for the courts. Also industry does not have the option of cost recovery on court orders. Telstra recommends that industry be given the ability to recover the costs arising in providing information in response to court orders.[75]

6.107 In its submission Telstra also noted a risk of agencies excluded from the TIA Act regime using other statutory powers to access telecommunications data:

> However, we note that as a result of the proposed amendments to the Telecommunications (Interception and Access) Act 1979, there is now uncertainty as to whether these organisations can revert to using coercive notice to produce or investigatory powers (provided to these bodies under other State or Commonwealth legislation) to access this data. We would recommend additional wording be included in the legislation to ensure there is no back door for these organisations to get access to retained data under other pieces of legislation.[76]

6.108 The Law Council of Australia noted the ability for agencies and other persons to obtain access to telecommunications data under other laws and recommended that access to telecommunications data under other laws or by court process should be precluded:

> The Bill does not limit in any way disclosures of data required to be retained where those disclosures are mandated by laws other than the Bill …

---

74 Mr Scott Millwood, *Submission 121*, p. 15.

75 Telstra, *Submission 112*, p. 5.

76 Telstra, *Submission 112*, p. 4.

> A variety of Federal, State and Territory Acts empower particular agencies to compel disclosure. For example, section 29 of the *Crime Commission Act 2012* (NSW) provides that an executive officer with special legal qualifications may, by notice in writing served on a person require the person to appear before the Commission at a particular time and place and produce to that officer a document or thing specified in the notice, being a document or thing that is relevant to an investigation.
>
> Subpoenas are frequently already issued to third parties by courts, including ISPs, to produce records. Further, parties to prospective or current litigation might seek such retained data as part of the discovery.
>
> In the absence of any restriction upon access to telecommunications data under other Federal, State or Territory laws or court process requiring disclosure of information or documents, there are obvious concerns about the privacy and security of telecommunications data held by authorised collecting agencies. Significant risks include attempting to determine journalists' sources, cases involving alleged infringement of online copyright, family law proceedings, civil claims involving use of machinery or motor vehicles, class actions or other legal proceedings.
>
> The Law Council recommends that access authorised by other Federal, State, or Territory laws, or pursuant to court process should be precluded to ensure that the impact of the Bill is clear and limited to achieving its stated purpose.[77]

6.109 The Law Council of Australia, also noted alternatives in a public hearing:

> Our submission is that the bill should be amended to preclude access. An alternative submission would be that it proscribes access so that access would only be permitted if and where particular access or classes of access were permitted by regulation …
>
> I can envisage that regulations might allow access either by agency, by specified level of court or by class of action.[78]

6.110 In response to a question from this Committee as to whether there may need to be some change in respect of this issue, the Attorney-General's Department stated:

---

77 Law Council of Australia, *Submission 126*, p. 21.

78 Mr Peter Leonard, Chairperson, Media and Communications Committee, Business Law Section, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2015, p. 37.

> It is the case, obviously, that data that is already available and data that will become available in accordance with data retention is available and amenable to other lawful process, including in the civil space whether that be through subpoena or other orders for production. Production in other contexts itself raises a number of challenges and the ability for persons in those proceedings to adduce such evidence as is relevant to their proceedings, and of course it extends into such matters as family law, other commercial situations other than the rights space, which has been the subject of some coverage. It is the case that that data would be available and it has been for some time and is amenable to that process.[79]

6.111 In a supplementary submission the Attorney-General's Department expressed concerns with restricting the availability of telecommunications data so as to prevent its availability for civil litigation:

> Access to telecommunications in civil and administrative proceedings is, and will continue to be important for plaintiffs to protect their interests and rights. Data can be of particular importance where civil proceedings are closely linked to a criminal matter. Proceedings where data may be relevant include proceeds of crime actions, civil child protection investigations, apprehended violence orders and actions involving incidents of stalking and harassment, which often involve the use of a carriage service. In the Department's view, there is a strong public interest in telecommunications data continuing to be accessible to plaintiffs.
>
> … Limiting or restricting access to telecommunications data in court proceedings may also give rise to constitutional risks relating to the separation of powers by limiting the scope of judicial discretion to obtain the information necessary to assist the court in exercising its judicial function.[80]

Committee comment

6.112 The Committee notes that telecommunications data is currently accessed under existing laws by persons or entities other than law enforcement and national security agencies using exceptions to the prohibition on disclosure contained in Division 3 of Part 13 of the Telecommunications Act. The Committee considers that the majority of these exceptions, for example in respect of emergency management, or the business needs of service providers, should continue to apply.

79 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 22.

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

6.113 However, the Committee holds concerns in respect of a possible increase in the frequency and volume of telecommunications data accessed by civil litigants as a result of the implementation of the proposed data retention regime, and has paid careful heed to suggestions that such access be restricted.

6.114 The Committee is aware of the potential for unintended consequences resulting from a prohibition on courts authorising access to data retained under the data retention scheme. The potential for possible interference with judicial power was also raised in evidence.

6.115 Nonetheless, the Committee considers that the proposed data retention regime is being established specifically for law enforcement and national security purposes and that as a general principle it would be inappropriate for the data retained under that regime to be drawn upon as a new source of evidence in civil disputes.

6.116 The Committee considers that the Bill should be amended to include a prohibition on civil litigant access to telecommunications data retained for the purpose of complying with the mandatory data retention regime. The Committee considers that this prohibition should only apply in respect of data retained solely for the purposes of the data retention regime. It should not apply more broadly to telecommunications data retained for other purposes, such as data that is currently retained for the business needs of the service provider.

6.117 The Committee considers that the amendment should include a regulation making power to enable provision for appropriate exclusions, such as family law proceedings relating to violence or international child abduction cases, and that the Minister for Communications and Attorney-General review this measure.

6.118 The Committee does not wish to prescribe how a regulatory power would work when it comes to what should be excluded. This will be a matter that will have to be reviewed and further considered by the Attorney-General.

Recommendation 23

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime.

To enable appropriate exceptions to this prohibition the Committee recommends that a regulation making power be included.

Further, the Committee recommends that the Minister for Communications and the Attorney-General review this measure and report to the Parliament on the findings of that review by the end of the implementation phase of the Bill.

Personal access

6.119 In its submission, the Law Council of Australia highlighted the importance of individuals being able to seek access to their own telecommunications data:

> An exception should be provided for individuals seeking to access their own telecommunications data. This may be essential, for example, in a criminal trial where an individual believes that telecommunications data may establish their innocence. If government agencies are able to access the telecommunications data of individuals to establish a prosecution, the Law Council considers that it is also appropriate for individual's to access such data to be able to establish a defence, or to understand the evidence and charges against them.[81]

6.120 The Pirate Party Australia expressed that there was some uncertainty as to whether users would be able to access telecommunications data they have generated.

> It is unclear whether provision will be made for subscribers and users to inspect or otherwise gain access to the retained data they and people using their accounts have generated. Under the Privacy Act 1988 companies have a general obligation to allow individuals to inspect and correct personal data that they hold. However, journalist Ben Grubb was (and appears to remain) engaged in a dispute with Telstra over a request for their personal telecommunications data. This issue ought to be resolved, and

81 Law Council of Australia, *Submission 126*, p. 21.

> preferably individuals would be permitted to inspect the records held.[82]

6.121 Telecommunications industry representatives raised concerns in their submissions in respect of the costs of personal access by customers to telecommunications data stored as part of the data retention regime.

6.122 The Communications Alliance and AMTA proposed that it should be explicit that carriers and carriage service providers are not required to provide individuals access on demand to all retained data, while reinforcing their right to access to their stored personal information:

> The Bill does not explicitly address the question of whether individuals should have the right under Australian Privacy Principle 12, to make demands upon CSPs to provide access to their personal metadata, especially the metadata captured by the mandatory data retention scheme …
>
> The size and cost of the task for a CSP to pull together and make available all the metadata relating to an individual should not be underestimated. The prospect of potentially millions of Australians making such requests to CSPs is little short of frightening. Such a scenario would generate enormous expense and resource demands on CSPs, for no clear or positive outcome. CSPs would need to create purpose-built security and management systems to meet the additional demands imposed on them by this new requirement.
>
> The Associations stress that we are not advocating any restriction on customer access to the Personal Information stored by CSPs about their customers – data such as billing information, address and identification details. This information should continue to be freely available to customers …[83]

6.123 When asked at a public hearing for comment on this concern, the Attorney-General's Department stated:

> There are a couple of things we can provide some preliminary comments on, at this stage. As Communications Alliance has probably flagged, there are arrangements under which people can access their own personal information. The Privacy Act provides a mechanism for individuals to request their own personal information. What is 'personal information' depends on the circumstances, but it is information that reasonably leads to the identification of a particular individual. What that is will depend

82 Pirate Party Australia, *Submission 124*, p. 12.

83 Communications Alliance and AMTA, *Submission 6*, p. [15].

> on the circumstances and will depend on what the information is, the circumstances in which it is received and how access is arranged. Particularly in the telecommunications context, that can vary according to network configurations—whether a particular data point is one that identifies an individual. Nevertheless, it is the case that, to the extent that carriers have personal information, individuals may apply to those carriers and request their personal information. Indeed, industry is entitled to recover the reasonable cost and is entitled to charge for the provision of personal information under that Privacy Act framework.[84]

6.124 In his submission, the Australian Privacy Commissioner provided a detailed response to the concerns expressed by the Communications Alliance and AMTA:

> 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). 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.
>
> 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 …[85]

6.125 In its submission, Telstra identified the potential for an increased regulatory burden imposed by the Privacy Act in respect of retained data:

> If compliance with the Bill increases the amount of personally identifiable information we hold about our customers, then it will increase the regulatory burden imposed on industry by the Privacy Act …

---

84 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014, p. 30.

85 Office of the Australian Information Commissioner, *Submission 92*, pp 36-37.

> On top of our obligation under the Privacy Act to protect against data breaches, the manner in which the data will need to be held to comply with the Bill may mean that Telstra could be required to make this data available to individual customers in response to an access request for personal information.[86]

6.126 Telstra noted in such a case that additional costs will be incurred, and that such costs may not be able to be fully recovered by charging customers for providing access to personal information:

> Providing this information to customers is not the same as providing information to authorised enforcement agencies and would involve additional costs, for example in verifying a customer's identity and redacting information on incoming calls to protect the privacy of other individuals. There is a fundamental difference between responding to a reasonably precise and limited request from agencies for information to dealing with blanket requests for all personal information about an individual.
>
> The costs associated with the systems, processes and labour, required to verify customer requests and retrieve the relevant data, has not been taken into account by Telstra in determining the cost impacts of the Data Retention Bill. Telstra does have the ability to charge customers for providing access to personal information, but we consider it a real risk that we would not be able to fully recover our costs in light of the Office of the Australian Information Commissioner's (OAIC) Australian Privacy Principles Guidelines on charging for access requests.[87]

Committee comment

6.127 In regards to personal access, the Committee notes Australian Privacy Principle 12 but considers that individuals should have an unambiguous right to access their personal telecommunications data retained under the mandatory data retention regime. The Committee recommends amendments to the Bill to clarify the right to access personal data retained under the data retention regime.

6.128 The Committee notes that telecommunications service providers are currently able to recover the cost under the *Privacy Act 1988* and considers that this model should apply to these arrangements.

---

86 Telstra, *Submission 112*, pp. 4-5.

87 Telstra, *Submission 112*, p. 5.

Recommendation 24

The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to make clear that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime. Telecommunications service providers should be able to recover their costs in providing such access, consistent with the model applying under the Privacy Act in respect of giving access to personal information.

Authorisation process for accessing historical telecommunications data

6.129 At a public hearing, the Attorney-General's Department confirmed that the Government does not intend to amend the existing authorisation process in the Bill:

> **MR DREYFUS**: …This bill—and if you can confirm—is not dealing in any way with the powers that there presently are for ASIO, the Australian Federal Police or other police forces to access telecommunications information. Is that right?
>
> **Ms Harmer**: The only amendment to the access arrangements is to reduce the number of agencies who can access the data, but the access thresholds are not changed.[88]

6.130 However, the Committee notes that a significant number of submissions have raised concerns with the adequacy of the existing authorisation process or expressed the view that additional safeguards are necessary in light of the proposed data retention regime.

6.131 The remainder of this chapter will examine the following issues raised in evidence in the context of the proposed data retention regime:

- whether a warrant issued by an independent body (or similar process) should be required to authorise access to telecommunications data;
- whether the statutory thresholds for access to historic telecommunications data should be adjusted;
- whether additional requirements for access should apply in respect of privileged or other sensitive communications;

88 The Hon Mr Dreyfus QC MP and Ms Anna Harmer, acting First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 17 December 2014, p. 8.

- whether additional requirements in respect of destruction of telecommunications data in the possession of agencies are required.

The current position

6.132 The Explanatory Memorandum provides an overview of the process for obtaining access to historical telecommunications data:

> The TIA Act establishes a process of authorisation for access to telecommunications data that requires senior management to authorise access to this data before it is disclosed to an agency. The authorisation process requires the authorised officer to consider the need for access to this information on a case-by-case basis in accordance with a prescriptive legal framework.[89]

6.133 In its submission, the Attorney-General's Department provided further detail on which officers may authorise disclosure under the existing internal authorisation process:

> 'Authorised officers' of enforcement agencies may authorise the disclosure of telecommunications data under the TIA Act. Authorised officer are defined in section 5 of the TIA Act to include the following:
>
> - i. the head of an enforcement agency; or
> - ii. a deputy head of an enforcement agency; or
> - iii. a person who holds an office or position in the enforcement agency that is covered by an authorisation in force under subsection 5AB(1).
>
> Under section 5AB of the TIA Act, an agency head may authorise, in writing, management offices or positions within their agency for the purposes of authorising access to telecommunications data.[90]

6.134 The Department also described the legislative thresholds that apply when officers of an organisation are considering telecommunications data access authorisations:

> Chapter 4 of the TIA Act sets out the mechanisms for ASIO and the enforcement agencies to authorise the disclosure of data for a variety of lawful purposes.
>
> Section 178 of the TIA Act allows an authorised officer of an enforcement agency to authorise a C/CSP to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of the criminal law …

89 Data Retention Bill, *Explanatory Memorandum*, p. 19.

90 Attorney-General's Department, Submission 27, p. 42.

> Section 178A of the TIA Act allows an authorised officer of a police force to authorise a C/CSP to disclose historic telecommunications data to assist in locating a missing person.
>
> Section 179 of the TIA Act allows an enforcement agency to authorise a C/CSP to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of law imposing a pecuniary penalty or for the protection of the public revenue …
>
> For all of the above disclosure authorisation powers, section 180F of the TIA Act requires an authorised officer to take the privacy impact into account when making any such authorisation.[91]

6.135 The authorisation process for ASIO is similar. The Director-General of Security, a Deputy Director-General of Security, or an approved ASIO officer may authorise access to historical telecommunications data where they are satisfied that the disclosure would be in connection with the performance by ASIO of its functions.[92]

6.136 In response to a request from this Committee to outline how the process of access works, the New South Wales Police Force (NSW Police) explained:

> All of our inspectors and above—we call them commissioned officers—…
>
> They are all authorised under the act—I think it is section 5AB. They are authorised officers to approve metadata requests under section 178 of the TIA act. They are in the field, say, at a particular location. Someone puts the request up to the inspector. They call in the boss. They discuss it—a particular crime has just been committed or is about to be committed—and there is a process in place. There will be discussion. There is a cost involved too. The constable or the detective will need to talk to the boss to make sure that everyone is happy, and costs will obviously be paid for the metadata. They look at the privacy aspects of the particular crime and the safeguards. There is a process on the computer called our 'I Ask' system. They log in online. They put down a narrative of the brief and so on. It goes through to the 'I Ask' system at Parramatta where it is approved. That system then talks to the carrier's system and it is vetted by 'I Ask', which is done by another inspector. There is more supervision and vetting, and the data is obtained from the carrier. At the local level, the inspector will approve that particular request. They will look at all the

91 Attorney-General's Department, Submission 27, p. 42.

92 *Telecommunications (Interception and Access) Act 1979*, section 175.

> safeguards, facts and circumstances to justify the request, and so on. It goes to 'I Ask'. There is another vetting process at 'I Ask', and then the carrier accesses the records back to the officer who requested the data under the process.…
>
> It is standardised, accounted, documented, recorded …[93]

Should a warrant from an independent authority be required?

6.137 A significant number of submitters have expressed the view that there is a need for an increase in procedural protections in respect of agency access to telecommunications data.

6.138 For example, in their submission, Professor Geroge Williams and Dr Keiran Hardy raised the following concern:

> We are concerned by the prospect that enforcement agencies will effectively be able to access metadata on a 'self-serve' basis. Given that metadata can reveal a significant amount of identifying information about an individual, we believe that greater procedural protections for accessing metadata should apply….
>
> This could be achieved through a warrant process along the lines of that allowing access to stored communications.…
>
> Metadata is not trivial information and enforcement agencies should not be free to access that information wherever doing so is reasonably necessary to enforce minor infringements, such as parking or library fines.[94]

6.139 The councils for civil liberties across Australia highlighted that, without prior oversight, any abuse of the legal parameters could only be detected after the fact. The councils argued the necessity of judicial oversight prior to access:

> The CCLS greatest concern about the proposed safeguards is the lack of prior oversight of the operation of enforcement agencies access to telecommunications meta-data …
>
> It is clearly unacceptable for the 'enforcement agencies' or ASIO to be their own authorisers of access to such personal information. Any oversight of their processes and detection of any abuse of the legal parameters could only be detected post hoc.
>
> There is an obvious and well tested, traditional safeguard that should be included in the bill. Access to both retrospective and prospective meta-data under the proposed scheme should only be

93 Detective Superintendent Arthur Kopsias, APM, Telecommunications Interception Branch, New South Wales Police Force, *Committee Hansard*, Canberra, 30 January 2015, pp. 58-59.

94 Professor Williams and Dr Hardy, *Submission 5*, p. 5-6.

> on the basis of a prior warrant authorisation from a judicial authority.[95]

6.140 The Committee notes that the Parliamentary Joint Committee on Human Rights also recommended use of a warrant:

> [T]he committee notes that the proposed oversight mechanisms in the bill are directed at reviewing access powers after they have been exercised. However, the statement of compatibility does not address the question of why access to metadata under the scheme should not be subject to prior review though a warrant system, as is the case for access to other forms of information under the TIA Act.
>
> The committee considers that requirements for prior review would more effectively ensure that the grant of access to metadata under the scheme would be consistent with the right to privacy.
>
> The committee therefore recommends that, so as to avoid the unnecessary limitation on the right to privacy that would result from a failure to provide for prior review, the bill be amended to provide that access to retained data be granted only on the basis of a warrant approved by a court or independent administrative tribunal, taking into account the necessity of access for the purpose of preventing or detecting serious crime and defined objective grounds.[96]

6.141 A number of submitters expressed their support for the Parliamentary Human Rights Committee recommendation. Blueprint for Free Speech recommended that any access to telecommunications data should be supported by a warrant on the terms set out by that Committee.[97] The Law Institute of Victoria noted the Human Rights Committee's recommendation and expressed the view that judicial oversight should be required. Mr Josh O'Callaghan referred to the Committee's recommendation and highlighted the protection warrants provide:

> I also have an issue with current system we have; which allows the warrantless access (without judicial oversight; under any circumstance) of the existing telecommunications networks.…
>
> By removing the process to obtain warrants, citizens are losing their right for judicial protection against corruption and abuse.[98]

---

95 Councils for civil liberties across Australia, Submission 129, pp. 15-16.

96 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, p. 18.

97 Blueprint for Free Speech, *Submission 54*, p. 14.

98 Mr Josh O'Callaghan, *Submission 29*, p. 1.

6.142 The Australian Human Rights Commission recommended in its submission that an independent authorisation system by a court or administrative body be implemented. As with a number of other submitters, the Commission noted that access to telecommunications data may not be any less intrusive than access to content:

> The current regime allows agencies to access communications data without a warrant but mandates a warrant for access to the content of communications. The Commission considers that a warrant system is necessary for the access to communications data as well. This is especially the case given the question of whether the distinction between content and communications data for the purposes of the right to privacy can be legitimately maintained …
>
> Contrary to the claims made in the Explanatory Memorandum, the Commission considers the retention of and access to communications data may not be any less intrusive than retention of and access to content. The requirement to store communications data on each and every customer just in case that data is needed for law enforcement purposes is a significant intrusion on the right to privacy and justifies a warrant system for access to it.[99]

6.143 The Commission also referred to international precedent for use of warrants to access telecommunications data:

> The Commission notes that the Court of Justice of the European Union considered that an independent administrative or judicial body should make decisions regarding access to the retained communications data on the basis of what is strictly necessary …
>
> Further, requiring a warrant to access metadata is not without precedent in other countries. In the EU, eleven Member States require judicial authorisation for each request for access to retained data. In three Member States judicial authorisation is required in most cases. Four other Member States require authorisation from a senior authority but not a judge.[100]

6.144 In its submission, the Commission noted the safeguards that apply under the existing legislation and the Bill, but expressed the concern that they only apply after a power has been exercised.

> While these safeguards are important checks on the scheme, they are all directed at reviewing access powers after they have been exercised. The Commission considers that a warrant or authorisation system for access to retained data by a court or

99 Australian Human Rights Commission, *Submission 42*, p. 11.

100 Australian Human Rights Commission, *Submission 42*, pp. 10-11.

> administrative body provides a more effective safeguard to ensure that the right to privacy is only limited where strictly necessary.[101]

6.145 Australian Lawyers for Human Rights explained why, in its view, a warrant to access telecommunications data is necessary:

> Today, warrants should be required to access metadata so that (1) individuals may not be investigated by government bodies without proper cause, and so that (2) an appropriate check or balance is applied through the mechanism by which the warrant is obtained from the courts.
>
> To remove the requirement for prior authorisation via a warrant is to undermine both democracy and the rule of law by reducing the checks and balances essential to a democratic system.[102]

6.146 The Human Rights Law Centre expressed the view that a warrant or other prior approval process is necessary, and also expressed the need for a notification and review mechanism:

> A warrant or other similar prior approval process is necessary to ensure that issues of privacy are considered by an independent authority and that there is sufficient evidence to avoid a fishing expedition …
>
> The absence of a warrant or other independent authorisation process prior to access and use of the stored data gives rise to serious concerns regarding the propriety, and apparent propriety, of the access and use …
>
> A warrant or similar prior approval process should also provide a mechanism for individuals to be notified and have the opportunity to challenge the legality of access to their telecommunications data. Notification could occur after access where ex parte approval was necessary for law enforcement or national security purposes. This process should mitigate the concern that the right to an effective remedy is being impermissibly interfered with because individuals are unable to challenge decisions or applications in relation to their stored metadata because they are never informed of the decisions or applications.[103]

6.147 The Parliamentary Human Rights Committee similarly recommended a requirement for individuals to be notified that their data has been subject

---

101 Australian Human Rights Commission, *Submission 42*, p. 12.

102 Australian Lawyers for Human Rights, *Submission 88*, p. 7.

103 Human Rights Law Centre, *Submission 71*, p. 8.

to an application for authorisation to access, and recommended a process to allow individuals to challenge such access.[104]

6.148 Mr Scott Millwood strongly advocated for the use of a targeted warrant system for accessing telecommunications data:

> While oversight provisions are a welcome inclusion in the Bill, an oversight function by the Commonwealth Ombudsman is not comparable with the meaningful judicial oversight provided by the targeted warrant system. This submission recommends that serious consideration be given to ensuring access to metadata is governed by a warrant system, in which judicial consideration can be given to the requirements of necessity and proportionality. This would simultaneously address the requirement of a legal avenue for remedy for victims of violations of their rights to privacy under the data retention regime.[105]

6.149 Mr Millwood also noted the risk of telecommunications data being used for political purposes, a concern that was reflected in a number of submissions to this inquiry:

> The hard truth is, systems of mass surveillance are inevitably used to target political opposition. It is conceivable that use or misuse of an individual's metadata could cause great damage to an individual's right to freedom of expression and right to participate in Australian public life.[106]

6.150 Guardian Australia similarly expressed its concerns with the lack of a pre-disclosure independent oversight mechanism for access to telecommunications data, and also proposed the use of a public interest monitor in such a process:

> Guardian Australia submits that it is reasonable for the public to expect that authorisation from an independent, appropriately qualified person ought to be required before metadata is accessed. Independent authorisation is such a commonly occurring feature of the safeguards used by democratic societies in the context of surveillance schemes that the Committee is requested to investigate further, to test seriously the agencies' claims about cost in time and money, and to recommend an appropriate process for independent authorisation prior to access.
>
> … The Committee is requested to recommend the creation of an independent Public Interest Monitor role. A suitably qualified and

104 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, p. 21.

105 Mr Millwood, *Submission 121*, p. 14

106 Mr Millwood, *Submission 121*, p. 16.

> experienced person should have the primary function of testing the arguments of agencies which seek to conduct surveillance and of articulating the privacy and others interests which ought to be weighed by the decision-maker.[107]

6.151 The Australian Privacy Foundation and the councils for civil liberties across Australia also expressed support for a public interest monitor in the context of a warrant or similar process.[108]

6.152 In response to suggestions that a warrant regime should be used, law enforcement and security agencies noted the existing protections and safeguards that apply and raised significant concerns in respect of the impact such a requirement would have on their operations.

6.153 The AFP explained its concerns with a warrant requirement to access telecommunications data in its submission:

> The AFP considers that, given the existing safeguards, constraints and processes governing the authorisation regime, and the extended oversight provisions under the Bill, that a warrant scheme for access to telecommunications data would not significantly improve accountability or transparency of the scheme. Rather, the AFP considers that such a scheme would generate unnecessary administrative burden and costs on both agencies seeking access to telecommunications data and on the issuing authority for such warrants.
>
> 32. The AFP is concerned that the time (not even counting the financial cost) required per request to prepare and progress a warrant for telecommunications data would reduce operational responsiveness in time sensitive cases and create a bureaucratic burden, diverting investigative resources from the field. The AFP conservatively estimates, based on other warrant applications that the process for preparing such a warrant would take at least 8 hours of dedicated work. Extending this to the existing rate of requests for telecommunications data, this would equate to a requirement for over 100 staff to be solely committed to warrant preparation duties.
>
> 33. A scheme requiring agencies to obtain a warrant for historical telecommunications data would also create a significant additional burden on the already stretched Administrative Appeals Tribunal and judicial system, who would be required to consider

107 Guardian Australia, *Submission 132*, pp. 12-13.

108 Australian Privacy Foundation, *Submission 75*, p. 3; Councils for civil liberties across Australia, *Submission 129*, p. 16.

> approximately 25,000 applications from the AFP alone every year.[109]

6.154 In its submission, ASIO explained its concerns with a warrant mechanism, and also noted the extensive safeguards that currently apply:

> ASIO's concern with implementing a warrant regime for data access is its impact on our operational response and agility: the significant bureaucratic overlay such a scheme would impose and the consequential delay in assessing and responding to emerging security threats before they are realised.[110]

6.155 At public hearing, representatives of New South Wales, South Australia and Victoria police forces explained to the Committee how metadata is used and the impact a warrant process could have on their operations. South Australia Police stated:

> Metadata is really just about where the communication occurred, when it occurred, place, time—those sorts of issues. As you quite rightly say, it does not actually relate to the content of that metadata. Often, when we seek that metadata, we are just looking for information because we do not really have much else to go on. We are using that information tool to find out what contact, what communication, the suspects or the victim have had and to then go and speak to those individuals to find out what is the relationship and just going through that process, as any good investigator should do. Really it is an intelligence tool to provide us with information to assist us with that investigation. Often the metadata does not get us anywhere because it is not relative to the investigation.[111]

6.156 The NSW Police noted the impact a warrant regime could have:

> [T]he first 24 hours in a homicide investigation is critical, a significant time delay to go under a warrant regime would significantly impact on both the effectiveness and certainly the efficiency of criminal investigations …
>
> I would say the balance at the moment is quite appropriate in terms of metadata. As I said, internally there are checkpoints that we need to go through to get there. There is external oversight—and I can have Superintendent Kopsias talk in terms of the telecommunications interception act and Ombudsman, Commonwealth and state, oversighting. In the initial stages of an

109 AFP, *Submission 7.1*, pp. 12-13.

110 Australian Security Intelligence Organisation, *Submission 12.1*, p. 48.

111 Assistant Commissioner Dickson, *Committee Hansard*, Canberra, 30 January 2015, p. 45.

> investigation, it is really about gathering information as quickly as we can so we can try to narrow down suspects, try to identify communications and found the investigation and the direction we are going to go with it. If a significant layer of bureaucracy is put on top of that, that will significantly impede investigations. I would think that they are appropriate, and I certainly take note of Mr Byrne's comments before. But when you look at the significant number of inquiries that are made for metadata each year and the way that they are handled compared to the response we do get from both the state and Commonwealth Ombudsman, I think we have the processes very appropriate.[112]

6.157 NSW Police added this further comment on the potential impact of a warrant regime:

> From a New South Wales Police Force prospective, the volume of our metadata requests if we put a warrant regime on top of the metadata scheme would—I will make a bold statement—virtually cripple our organisational capacity to effectively deal with organised crime and serious crime. I would make that statement to you. It is not just responding during business hours; it is also after hours. We respond to kidnappings and other serious crime after hours and on weekends. You would need after-hours people to do that type of work. Just the sheer volume of metadata and TI requests would hamper our investigative capacity.
>
> In terms of oversight, I do not think a warrant scheme would add more to due diligence and to the accountability and oversight process currently in place at the moment. As Mr Lanyon told you, we have enough internal processes and accountability schemes in place to ensure governance and equitable practices are adhered to at all times in compliance with the legislative practices that we adhere to.[113]

6.158 Victoria Police added:

> [I]f we were to move to a judicial warrant situation for metadata, one of the things I think it would throw up in terms of an anomaly is that telecommunications interception warrants, by definition, require metadata within the applications—and quite a deal of metadata—to substantiate the application. We would effectively be moving to a situation where, in a lot of instances, we would

112 Assistant Commissioner Malcolm Lanyon APM, New South Wales Police Force, *Committee Hansard*, Canberra, 30 January 2015, pp. 46, 47.

113 Detective Superintendent Arthur Kopsias APM, New South Wales Police Force, p. 47.

> need a warrant to obtain the information that we would need to obtain the warrant. I think that would raise a whole range of issues as well.[114]

6.159 A number of submitters did not accept agency concerns regarding the impact of a warrant requirement on the ability to perform their functions. The councils for civil liberties across Australia submitted:

> The CCLS do not accept the argument that having to access a warrant will impose an unmanageable administrative burden on the agencies or ASIO. The warrant process provides an important procedural safeguard without any great inconvenience. Such inconvenience and administrative burden that does accompany it, is a reasonable and necessary trade-off for such significant intrusion into the privacy rights of the community.[115]

6.160 The Law Council of Australia acknowledged that an increase in warrant applications would result, but considered that this would cause agencies to only apply for access in cases when an interference with privacy was considered necessary:

> The Law Council understands that there are concerns that a warrant-based system would limit the ability of law enforcement and national security agencies to employ what is often the lowest risk, least resource-intensive and least intrusive investigative tool. The Law Council does not agree that the method of access to retained communications should be the paramount consideration. Rather, protection and oversight of rights of privacy should be paramount …
>
> The Law Council acknowledges that a warrant-based system for access to telecommunications data would increase the number of warrant applications. However, it would serve as an important deterrent for agencies to only apply for access when an interference with privacy is considered necessary.
>
> The Law Council rejects the argument that, even if accompanied by increased resourcing, a warrant regime would distort the ability of issuing authorities to perform their day-to-day functions as members of the judiciary or AAT. This is an issue of adequate resourcing of the Courts and the AAT. The government has a responsibility to sufficiently resource those bodies charged with supervision of such activities to ensure that rights of privacy are not unnecessarily infringed upon.

---

114 Inspector Gavin Segrave, Victoria Police, *Committee Hansard*, Canberra, 30 January 2015, p. 49.

115 Councils for civil liberties across Australia, *Submission 129*, p. 16.

6.161 In response, the Attorney-General's Department provided a number of reasons why it did not consider a warrant regime appropriate:

> The benefits of introducing a warrant regime would be outweighed by the impact on agencies' ability to combat serious crime and protect public safety. Timely access to telecommunications data can provide agencies with vital leads before evidence can be lost or destroyed. However, warrant applications are resource intensive, and can take days, if not weeks, to prepare and complete. Delaying an agency's ability to begin an investigation by this length of time would seriously harm their ability to investigate crimes or threats to national security.
>
> Telecommunications data is used most commonly in the early stages of an investigation, when evidence is at risk of being lost, or where victims might be in imminent risk of danger. For example, a police force investigating a suspected kidnapping would often begin their investigation by seeking information about whom the victim had been communicating with immediately prior to their kidnapping. Early information about the whereabouts of the victim would increase the chances of a successful rescue.
>
> Warrants are also typically reserved for the most intrusive powers, such as the power to enter a home, intercept phone calls, or access stored communications. Many information-gathering powers that are exercised by agencies under Commonwealth, State and Territory laws do not rise to that level of intrusiveness and may be exercised without a warrant. Examples of such powers are powers to obtain banking, financial and healthcare records. The power to access data is only of the same level of intrusiveness as these powers. Non-warranted access to information is a normal part of any law enforcement framework.
>
> Furthermore, to require a warrant in this circumstance would be counterintuitive to the fundamental tenet of proportionality because telecommunications data serves to establish the case for more intrusive powers to be deployed under a warrant.

6.162 The Attorney-General's Department also noted that precedent for non-warranted access to information is found in a number of areas within the existing Australian legal system:

> [W]hile there are warrants for access to some types of information and tools, warrants are typically reserved for those tools that are most intrusive. The committee has already commented today on telecommunications interception warrants, but there are a range of other warrants for more intrusive steps—search warrants et cetera.

> However, access under alternative mechanisms is certainly by no means unprecedented. Indeed, it is common through 'notice to produce' authorisation processes et cetera to access more routine ranges of information that are less intrusive. Telecommunications data, as we said, is a basic data point. It is typically used at the beginning of investigations to commence inquiries, to identify inquiries and to pursue those. It is a relatively less intrusive range of information. It is also often required to progress investigations quickly and to provide the information that is then required to support something like an interception warrant. So it then supports warranted access to other tools.[116]

6.163 Professor Williams and Dr Hardy acknowledged the significant administrative burden of a judicial warrant process and proposed a ministerial warrant process as an alternative.

> We accept that a warrant process along these lines could pose a significant administrative burden to law enforcement and intelligence agencies investigating serious criminal offences and threats to national security. As such, a preferable alternative might be to implement a ministerial warrant process. This could be incorporated into existing ministerial warrant processes where available to ensure maximum efficiency without compromising procedural safeguards …
>
> A ministerial warrant process would allow law enforcement and intelligence agencies to access metadata in a timely fashion whilst ensuring that there is enhanced political accountability for the regime.[117]

6.164 Appearing before the Committee, Professor Gillian Triggs, President of the Australian Human Rights Commission, acknowledged the issues with the imposition of a warrant process and suggested some more nuanced administrative process should be adopted:

> We suggest that some form of administrative—possibly judicial but for practical purposes administrative—body be developed in advance of the access or collection process so that there is some form of control … If it is accepted that a warrant is necessary for content, I think it at least has to be further explored why it is not necessary to have a warrant at the beginning of the process.
>
> Again, I am conscious of the concerns that the warrant process can be time consuming, expensive and difficult to establish, and that is

116 Ms Harmer, *Committee Hansard*, Canberra, 17 December 2014.

117 Professor Williams and Dr Hardy, *Submission 5*, p. 6.

> very important when we are dealing with critical questions of life and serious criminal offences. So we would suggest that, rather than going necessarily through a warrant process, some more nuanced process of administrative authorisation be adopted which is simpler, clearer and cleaner …[118]

6.165 The Attorney-General's Department referred to the use of generic warrants in some European jurisdictions, but noted the United Kingdom's Interception of Communications Commissioner's concerns in respect of how proportionality can be judged properly under such schemes, and expressed concern that use of a generic warrant may result in important checks being removed:

> The Australian scheme is comparable to that which exists in the UK where a disclosure of information to be sought individually which allows the proportionality of each particular disclosure to be considered separately. This is required by section 180F of the TIA Act, which provides that authorising officers must have regard to whether any interference in the privacy of any person or persons that may result from a particular disclosure is justifiable, having regard to the likely relevance and usefulness of the information and the reason why the disclosure or use is proposed to be authorised.
>
> Those considerations are important checks that would possibly be lost from the investigative process if 'generic' whole-of-investigation warrants were to be adopted. The checks may be lost as the issuing authority would be required to decide whether or not to authorise disclosure of information without knowing the relevance of particular pieces of information to an investigation or the privacy impact of any such disclosures.
>
> The Department's view is that the current law and policy settings in the TIA Act are preferable, as they require the person authorising the disclosure of this basic investigative material to turn their mind to privacy and proportionality considerations when deciding whether or not to authorise particular disclosures.[119]

6.166 The Australian Privacy Commissioner had considered a 'generic' warrant and concluded in his submission that it would not be effective:

---

118 Professor Gillian Triggs, President, Australian Human Rights Commission, *Committee Hansard*, Canberra, 29 January, p. 71.

119 Attorney-General's Department, *Submission 27*, p. 19.

> 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. 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.[120]

6.167 In a supplementary submission, the Commissioner also considered the issue of additional safeguards that might be introduced for the use of telecommunications data for more minor crimes. The Commissioner proposed three alternatives, the first being the introduction of a warrant, and the second being a more restricted warrant regime applying in relation to minor offences:

> An alternative to introducing a blanket warrant requirement, could be an amendment to Chapter 4 of the TIA Act to require enforcement agencies to obtain a warrant where access to telecommunications data is sought in relation to the investigation of an offence other than a 'serious contravention', as defined in s 5E of that Act.
>
> While the requirement to obtain a warrant in relation to minor offences may appear counterintuitive, such an approach would recognise the urgency of requests for telecommunications data necessary for the investigation of serious offences and threats to national security. This is also in-keeping with the intention of the proposed data retention scheme, which has focused on the need to ensure that Australian enforcement and security agencies have access to the information they require to combat such serious offences and threats.[121]

6.168 The third alternative suggested by the Commissioner was amending section 180F of the TIA Act to require authorised officers to have regard to additional factors:

> [T]he Bill could amend s 180F of the TIA Act to explicitly require an authorised officer to have regard to the following additional factors:
>
> - the seriousness of the offence,

120 Office of the Australian Information Commissioner, *Submission 92*, p. 20.

121 Office of the Australian Information Commissioner, *Submission 92.1*, p. 3.

- whether there are any other reasonable methods of investigating the offence, that do not involve the use of telecommunications data, available to the enforcement agency, and
- the likely impact on the community of the enforcement agency not being able to access the relevant telecommunications data.[122]

6.169 During a public hearing, the Committee asked Professor George Williams and Dr Keiran Hardy whether the Single Point of Contact (SPoC) mechanism, as used in the United Kingdom, would be a useful safeguard to include in the Data Retention Bill. In a supplementary submission, Professor Williams and Dr Hardy outlined the scheme and expressed the view that it would not resolve issues of external oversight.

> A SPoC is an accredited individual (or group of individuals) in a public authority who acts as a 'gatekeeper' before requests for communications data are submitted to a senior authorising officer.
>
> For example, if a junior police officer wanted to access communications data under Part 1, Chapter 2 of the Regulation of Investigatory Powers Act 2000 (UK), he or she would first submit an application to the SPoC. The SPoC would then consider the merits and lawfulness of that request, and provide advice on its drafting, before sending it to a senior designated officer to be authorised.
>
> We believe that such a scheme could be a useful addition to the Bill currently before the Committee, but it would not resolve the Bill's major issues. A SPoC regime would not add any external oversight or political accountability to the proposed data retention regime, as it would operate internally within enforcement agencies and criminal law enforcement agencies. It would also not resolve other key issues raised by the Bill, such as whether local councils should have access to metadata for the purpose of enforcing fines and the like. We believe that the government should focus on resolving these key issues in the primary legislation.[123]

Committee comment

6.170 A number of submitters raised concerns regarding the authorisation process for access to telecommunications data. In particular some submitters argued that access to telecommunications data is no less

122 Office of the Australian Information Commissioner, *Submission 92.1*, pp. 3-4.

123

intrusive than access to the content of telecommunications, and consequently that the same pre-access approval processes should apply.

6.171 The Committee acknowledges that in some circumstances access to telecommunications data can represent a significant privacy intrusion. However, the Committee notes the evidence provided that telecommunications data and telecommunications content are not used in the same way by law enforcement and security agencies, and does not consider that the same authorisation processes must necessarily apply. However the Committee has paid particular attention to assessing the adequacy of existing safeguards and oversight mechanisms for authorisation of access to telecommunications data.

6.172 The formulation of safeguard and oversight mechanisms in this context requires a careful balancing of competing public interests – maximising accountability, integrity and protection of liberty while minimising adverse impacts on both the ability and the agility of agencies to perform their legitimate functions of enforcing the law and safeguarding the Australian community.

6.173 During the conduct of this inquiry, the Committee has received compelling evidence that the introduction of a warrant process (judicial or ministerial) for access to telecommunications data would significantly impede the operational effectiveness of agencies and that this would be to the detriment of the protection of the Australian community. The Committee was not convinced that a 'generic' warrant would be a suitable alternative.

6.174 After close consideration of the evidence, the Committee concludes that the existing internal authorisation regime contained in the TIA Act is appropriate, noting the other safeguards and oversight mechanisms that apply.

Thresholds for authorising access to telecommunications data

6.175 Some submitters raised concerns that the threshold for authorising access to telecommunications data is not proportionate to the level of privacy intrusion that may arise under the regime. Some proposed that the thresholds for agencies to access telecommunications data should be amended to include a requirement as to the gravity of the offence/security matter being investigated. For example, the Australian Privacy Foundation stated in its submission that it considers there is a strong case for applying the current threshold for accessing content to agency access to telecommunications data:

> Given the extent to which access to telecommunications data my interfere with the right to privacy just as much as access to

> communications content, the APF consider there is a strong case for introducing a uniformly high threshold for access to both communications content and telecommunications data.[124]

6.176 The Law Institute of Victoria recommended that access to telecommunications data be restricted to criminal law enforcement agencies for preventing, detecting or prosecuting serious crimes. In reaching this conclusion the Institute stated:

> This Bill does not refer to 'serious crime'. There are no criteria which would ensure that data is only accessed or used for purposes of prevention, detecting or prosecuting serious crime or even matters that constitute criminal offences. The Bill goes beyond a legitimate purpose. The agencies that can be classified as 'enforcement agencies' can access data related to their function of enforcing offences that impose pecuniary penalties and/or protect public revenue.[125]

6.177 The Australian Human Rights Commission noted the Court of Justice decision in respect of the EU Data Retention Directive, and concluded that access to historical telecommunications data should be limited to sufficiently serious crimes:

> As outlined above, the Court of Justice of the European Union found that the EU Data Retention Directive was not a proportionate interference with the right to privacy. One of the reasons for this was that it considered that access and use of the data should be restricted to the prevention, detection or prosecution of defined, sufficiently serious crimes.
>
> The Commission considers that access to communications data should be restricted to sufficiently serious crimes to warrant the intrusion on the right to privacy.[126]

6.178 The Parliamentary Joint Committee on Human Rights, in its review of the Bill, recommended changes to the existing authorisation scheme to address concerns in respect of the existing threshold for access to telecommunications data:

> The lack of a threshold, relating to the nature and seriousness of the offence, for access to retained data appears to be a disproportionate limitation on the right to privacy. The committee considers that to ensure a proportionate limitation on the right to privacy, an appropriate threshold should be established to restrict

124 Australian Privacy Foundation, *Submission 75*, pp. 24-25.

125 Law Institute of Victoria, *Submission 117*, p. 12.

126 Australian Human Rights Commission, *Submission 42*, p. 9.

> access to retained data to investigations of specified threatened or actual crimes that are serious, or to categories of serious crimes such as major indictable offences (as is the current threshold for requiring the option of trial by jury). The committee is additionally concerned that the threshold of 'reasonably necessary' for the enforcement of offences may lack the requisite degree of precision.
>
> The committee therefore recommends that the bill, so as to avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of any offence, be amended to limit disclosure authorisation for existing data to where it is 'necessary' for the investigation of specified serious crimes, or categories of serious crimes.[127]

6.179 A number of submitters to this inquiry support the Parliamentary Human Rights Committee's recommendation. For example, the Victorian Commissioner for Privacy and Data Protection stated:

> The Bill should be amended to include clearly defined objective thresholds for access to retained data by criminal law enforcement agencies. These thresholds should be set taking into account the public interest, including consideration of the principles of proportionality, necessity, effectiveness, and transparency. Access should only be available in relation to serious offences, for example, offences that attract significant periods of imprisonment. The PJCHR recommendation to limit disclosure authorisation for existing data to where it is necessary for the investigation of specified serious crimes, or categories of serious crimes is supported.[128]

6.180 The Human Rights Law Centre noted the Human Rights Committee's recommendation and added:

> The failure to set out objective criteria restricting access and use of data for the purpose of preventing and detecting carefully defined serious offences or of conducting criminal prosecutions was one of the key criticisms levelled at the Directive in the Digital Rights decision.
>
> The same criticism was raised in Germany in relation to legislation intended to implement the Directive into German law. The legislation was found to be disproportionate and unconstitutional, in part because the stored data could be accessed for a wide

127 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, p. 16.

128 Commissioner for Privacy and Data Protection (Victoria), *Submission 39*, p. 7.

> variety of purposes, rather than strictly for the investigation of serious crimes.
>
> The Bill should establish a gravity threshold so that retained metadata can be accessed and used only where it is necessary for investigating serious crimes; not minor or trivial offences.[129]

6.181 The Muslim Legal Network (NSW) expressed the view that access to data should be restricted to investigations of terrorism related offences only:

> [W]e strongly believe that not only should the type of enforcement agencies that can access retained data be restricted, but the purpose of accessing the retained data should be limited to the investigations of terrorism related offences only. The overriding rationale of data retention, if it is to be accepted into Australian law, should be one of targeted surveillance and not mass surveillance. Mass surveillance is ineffective, disproportionate and a woefully inadequate response to the threat of terrorism.[130]

6.182 In its submission the Attorney-General's Department highlighted the importance of access to telecommunications data for all investigations, serious or otherwise:

> Telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, and almost any activity prejudicial to security that has been facilitated, enabled or carried out via communications technology. For online investigations, telecommunications data is, in many cases, the primary form of information used by law enforcement agencies to identify, investigate, prevent and prosecute these serious crimes and threats to national security. It is used in almost all national security investigations conducted by the Australian Security Intelligence Organisation (ASIO), including almost all counter-terrorism, espionage and intelligence investigations, and all cyber-security investigations.
>
> Telecommunications data can provide important leads for agencies, including evidence:
>
> - of connections and relationships between persons of interest
> - of suspects' movements and behaviours
> - of events immediately before and after a crime, and
> - to exclude people from suspicion.
>
> Telecommunications data is also foundational information required as a necessary precondition to more intrusive

129 Human Rights Law Centre, *Submission 71*, p. 10.

130 Muslim Legal Network (NSW), *Submission 198*, p. 10.

> investigative tools such as access to stored communications and telecommunications interception. Conversely, it is always desirable to rule innocent parties out from suspicion as early as possible, both to prevent any unnecessary intrusion on their privacy, and to ensure that scarce investigative resources are used efficiently. While all investigative techniques involve some degree of intrusion, the use of telecommunications data is one of the least privacy intrusive investigative tools available to agencies.[131]

6.183 The Department noted restricting access to 'serious crime' would have 'an unquantified impact on the investigation of crime types that agencies' currently have the capabilities to investigate'.[132]

6.184 The Department also explained its view that introduction of a threshold for access to telecommunications data based on the seriousness or gravity of an offence would be in contravention of the Cybercrime Convention:

> As a party to the Council of Europe Convention on Cybercrime, Australia has international obligations to make access to telecommunications data available for the investigation of all criminal offences. Article 14(2) of the Cybercrime Convention requires parties to ensure that telecommunications data is available for the investigation of any criminal offence, not just serious offences. Accordingly, amendments that reduce the number of agencies that have access to telecommunications data based on the gravity of the conduct in question would contravene Australia's obligations under the Convention. However, Australia's obligations under the Cybercrime Convention do not preclude reducing the range of agencies that have access to data, because Australia's obligations under the Cybercrime Convention relate only to the availability of telecommunications data for all offences, without specifying the range of agencies which must have access to such data.[133]

6.185 At a public hearing the Australian Privacy Commissioner noted that in his submission he had proposed that the Bill be amended to limit the purposes for which telecommunications data can be used and disclosed to the investigation of serious crime and threats to national security. However, the Commissioner went on to revise his position, noting the Attorney-General's Departments advice in respect of the application of the Cybercrime Convention:

---

131 Attorney-General's Department, *Submission 27*, p. 5.

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

133 Attorney-General's Department, *Submission 27*, p. 42.

> [S]ince lodging that submission, I note that the Attorney-General's Department has suggested that to meet Australia's obligations under the Council of Europe's cybercrime convention access to telecommunications data cannot be limited in this way. If that is the case then I consider that further thought needs to be given to what additional safeguards might be put in place when access is for the purpose of the investigation of minor offences.[134]

6.186 Subsequent to the hearing, the Commissioner provided a supplementary submission in which he set out a number of suggestions for additional safeguards that might be put in place. This included implementation of a warrant regime, or amending section 180F of the TIA Act to require an authorised officer to have regard to the seriousness of the offence and the likely impact on the community of the enforcement agency not being able to access telecommunications data for the investigation of that offence.[135]

Committee comment

6.187 The Committee has considered very carefully the views expressed that telecommunications access should be limited to sufficiently serious matters, such as serious contraventions of the law or serious national security issues.

6.188 The Committee notes that the level of intrusion into privacy incurred by accessing telecommunications data will vary depending on the particular circumstances, including the nature and volume of the telecommunications data accessed. The Committee also notes the complexities in balancing the competing public interests of individual privacy with enforcement of the law and protection of national security.

6.189 On balance, the Committee considers that the requirement in section 180F should be replaced with a more stringent requirement for the authorising officer to be satisfied on reasonable grounds that the particular disclosure or use of telecommunications data being proposed is proportionate to the intrusion into privacy.

6.190 In making this decision, the authorising officer should have regard to a list of specified factors, including the gravity of the conduct being investigated, the reason why the disclosure is proposed to be authorised, and the likely relevance and usefulness of the information to the investigation.

---

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

135 Office of the Australian Information Commissioner, *Submission 92.1*, pp. 1-4.

6.191 A similar requirement should apply in respect of authorisations made by ASIO officers. The Committee notes that this could be achieved by appropriate amendments to the mandatory guidelines issued to ASIO by the Attorney-General.

6.192 The Committee also considers that enhanced accountability and oversight in respect of agencies' authorisation powers are necessary to provide reassurance to the Parliament and the community, and has addressed this further in Chapter 7.

Recommendation 25

The Committee recommends that section 180F of the *Telecommunications (Interception and Access) Act 1979* be replaced with a requirement that, before making an authorisation under Division 4 or 4A of Part 4-1 of the Act, the authorised officer making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate.

In making this decision the authorised officer should be required to have regard to:

- **the gravity of the conduct being investigated, including whether the investigation relates to a serious criminal offence, the enforcement of a serious pecuniary penalty, the protection of the public revenue at a sufficiently serious level or the location of missing persons;**
- **the reason why the disclosure is proposed to be authorised; and**
- **the likely relevance and usefulness of the information or documents to the investigation.**

Protection of client legal privilege and journalist sources

6.193 A number of submitters expressed significant concerns with agencies accessing privileged or otherwise sensitive telecommunications data.

6.194 The Law Institute of Victoria raised concerns that the Bill lacks safeguards to protect confidential and privileged information:

> The Bill contains no safeguards to protect confidential and privileged information, such as communications subject to client legal privilege, health records and journalists' sources. The lack of

such safeguards was one of the flaws highlighted by the CJEU in assessing the EU Data Retention Directive:

> *… it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.*

As illustrated above, telecommunications data is capable of revealing substantial information, and this could include information about communications between a lawyer and their client. For example, information exchanged by email or calls about potential witnesses between the lawyer and associates of the client, experts or other relevant parties, could disclose a defence case. A litigation strategy or case theory could be identified based on witnesses or experts contacted by the lawyer.

The Bill should contain specific safeguards to prevent disclosure of potentially privileged and confidential information. This issue could be taken into account as part of the warrant process and may in appropriate circumstances give an individual an opportunity to challenge access on the basis of privilege.

6.195 Mr Brian Ridgway noted his concern with the lack of an exception for professional privilege:

> The Bill makes no provision for the exception of professional privilege so that metadata associated with:
>
> - lawyers and their clients
> - doctors and their patients
> - journalists and their contacts
> - Members of Parliament and their correspondents
>
> will be able to be collected, accessed and analysed along with everything else.[136]

6.196 The Law Council of Australia noted that:

> although telecommunications data alone may not reveal the content or substance of lawyer/client communications, it would, at the very least, be able to provide an indication of whether:
>
> - a lawyer has been contacted;
> - the identity and location of the lawyer;
> - the identity and location of witnesses;
> - the number of communications and type of communications between a lawyer and a client, witnesses and the duration of these communications.[137]

136 Mr Brian Ridgway, *Submission 20*, p. 4.

137 Law Council of Australia, *Submission 126*, p. 20.

6.197 The Council emphasised the fundamental importance of client legal privilege, and concluded that:

> where access to retained data is sought relating to a lawyer's communications, it is essential that agencies seeking access demonstrate how privileged and confidential communications will be protected before a warrant can be issued and that sanctions for non-compliance be included.[138]

6.198 The Council also expressed the view that the scheme's application to other relationships whose communications are subject to the obligation of professional confidentiality regimes needs to be reconsidered, and made two recommendations in respect of privileged or sensitive data:

- Where access to retained data is sought for persons with legal obligations of professional confidentiality, there should be a requirement for agencies seeking access to demonstrate how privileged and confidential communications will be protected before a warrant can be issued.
- The TIA Act should include a legislative presumption that will ensure notice to lawyers and journalists in all but the most exceptional cases where access to retained telecommunications data is sought.[139]

6.199 In response to concerns in respect of client legal privilege, the Attorney-General's Department noted that:

> At common law, legal professional privilege attaches to the content of privileged communications, not to the fact of the existence of a communication between a client and their lawyer (See: *National Crime Authority v S* [1991] FCA 234). This distinction is demonstrated in the routine practice of parties to proceedings filing affidavits of documents listing documents in their possession that are not being produced on the ground of privilege, thereby disclosing the fact of the existence of the document…[140]

6.200 The Department further noted the statutory restrictions preventing the accessing of content under the telecommunications data access regimes, and concluded:

> As such, the data retention regime, and agencies' powers to access telecommunications data more broadly, do not affect or authorise the disclosure of the content of any communication, including any privileged communication.[141]

138 Law Council of Australia, *Submission 126*, p. 22.

139 Law Council of Australia, *Submission 126*, p. 23.

140 Attorney-General's Department, *Submission 27*, p. 21.

141 Attorney-General's Department, *Submission 27*, p. 21.

6.201 The Media, Entertainment & Arts Alliance (MEAA) expressed concerns, shared by a number of other submitters, that the proposed data retention regime would have a significant impact on the freedom of the media to perform its role:

> MEAA believes that any moves to increase the level of surveillance of journalists and their sources by intrusive means such as the data retention proposed in the Bill will harm the ability of journalists to scrutinise the powerful and hold them to account, to expose corruption, to champion and campaign for important issues, and to gain the trust of our audience and our sources.[142]

6.202 MEAA went on to explain the reliance of journalists on confidential sources and their concern that the Bill threatens the confidentiality of those sources:

> Journalists rely on sources of information to carry out these duties. At times, those sources request anonymity – perhaps because they are in fear or could be subject to some form of violence, harassment or intimidation, particularly if they are a 'whistleblower'.
>
> The Bill threatens to expose the identity of sources and journalists as well as the communications between them and information they exchange.
>
> The Bill will undoubtedly undermine the crucial ethical obligation of journalists to protect the identity and information of confidential sources.
>
> This erosion of journalist privilege that is the consequence of the Bill will have a chilling effect on whistleblowers seeking to expose illegality, corruption or wrongdoing.[143]

6.203 The MEAA noted that the majority of legal jurisdictions, including the Commonwealth, recognise the principle of journalist privilege, and recommended that the Bill not proceed, but if it does:

> that appropriate checks and balances be introduced to ensure that the national security laws cannot be used to impede, threaten, contain or curtail legitimate reporting of matters in the public interest and that journalists and their confidential sources are free to continue to interact and communicate without being subjected to surveillance that would undermine the principles of press freedom.[144]

142 Media, Entertainment and Arts Alliance, *Submission 90*, p. 3.

143 Media, Entertainment and Arts Alliance, *Submission 90*, p. 3.

144 Media, Entertainment and Arts Alliance, *Submission 90*, pp. 9-10.

6.204 In response to suggestions that special status be afforded to the telecommunications data of journalists, the Attorney-General's Department noted the importance for the powers to apply generally and that legitimate whistleblowers would be protected by public interest disclosure legislation:

> Disclosures of data are available to support the enforcement of the criminal law, administration of pecuniary penalties and the protection of the public revenue. It is not appropriate to afford a special status to particular types of communications as powers of this type should, by their nature, be applied generally. However, to the extent that concerns relate to the disclosure of the identity of legitimate whistle-blowers, it is important to note that such persons have specific protection under the *Public Interest Disclosures Act 2013* (PID Act). The effect of those protections is that disclosures by legitimate whistle-blowers are not criminal acts. Accordingly, telecommunications data would not be available by reason of the disclosure.[145]

6.205 A submission by joint media organisations noted a recent report by Human Rights Watch in respect of the United States that large-scale surveillance makes it difficult for journalists to communicate with sources securely. The submission noted:

> The cumulative impact of these matters is a chilling effect on news gathering through increasing the perceived risks to sources including whistleblowers – in an environment which has also heightened the risk to news gathering by criminalising some reportage and not providing adequate protections for some categories of whistleblowers.[146]

6.206 Private Media raised similar concerns in its submission, noting the importance of the media as a watchdog, and the critical importance of protecting confidential sources:

> Whistleblowers and confidential sources are fundamental to this media role. Without individuals who are prepared to reveal wrongdoing and provide transparency, the media is unable to perform this role and powerful interests can operate with less accountability. For such individuals, anonymity and confidentiality are crucial … It is thus critical that the media is able to offer confidential sources protection – and this is already

145 Attorney-General's Department, *Submission 27*, pp. 21-22.

146 Joint media organisations, *Submission 125*, p. 3.

> recognised in federal legislation such as the Evidence Amendment (Journalists Privilege) Act 2010.
>
> However, a data retention scheme of the kind proposed in the Bill will make it significantly easier for powerful interests -- whether governments, well-resourced individuals or corporations – to pursue, harass, prosecute and intimidate whistleblowers who contact media outlets, because information relating to who has contacted journalists via any form of electronic communication will be stored for two years …[147]

6.207 Private Media referred in its submission to upcoming changes in the United Kingdom, and suggested similar arrangements should be introduced in Australia:

> The UK government, which last year introduced its own version of data retention, has acknowledged that police misuse of powers to access metadata had been 'entirely inappropriate' and will change the UK's data access laws to require police to obtain a warrant if they want to obtain a journalists' metadata, with a presumption that access would not be granted if the journalist was acting in the public interest.[148]

6.208 On this issue the Attorney-General's Department provided the following evidence in their submission:

> On 9 December 2014, the UK Home Office published a draft Code of Practice discussion paper on access to data. This issue of access to journalists' telecommunication during the investigation of crimes had been raised as an issue by that profession. The draft code of practice makes clear that communications data is not subject to any form of professional privilege. However, the Code notes that access to data relating to some professions may have a higher degree of privacy interference (the draft code specifies doctors, lawyers, journalists, MPs and ministers of religion).
>
> Some media reports had suggested that the UK Government was considering requiring law enforcement agencies to obtain warrants to access journalists' data. Rather than warrants, the Home Office proposes that authorising officers should give special consideration to necessity and proportionality when considering authorising the disclosure of data relating to the particular professions noted above.[149]

147 Private Media, *Submission 77*, p. 2.

148 Private Media, *Submission 77*, p. 2.

149 Attorney-General's Department, *Submission 27*, p. 22.

6.209 The supplementary submission from joint media organisations emphasised the concern of those organisations that the collection and storage of metadata could be accessed to identify journalists' sources, making it less likely that sources will share information and consequently have a chilling effect on reporting in the public interest. The submission proposed a tiered range of amendments to address this concern which can be summarised (in descending order of preference) as follows:

- media exemption from all three tranches of national security legislation;
- media exemption for the Bill;
- requirement for a warrant to access metadata of journalists and their sources;
- persons empowered to authorise requests to access data must be limited to the most senior officials of an agency, and the threshold for access must be more objective.[150]

Committee comment

6.210 The Committee recognises that certain telecommunications data has the potential to possess an additional level of sensitivity because of the nature of the relationship of those communicating, including client legal privilege that applies to certain communications between lawyers and their clients, and journalist relationships with confidential sources.

6.211 In the context of client legal privilege the Committee notes the evidence from the Attorney-General's Department that privilege attaches to the content of the communications, and that access to telecommunications data will not include any such content.

6.212 The Committee acknowledges the evidence from the Law Council of Australia that telecommunications data can nonetheless reveal a range of information about the communications between a lawyer and client from which certain inferences may be able to be made.

6.213 However, the Committee does not consider, on the evidence available, that there is a need for additional legislative protection in respect of accessing telecommunications data that may relate to a lawyer.

6.214 In the context of journalists and their sources, the Committee notes the capacity for telecommunications data to be used to identify confidential sources. The Committee acknowledges the claims that this may have a 'chilling impact', although the Committee also notes that in some circumstances, such as the investigation of serious crimes, it may be

150 Joint media organisations, *Submission 125.1*, pp. 1-3.

appropriate and proper for journalists to be investigated by law enforcement agencies.

6.215 The Committee acknowledges the importance of recognising the principle of press freedom and the protection of journalists' sources. The Committee considers this matter requires further consideration before a final recommendation can be made.

6.216 In the absence of pre-access oversight by an independent body, the Committee also considers it reasonable to require the Ombudsman or Inspector-General of Intelligence and Security (IGIS), as appropriate, to be notified of the making of an authorisation which is for the purpose of determining the identity of a journalist's sources.

Recommendation 26

The Committee acknowledges the importance of recognising the principle of press freedom and the protection of journalists' sources. The Committee considers this matter requires further consideration before a final recommendation can be made.

The Committee therefore recommends that the question of how to deal with the authorisation of a disclosure or use of telecommunications data for the purpose of determining the identity of a journalist's source be the subject of a separate review by this Committee.

The Committee would report back to Parliament within three months.

In undertaking this inquiry, the Committee intends to conduct consultations with media representatives, law enforcement and security agencies and the Independent National Security Legislation Monitor. The review will also consider international best practice, including data retention regulation in the United Kingdom.

Recommendation 27

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to require agencies to provide a copy to the Commonwealth Ombudsman (or Inspector General of Intelligence and Security (IGIS) in the case of ASIO) of each authorisation that authorises disclosure of information or documents under Chapter 4 of the Act for the purpose of determining the identity of a journalist's sources.

The Committee further recommends that the IGIS or Commonwealth Ombudsman be required to notify this Committee of each instance in which such an authorisation is made in relation to ASIO and the AFP as soon as practicable after receiving advice of the authorisation and be required to brief the Committee accordingly.

Destruction of accessed telecommunications data

6.217 The TIA Act does not currently contain any requirements in in respect of destruction of telecommunications data accessed by enforcement agencies or ASIO. The Law Council of Australia identified in its submission this lack of destruction requirements in respect of accessed data, and supported the inclusion of such a requirement:

> Chapter 4 of the TIA Act does not require enforcement agencies to destroy in a timely manner telecommunications data containing personal information which is irrelevant to the agency or no longer needed.
>
> The Law Council strongly supports the inclusion of provisions which establish positive obligations of this kind.[151]

6.218 The Law Institute of Victoria similarly queried what requirements will be put in place to ensure the timely destruction of retained data by agencies after the purpose for which the data was requested has been satisfied.[152]

6.219 At a public hearing, the IGIS noted the lack of a legislative requirement for ASIO to delete telecommunications data that is no longer needed:

> My second point is about what happens to data once it has been lawfully obtained by ASIO. This is an issue that is actually broader than telecommunications data, but it is highlighted by the increase in the volume of data that would be available under the proposed scheme. There are certainly good reasons ASIO may need to keep

151 Law Council of Australia, *Submission 126*, p. 25.

152 Law Institute of Victoria, *Submission 117*, p. 5.

> some data for a long time. But there is other data that, although it is obtained lawfully, turns out not to be relevant to security or is no longer relevant to security after a period of time. The balance between security and privacy, in my view, requires that this information should not be retained indefinitely, and I think that the general public would expect that material found not to be relevant to security would be deleted after a period of time.
>
> There are currently provisions that allow for the destruction of data by ASIO, but at the moment there seems to be little or no legislative requirement for ASIO to delete telecommunications data or other material that is no longer needed. In 2010 my predecessor looked at the retention of data by ASIO and suggested that ASIO should modify its policies and practices. The agreement between ASIO and the National Archives of Australia was reviewed in 2012, and the subject of the retention and destruction of data by ASIO is a focus for my office this year. While this project is ongoing, I do think this matter could also usefully be examined as part of the review of the Attorney-General's guidelines previously proposed by this committee and agreed to by government.[153]

6.220 When asked by the Committee whether there should be a compulsion for the agency, when it is finished with the data and it is not of any use in terms of legal purposes, to destroy the data, the IGIS stated:

> I can understand that there would be an impost in terms of resources to assess that at a certain point in time. However, I think that needs to be balanced against what I would consider to be the general public expectation that, if matter is found to be not relevant to security or no longer relevant to security, it should be deleted. I am not sure that balance is correct at the moment.[154]

6.221 The IGIS was also asked by the Committee to comment on whether there could be elements of the information that ASIO holds, such as pattern of life analysis, that they retain to see where investigations might take those patterns into the future. Dr Thom stated:

---

153 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 29 January 2015, p. 37.

154 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 29 January 2015, p. 40.

> Absolutely. There is a large amount of information that would have to be retained forever according to the guidelines, and I have no concerns about that at all.[155]

6.222 In response to a question on this issue from the Committee on whether the Bill should contain a mandatory destruction component, Professor George Williams gave his opinion that such a regime would be appropriate:

> I think that would allay community concerns that their private information may be sought, perhaps legitimately, but then held for an extremely long period of time—well past the nature of the investigation—and perhaps looked at again sometime down the track in less appropriate circumstances. I think the community concern about what some see as a blanket surveillance regime is that the onus is on parliament to make sure a scheme is designed that is very well tailored to the problem. And there is a problem that needs to be met here. We need a bill that removes many of the quite significant loose ends, that being one of them, that as yet have not been adequately dealt with.[156]

Committee comment

6.223 The Committee acknowledges the importance of ensuring that agencies are subject to appropriate obligations in respect of the retention and destruction of telecommunications data. In this respect the Committee notes the application of the various federal and state privacy and archives obligations, as well as agency specific legislation.

6.224 The Committee considers it has not received sufficient evidence to form a conclusion as to whether there is a need for a discrete obligation for destruction of telecommunications data to be inserted into the TIA Act, and if so, what form that requirement should take.

6.225 In respect of ASIO, the Committee notes that the agreement between ASIO and the National Archives was reviewed in 2012 and notes that the retention and destruction of data by ASIO is to be a focus for the IGIS this year. The Committee welcomes these ongoing discussions between the IGIS and ASIO in respect of destruction of information, and the planned review of the Attorney-General's Guidelines later this year.

---

155 Dr Vivienne Thom, Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 29 January 2015, p. 40.

156 Professor George Williams, *Committee Hansard*, Canberra, 30 January 2015, p. 7.

Recommendation 28

The Committee recommends that the Attorney-General's Department oversee a review of the adequacy of the existing destruction requirements that apply to documents or information disclosed pursuant to an authorisation made under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* and held by enforcement agencies and ASIO.

The Committee further recommends that the Attorney-General report to Parliament on the findings of the review by 1 July 2017.

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

A

Appendix A – Proposed data set

Source: Attorney-General's Department.

Data Retention Bill – Proposed data set

The Australian Government has introduced a Bill to oblige telecommunications providers to retain a limited set of telecommunications data ('metadata') for two years.

It is not the content or substance of a communication and it is not a person's web-browsing history. Agencies will continue to need to obtain a warrant to access the content of a communication.

The categories of data that industry will be asked to retain is set out in the legislation. The categories of data are based closely on the European Union Data Retention Directive. Regulations will provide further details about what is to be collected and greater technical specificity under each of these categories. This will enable flexibility as technology changes and provide more certainty and consistency for industry. The regulations will also limit the retention of subscriber information described in item 1 (c)-(f) to two years from creation of that data.

The draft set has been released publicly with the Bill and referred to the Parliamentary Joint Committee on Intelligence and Security for review and public consultation. There will also be ongoing consultation and review with a joint government/industry Expert Working Group, which has been set up to settle implementation, the data set and funding of the scheme.

Kinds of information to be kept

Matters to which information must relate	**Draft data set**	**Explanation and examples**
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service;	This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a person's identity or link a service or account to a person. This category also includes details about services attached to account, such as the unique identifying number attached to a mobile phone, or the IP address allocated to an internet access account or service. This category further includes billing and payment information. This can be a valuable source of information for law enforcement agencies. For example, even if someone has lied about other identifying details, it is more difficult to falsify payment information. Information about the status of a service can include when an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen. Information about metrics relating to the relevant service, such as available bandwidth, or historic aggregate upload and download volumes, is useful in law

Matters to which information must relate	Draft data set	Explanation and examples
	(d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device; (f) any information about metrics of the relevant service or a related account, service or device.	enforcement and national security investigations. For example, it allows agencies to better allocate resources in support of warrants where more intrusive surveillance is justified. For instance, if a suspect regularly downloads large volumes of information, agencies may need to assign additional system resources when provisioning a warrant.
2. The source of a communication	Any identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.	The 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.
3. The destination of a communication	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.	The destination of a communication is the recipient. For example, destination includes the phone number that received a call or SMS. This will include destinations for online services, such as the user name, number and/or IP address of the recipient of a Voice over IP (VoIP) call. The Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a person has browsed.
4. The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – this may last from a few hours to several days.
5. The type of communication or relevant service used in connection with a communication	The following: (a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: call waiting, call forwarding, bandwidth allowances.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service provides more technical detail about the service. For example, for a mobile voice service, whether it is a GPRS or VoLTE service. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c) of the Act.

Matters to which information must relate	Draft data set	Explanation and examples
6. The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication.	Location records will be limited to the location of a device at the start and end of a communication, such as a phone call or SMS message. Paragraph 187A(7) of the Bill provides that two or more communications that together constitute a single communications session are taken to be a single communication. In relation to internet access sessions, this means that service providers will only be required to keep location records at the start and end of a session, which can last from a few hours to a several days. Paragraph 187A(4)(e) of the Bill provides that locations records are limited to information that is used by a service provider in relation to the relevant service. This 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. As a result of the above, the location records to be kept by service providers will not allow continuous monitoring or tracking of devices. Precise or real-time location information, such as a GPS location is also not part of data retention.

B

Appendix B – Recommendations from PJCIS report of May 2013

Source: Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013.

List of recommendations - 2013 report

2 Telecommunications Interception

Recommendation 1

The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:

- expresses the dual objectives of the legislation –
  - ⇒ to protect the privacy of communications;
  - ⇒ to enable interception and access to communications in order to investigate serious crime and threats to national security; and
- accords with the privacy principles contained in the *Privacy Act 1988*.

Recommendation 2

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the:

- privacy impacts of proposed investigative activity;
- public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and
- availability and effectiveness of less privacy intrusive investigative techniques.

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

Recommendation 3

The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

Recommendation 4

The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*.

Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.

The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.

Recommendation 5

The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

Recommendation 6

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- privacy impact of the threshold;
- proportionality of the investigative need and the privacy intrusion;
- gravity of the conduct to be investigated by these investigative means;
- scope of the offences included and excluded by a particular threshold; and
- impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.

Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes:

- the ability for the issuing authority to set parameters around the variation of attributes for interception;
- the ability for interception agencies to vary the attributes for interception; and
- reporting on the attributes added for interception by an authorised officer within an interception agency.

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

- attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;
- oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and
- reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.

Recommendation 8

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure:

- protection of the security and privacy of intercepted information; and
- sharing of information where necessary to facilitate investigation of serious crime or threats to national security.

Recommendation 9

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.

Recommendation 10

The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunications (Interception and Access) Act 1979* be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features:

- a single threshold for law enforcement agencies to access communications based on serious criminal offences;
- removal of the concept of stored communications to provide uniform protection to the content of communications; and
- maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;
- rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;
- reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and
- Parliamentary oversight of the use of interception.

Recommendation 11

The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.

Recommendation 12

The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.

Recommendation 13

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include provisions which clearly express

the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.

Recommendation 14

The Committee recommends that the *Telecommunications (Interception and Access Act) 1979* and the *Telecommunications Act 1997* be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.

Recommendation 15

The Committee recommends that the Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions.

Recommendation 16

The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.

Recommendation 17

The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority.

The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.

Recommendation 18

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:

- clear protection for the privacy of communications;
- provisions which are technology neutral;
- maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;
- clearly articulated and enforceable industry obligations; and
- robust oversight and accountability which supports administrative efficiency.

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:

- Independent National Security Legislation Monitor;
- Australian Information Commissioner;
- ombudsmen and the Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

3 Telecommunications security

Recommendation 19

The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide:

- a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference;
- a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and

- powers of direction and a penalty regime to encourage compliance.

The Committee further recommends that the Government, through a Regulation Impact Statement, address:

- the interaction of the proposed regime with existing legal obligations imposed upon corporations;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
- impacts on competition in the market-place, including:
  - ⇒ the potential for proposed requirements to create a barrier to entry for lower cost providers;
  - ⇒ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
  - ⇒ any other relevant effects.

4 Australian Intelligence Community Legislation Reform

Recommendation 20

The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words "and includes multiple computers operating in a network".

The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.

Recommendation 21

The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee

further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

Recommendation 22

The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*.

Recommendation 23

The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.

Recommendation 24

Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.

Recommendation 25

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.

Recommendation 26

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.

Recommendation 27

The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.

Recommendation 28

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.

Recommendation 29

The Committee recommends that should the Government proceed with amending the *Australian Security Intelligence Organisation Act 1979* to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.

Recommendation 30

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004,* in particular by optical devices.

Recommendation 31

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.

Recommendation 32

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.

Recommendation 33

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.

Recommendation 34

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.

Recommendation 35

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.

Recommendation 36

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.

Recommendation 37

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code.

The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.

Recommendation 38

The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.

Recommendation 39

The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the *Australian Security Intelligence Organisation Act 1979* should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.

Recommendation 40

The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Recommendation 41

The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

5 Data Retention

Recommendation 42

There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- any mandatory data retention regime should apply only to meta-data and exclude content;
- the controls on access to communications data remain the same as under the current regime;
- internet browsing data should be explicitly excluded;
- where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
- the data should be stored securely by making encryption mandatory;
- save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;
- the costs incurred by providers should be reimbursed by the Government;
- a robust, mandatory data breach notification scheme;

- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
- oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

Recommendation 43

The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:

- there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;
- there should be an annual report on the operation of this scheme presented to Parliament; and
- the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.

C

Appendix C – Summary of Implementation Working Group recommendations

Source: Data Retention Implementation Working Group*, Report 1 of the Data Retention Implementation Working Group*, December 2014.

Summary of IWG Recommendations

The IWG, following its discussions and support provided by industry experts, recommends that the Government consider a number of amendments to the proposed data set to support further clarity and assist implementation of the data retention scheme. The IWG recommendations relate to potential changes to both the data set itself, as well as changes to the explanatory material accompanying the data set. The matters that Government may wish to consider are summarised in the **Table 1** below, and are overlayed on the proposed data set and highlighted at **Attachment A** for ease of consideration.

Table 1: Summary of IWG recommendations

Recommendation	Details
IWG's proposed amendments to the data set	
1	Amend text to provide additional clarity on the distinction between actual usage or consumption and contractual terms regarding allowances or caps.
2	Amend text to replace the reference to "bandwidth" with "data volume usage" to improve clarity and distinguish from data allowances.
3	Remove the proposed requirement for service providers to retain metric information relating to plans and contracts (data set element 1(f)).
4	Change the phrase "any identifiers" in items 2 and 3 of the data set to "identifiers".
IWG's proposed amendments to policy and process	
5	Any proposed change to the regulations should only come into effect after Parliament has had an opportunity to review the proposal and the disallowance period has expired.
IWG's proposed amendments to the data set's explanatory material	
6	Include additional explanatory material providing specific examples of the application of data set elements in relation to identifiers across a selection of current service types to support clarity for industry while retaining technological neutrality

7	Include additional service-level examples illustrating how data retention applies, with particular reference to the application to access layer services (including where particular data points do not apply).
8	Include additional explanation, consistent with paragraph 187A(4)(b) of the Bill, highlighting the application of data retention obligations to wholesale and retail providers, including that a wholesale provider is not required to retain "downstream" information in relation to a service provided by a retail provider.
9	Include additional explanation stating, for the avoidance of doubt, that the data retention obligations do not require providers of free services that do not generate any billing information, to create or retain such data.
10	Include additional explanation, consistent with subsection 187A(7) of the Bill, illustrating the application of the concept of a "communication session", including more examples and noting that a communication session can last for an extended period (e.g. months in the case of some internet access sessions).
11	Include additional text, consistent with paragraph 187A(4)(b) of the Bill, clarifying that data set item 3, the destination of a communication, is not required in relation to internet access services.
12	Include an explanation of the difference between data usage and data allowance, including that these data points may be retained in a way that is consistent with a provider's existing records management, (e.g. aligned with that provider's billing cycle).
13	Replace any reference to a "person" with "subscriber".
14	Include, in relation to data set item 5 (type of communication) additional examples highlighting the meaning of "type" of communication in particular contexts.
15	Include additional explanatory material illustrating the operation of location information requirements in relation to non-mobile services.
16	Insert additional text to clarify that the data retention obligations do not preclude service providers from retaining items in the data set for longer than the required two year period for their own business purposes.

D

Appendix D – List of Submissions and Exhibits

Submissions

1. Mr Alexander Lynch
2. Mr Alexander Schnur
3. Mr Noel Butler
4. Mr Daniel Gorza
5. Professor George Williams and Dr Keiran Hardy, Gilbert + Tobin Centre of Public Law
    - 5.1 Supplementary
6. Communications Alliance Ltd and Australian Mobile Telecommunications Association
    - 6.1 Supplementary
7. Australian Federal Police
    - 7.1 Supplementary
    - 7.2 Supplementary
8. Victoria Police
    - 8.1 Supplementary
9. South Australia Police
    - 9.1 Supplementary
10. Northern Territory Police, Fire and Emergency Services
11. Western Australia Police
12. Australian Security Intelligence Organisation
    - 12.1 Supplementary
    - 12.2 Supplementary

38 Mr Glenn Bradbury
39 Commissioner for Privacy and Data Protection (Victoria)
40 Mr Hugh Murdoch
41 Heather Dowling
42 Australia Human Rights Commission
    42.1 Supplementary
43 Mr Adam Cooksley
44 Mr Cam Browning
45 Mr Geoff Walker
46 Viraf Bhavnagri
47 Ms Priya Shaw
48 Australian Commission for Law Enforcement Integrity
49 Ms Fiona Maley
50 Ms Pam Webster
51 Mr William Delaforce
52 Name Withheld
53 Ms Ashley Doodkorte
54 Blueprint for Free Speech
55 Mr Paul White
56 Mr Roger Clark
57 Dr Peter Evans
58 Mr Ken Stephens
59 Mr Andrew Horton
60 Mr Marco Setiawan
61 Mr Daniel Scott
62 Ms Catalina Zylberberg
63 Ms Bethany Skurrie
64 Mr David Murray
65 Mr Murray Deerbon
66 Ms Sue Bettison
67 Mr Donald Newgreen
68 Ms Sally Wylie
69 Mr Daniel Audsley
70 Dr Ricardo Cavicchioli and Dr Tassia Kolesnikow

71 Human Rights Law Centre

72 Police Federation of Australia

73 Mr Tom McDonnell

74 Commonwealth Ombudsman

75 Australian Privacy Foundation

75.1 Supplementary

76 Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church of Australia

77 Private Media

78 Name Withheld

79 Ms Catherine Cresswell

80 Privacy International

81 Eric Lindsay

82 Ian Hobbs

83 Bill Fisher

84 Universities Australia

85 Dr A Bryan Fricker

86 Optus

86.1 Supplementary

86.2 Supplementary

87 Rochelle Roberts

88 Australian Lawyers for Human Rights

89 Australian Computer Society

90 Media, Entertainment & Arts Alliance

91 Ms Terri Butler MP

92 Office of the Australian Information Commissioner

92.1 Supplementary

93 University of Sydney

94 Institute of Public Affairs

95 Amnesty International

96 Dr A J Wood

97 Electronic Frontiers Australia

98 Society of University Lawyers

99 Dr Paul Bernal

100 Corruption and Crime Commission (WA)
101 Name Withheld
102 Mr David Lovejoy
103 Paul Schnackenburg
104 Dr Felix Rauch
105 Roger Graf
106 Mr Oak McIlwain
107 Name Withheld
108 Jonathan Grace
109 Australian Information Industry Association
    109.1 Supplementary
110 Open Knowledge Australia
111 Communications Law Centre, University of Technology Sydney
112 Telstra
    112.1 Supplementary
    112.2 Supplementary
113 Mr Terry Darling
114 Dr John Selby, Professor Vijar Varadharajan and Dr Yvette Blount
115 Mr Doug Carter
116 Name Withheld
117 Law Institute of Victoria
    117.1 Supplementary
118 Thoughtworks Pty Ltd
119 Daniel Black
120 Australian Communications Consumer Action Network
121 Mr Scott Millwood
122 Internet Society of Australia
    122.1 Supplementary
123 Mr Mark Newton
124 Pirate Party Australia
125 Joint media organisations
    125.1 Supplementary
126 Law Council of Australia
    126.1 Supplementary

127 Australian Customs and Border Protection Service
128 FutureWise
129 Councils for civil liberties across Australia
130 Vodafone
    130.1 Supplementary
    130.2 Supplementary
131 Inspector-General of Intelligence and Security
132 Guardian Australia
133 Mr John Blair
134 Mr Albert Lightfoot
135 Mr Noel Falk
136 Ash Naughton
137 Mr Ben Marshall
138 Name Withheld
139 Mr Alan Lamb
140 Mr Graeme Tychsen
141 Mr Gordon Curtis
142 Mr Bill Egan
143 Ms Eileen Whitehead
144 Ms Jane Paterson
145 Mr Leon Lack
146 Mr Maurice Jones
147 Mr Einar Thorsteinsson
148 Mr Robert Lammers
149 Mr Paul James
150 Name Withheld
151 Ms Anne Layton-Bennett
152 Ms Heather Stock
153 Mr James McPherson
154 Ms Barbara Reed
155 Ms Katrina McAlpine
156 Ms Dimity Odea
157 Mr Simon Kemp
158 Mr Paul Wilkins

159 Ms Stephanie Stewart
160 Mr David Powell
161 Ms Elayne Jay
162 Ms Kerrie Matchett
163 Ms Eve Stocker
164 Mr Ben Smith
165 Mr Nathan Sherburn
166 Name Withheld
167 Mr Keith Wilson
168 Mr Anthony Hughes
169 Ms Jenny Rae
170 Name Withheld
171 Ms Belinda Wright
172 Arda Barut
173 Chris Anderson
174 Yoon Leng Ooi
175 Mr Stephen Vicarioli
176 Mr Malcolm McKinnon
177 Ms Deborah Harris
178 Ms Lidia Nemitschenko
179 Leigh Milne
180 Shirley McRae and Wanda Grabowski
181 Ms Sharon Whitewood
182 Mr James Bowling
183 Chris Ogilvie
184 Andy Spate
185 Roger Marchant
186 Mr Ken White
187 Bob Brown
188 Name Withheld
189 Cara Clark
190 Mr Michael Latta
191 Mr Anthony Cavanna
192 Name Withheld

193 Name Withheld
194 David Vaile and Paolo Remati
195 Charles Lowe
196 Proctor McKenzie
197 D Adams
198 Muslim Legal Network (NSW)
199 NSW Ministry for Police and Emergency Services
200 Ms Erica Jolly
201 Crime and Corruption Commission (Queensland)
202 State and Territory police forces
203 Mr Phill Ball
204 Mr Shane Greenaway

Exhibits

1. Law Council of Australia
   Law Council policy position on a mandatory telecommunications data retention scheme, November 2014
   (Related to Submission No. 126)
2. Attorney-General's Department
   Report 1 of the Data Retention Implementation Working Group
   (Related to Submission No. 27)

E

Appendix E – Witnesses appearing at public and private hearings

Wednesday, 17 December 2014 (public hearing)

Attorney-General's Department

Ms Katherine Jones, Deputy Secretary

Ms Anna Harmer, A/g First Assistant Secretary

Mr Simon Lee, A/g Director

Australian Crime Commission

Mr Christopher Dawson, Chief Executive Officer

Ms Kathryn McMullan, National Manager

Australian Federal Police

Mr Andrew Colvin, Commissioner

Mr Michael Phelan, Deputy Commissioner National Security

Mr Tim Morris, Assistant Commissioner, National Manager High Tech Crime Operations

Australian Security Intelligence Organisation

Ms Kerri Hartland, A/g Director-General

Australian Mobile Telecommunications Association

Mr Chris Althaus, Chief Executive Officer

Communications Alliance

Mr John Stanton, Chief Executive Officer

Mr Peter Froelich, Industry Member

Mr Michael Elsegood, Industry Member

Wednesday, 17 December 2014 (private hearing)

Australian Crime Commission

Ms Kathryn McMullan, National Manager

Australian Federal Police

Mr Michael Phelan, Deputy Commissioner National Security

Australian Security Intelligence Organisation

Ms Kerri Hartland, A/g Director-General

First Assistant Director-General, Counter Espionage and Interference

First Assistant Director-General, Counter-Terrorism

Attorney-General's Department

Ms Katherine Jones, Deputy Secretary

Ms Anna Harmer, A/g First Assistant Secretary

Thursday, 29 January 2015 (public hearing)

Australian Commission for Law Enforcement Integrity

Mr Michael Griffin AM, Integrity Commissioner

Ms Sarah Marshall, Executive Director, Operations

Mr Nick Sellars, Executive Director, Secretariat

Ms Penny McKay, Principal Lawyer

Australian Communications Consumer Action Network

Ms Narelle Clark, Deputy Chief Executive Officer

Ms Katerina Pavlidis, Grants and Research Officer

Australian Computer Society

Ms Brenda Aynsley, President

Mr Athol Chambers, Manager, Federal and State Government Relations

Australian Human Rights Commission

Professor Gillian Triggs, President

Ms Bronwyn Barnes, Lawyer

Australian Information Industry Association

Ms Susan Campbell, Chief Executive Officer

Ms Suzanne Roche, General Manager, Policy and Advocacy

Australian Securities and Investments Commission

Mr Greg Tanzer, Commissioner

Mr Chris Savundra, Senior Executive Leader, Market Enforcement

Mr David Lusty, Special Counsel

Electronic Frontiers Australia

Mr Jon Lawrence, Executive Officer

Internet Society of Australia

Mr Laurie Patton, Chief Executive Officer

Mr George Fong, President

Ms Holly Raiche, Chair, Policy Committee

Joint Media Organisations

Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, NewsCorp

Mr Mark Hollands, Chief Executive, The Newspaper Works

Ms Sarah Kruger, Senior Lawyer, SBS

Ms Julie Flynn, Chief Executive Officer, Free TV Australia

Office of the Australian Information Commissioner

Mr Timothy Pilgrim, Australian Privacy Commissioner

Ms Angelene Falk, Assistant Commissioner

Office of the Commonwealth Ombudsman

Mr Colin Neave, Commonwealth Ombudsman

Mr Richard Glenn, Deputy Ombudsman

Ms Erica Welton, Director, Inspections and Law Enforcement

Office of the Inspector-General of Intelligence and Security

Dr Vivienne Thom, Inspector-General of Intelligence and Security

Mr Jake Blight, Assistant Inspector-General of Intelligence and Security

Telstra

Mrs Jane van Beelen, Executive Director

Mr James Shaw, Government Relations

Mr Michael Burgess, Chief Information Security Officer

Mrs Kate Hughes, Chief Risk Officer

Vodafone Hutchison Australia

Mr Matthew Lobb, General Manager, Industry Strategy and Policy

Friday, 30 January 2015 (public hearing)

Attorney-General's Department

Mr Chris Moraitis, Secretary

Ms Anna Harmer, A/g First Assistant Secretary

Mr Simon Lee, A/g Director

Australian Crime Commission

Ms Kathryn McMullan, National Manager

Australian Federal Police

Mr Michael Phelan, Deputy Commissioner National Security

Deputy Commissioner Graham Ashton, Capability

Assistant Commissioner Tim Morris, National Manager High Tech Crime Operations

Australian Privacy Foundation

Mr David Lindsay, Vice-Chair

Dr Roger Clarke, Past Vice-Chair

Australian Security Intelligence Organisation

Mr Duncan Lewis, Director-General of Security

Bravehearts

Mrs Hetty Johnston, Founder and Chief Executive Officer

Miss Carol Ronken, Research Manager

Councils for civil liberties across Australia

Mr Michael Cope, President, Queensland Council for Civil Liberties

Dr Lesley Lynch, Secretary, New South Wales Council for Civil Liberties

Mr Hugo de Kock, Member, Liberty Victoria

Individuals

Professor George Williams

Law Council of Australia

Mr Duncan McConnel, President

Mr Peter Leonard, Chairperson of Law Council of Australia (Business Law) Media and Communications Committee

Ms Olga Ganopolsky, Chair, Privacy Law Committee, Business Law Section

Mr Matthew Dunn, Director of Policy

Dr Natasha Molt, Senior Policy Lawyer, Criminal Law

Media, Entertainment & Arts Alliance

Mr Christopher Warren, Federal Secretary

Mr Paul Murphy, Director, Media

New South Wales Police

Assistant Commissioner Malcolm Lanyon, Commander, Special Services Group

Detective Superintendent Arthur Kopsias, Commander, Telecommunications Interception Branch

Optus

Mr David Epstein, Vice President

Mr Michael Elsegood, Manager, Regulatory Compliance and Safeguards

South Australia Police

Assistant Commissioner Paul Dickson, Crime Service

Victoria Police

Inspector Gavan Segrave, Intelligence & Covert Support Command

Monday, 9 February 2015 (private hearing)

Attorney-General's Department

Ms Katherine Jones, Deputy Secretary

Ms Anna Harmer, Assistant Secretary

Mr Daniel Abraham, Director

Mr Gregory Sadler, Senior Legal Officer