

The Senate

Legal and Constitutional Affairs
References Committee

Comprehensive revision of the
*Telecommunications (Interception and
Access) Act 1979*

March 2015

© Commonwealth of Australia 2015

ISBN 978-1-76010-181-7

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website: <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

This document was produced by the Senate Legal and Constitutional Affairs Committee secretariat and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Members of the committee

Members

Senator Scott Ludlam (AG, WA) (Inquiry Chair) (from 12 December 2013)
Senator the Hon Ian Macdonald (LP, QLD) (Deputy Chair) (from 10 July 2014)
Senator Catryna Bilyk (ALP, TAS) (from 1 July 2014)
Senator Jacinta Collins (ALP, VIC) (from 1 July 2014)
Senator the Hon Joe Ludwig (ALP, QLD)
Senator Linda Reynolds (LP, WA) (from 1 July 2014)

Former members

Senator Zed Seselja (LP, ACT) (Deputy Chair) (until 30 June 2014)
Senator Gavin Marshall (ALP, VIC) (until 30 June 2014)
Senator the Hon Lisa Singh (ALP, TAS) (until 30 June 2014)

Participating members

Senator David Leyonhjelm (LDP, NSW) (from 1 July 2014)
Senator Nick Xenophon (IND, SA)

Substituted members

Senator Scott Ludlam (AG, WA) to replace Senator Penny Wright (Chair) (AG, SA)

Secretariat

Ms Sophie Dunstone, Committee Secretary
Ms Sandra Kennedy, Principal Research Officer
Ms Jo-Anne Holmes, Administrative Officer

Suite S1.61 Telephone: (02) 6277 3560
Parliament House Fax: (02) 6277 5794
CANBERRA ACT 2600 Email: legcon.sen@aph.gov.au

Table of contents

Members of the committee	iii
List of abbreviations	x
Overview	1
Chapter 1	3
Introduction	3
The referral	3
Background to the terms of reference	3
The current inquiry	6
Acknowledgement.....	7
Note on references.....	7
Scope and structure of the report.....	7
Chapter 2	9
<i>The Telecommunications (Interception and Access) Act 1979</i>	9
Why is reform needed?.....	9
Support for reform.....	10
Law enforcement and national security agencies.....	10
Civil liberty and rule of law stakeholders	11
Approach to reform	11
Balancing the right to privacy and national interests	12
Chapter 3	15
Warranted access to telecommunication content	15
An overview of the warrant regime.....	15
Telecommunications service warrants and named person warrants	16
Stored telecommunications warrants.....	17

Removing legislative duplication in the warrant regime.....	18
A single attribute-based interception regime.....	19
How would it work?	22
Concerns raised in relation to attribute-based interception	22
Chair's Minority Additional Comments.....	25
Access to telecommunications data.....	25
An overview of the telecommunications data access regime.....	25
What is telecommunications data?	26
Using telecommunications data.....	29
The need to review the threshold for access to telecommunications data	33
Introduction of oversight for telecommunications data	36
Should access to 'telecommunications data' require a warrant?	38
Chair's views and recommendations: existing regime for authorising access to telecommunications data.....	40
Mandatory data retention.....	42
Background.....	42
Why is mandatory data retention being proposed?	43
Scope of the proposed mandatory data retention regime	45
International developments	61
Is international practice moving away from mandatory data retention?	61
Alternatives to mandatory data retention	70
Chair's views and recommendations: mandatory data retention.....	72
Introduction	72
Broader reform is required	72
The need for a definition	73
Access to telecommunications data.....	74
The proposed retention period.....	75
A destruction requirement	75

Oversight	76
Protection of press freedom.....	76
Mandatory data breach notification scheme.....	76
Divergent views on '5 Eyes' collaboration	78
Additional Remarks from Government Senators.....	81
The Reform Agenda	81
Streamlining the Warrant Regime	82
Oversight and the Commonwealth Public Interest Monitor.....	83
Metadata – Definition.....	83
Mandatory Data Retention	84
Objects Clause	85
Destruction requirement.....	85
Conclusions and Recommendations.....	85
Comments from Opposition Senators.....	87
Recommendations of the 2013 PJCIS Report with respect to telecommunications interception.....	89
Conclusion.....	94
Appendix 1 - Recommendations 1 to 18, 42 and 43 of the PJCIS Report of the Inquiry into Potential Reforms of Australia's National Security Legislation.....	97
Appendix 2 - Public submissions	105
Appendix 3 - Public hearings and witnesses.....	107
Appendix 4 - Examples of telecommunications data generated by a website, a Facebook page and a tweet.....	111
Appendix 5 - Tabled documents, answers to questions on notice and additional information.....	113
Appendix 6 - Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006	115

List of abbreviations

AAT	Administrative Appeals Tribunal
ACC	Australian Crime Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AHRC	Australian Human Rights Commission
ALRC	Australian Law Reform Commission
AMTA	Australian Mobile Telecommunications Association
APP	Australian Privacy Principles
ASIO	Australian
CAC	Communications Access Co-ordinator
CIA	Central Intelligence Agency
CSP	Carriage Service Provider
ECHR	European Court of Human Rights
ECJ	European Court of Justice
EM	Explanatory Memorandum
EU	European Union
IBAC	Independent broad-based anti-corruption commission
ICCPR	International Covenant on Civil and Political Rights
IPA	Institute of Public Affairs
ISOC-AU	Internet Society of Australia
MEAA	Media Entertainment and Arts Alliance
NSA	National Security Agency
OAIC	Office of the Australian Information Commission
PJCHR	Parliamentary Joint Committee on Human Rights

PJCIS	Parliamentary Joint Committee on Intelligence and Security
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>
UN	United Nations
URL	Uniform resource locator
VOIP	Voice over internet protocol

Overview

The committee's inquiry has spanned 15 months. During that time, the committee received much evidence highlighting the need for urgent and comprehensive reform of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) including substantial comment on the matter of mandatory data retention. During the later stages of the committee's inquiry, the government announced that it would be introducing a mandatory telecommunications data retention regime.

Although the issues of comprehensive reform of the TIA Act and mandatory data retention are not mutually exclusive, to the extent possible, they have been considered separately to ensure that adequate consideration is given to both matters.

This majority consensus report details the need for reform of the existing TIA Act.

Separate additional remarks on the matters of data access and data retention are provided by the committee Chair, the government members of the committee and the opposition members of the committee.

Chapter 1

Introduction

The referral

1.1 On 12 December 2013, the Senate referred the following matter to the Legal and Constitutional Affairs References Committee for inquiry and report by 10 June 2014:

Comprehensive revision of the Telecommunications (Interception and Access) Act 1979 (the TIA Act), with regard to:

- a) the recommendations of the Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice report, dated May 2008, particularly recommendation 71.2; and
- b) recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security Inquiry into the potential reforms of Australia's National Security Legislation report, dated May 2013.¹

1.2 The Senate later extended the reporting date – to 27 August 2014, 29 October 2014, 3 December 2014, 12 February 2015 and 18 March 2015.² As a result of the introduction of the Abbott Government's Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 and its referral to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry and report by 27 February 2015, the Senate again extended the reporting date of the inquiry to enable the committee to consider the government's proposed data retention policy and the findings of the PJCIS.³

Background to the terms of reference

1.3 As the terms of reference indicate, the committee was required to comprehensively review the Telecommunications (Interception and Access) Act 1979 (TIA Act) having regard to recommendations made by two other bodies—the Australian Law Reform Commission (ALRC) in its report, For Your Information: Australian Privacy Law and Practice, and the PJCIS, in its report of the Inquiry into Potential Reforms of Australia's National Security Legislation. These earlier inquiries are briefly discussed below.

1 *Journals of the Senate*, 12 December 2013, p. 373.

2 *Journals of the Senate*, 14 May 2014, p. 793; *Journals of the Senate*, 27 August 2014, p. 1318; *Journals of the Senate*, 29 October 2014, p. 1673; *Journals of the Senate*, 1 December 2014, p. 1917; and *Journals of the Senate*, 12 February 2015, p. 2159.

3 *Journals of the Senate*, 18 March 2015, p. 2320.

The Australian Law Reform Commission—For Your Information: Australian Privacy Law and Practice

1.4 On 30 January 2006, the then Attorney-General, the Hon Philip Ruddock MP, referred 'matters relating to the extent to which the Privacy Act 1988 and related laws continue to provide an effective framework for the protection of privacy in Australia' to the ALRC for inquiry and report.⁴ In referring the matter, the Attorney-General requested that, among other things, the ALRC have regard to:

- the rapid advances in information, communication, storage, surveillance and other relevant technologies;
- possible changing community perceptions of privacy and the extent to which it should be protected by legislation; and
- emerging areas that may require privacy protection.⁵

1.5 The ALRC presented its report, titled 'For Your Information: Australian Privacy Law and Practice', on 30 May 2008 making 295 recommendations. The primary focus of the ALRC's report was information privacy,⁶ however, the issue of privacy and telecommunications⁷ was considered in Part J of its report. In Part J the ALRC acknowledged 'the need for telecommunications regulation to respond to a convergent communications environment'⁸ but noted that as issues relating to convergence were beyond the scope of its terms of reference they should be considered separately. To that end, in recommendation 71.2 the ALRC called for a review of telecommunications legislation. Recommendation 71.2 reads as follows:

The Australian Government should initiate a review to consider whether the Telecommunications Act 1997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

4 Australian Law Reform Commission (ALRC), *For your information: Australian Privacy Law and Practice*, May 2008, p. 19.

5 ALRC, *For your information: Australian Privacy Law and Practice*, May 2008, p. 19.

6 Information privacy involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection'. See: ALRC, *For your information: Australian Privacy Law and Practice*, May 2008, p. 142.

7 Privacy of communications covers the security and privacy of mail, telephones, email and other forms of communication. See: ALRC, *For your information: Australian Privacy Law and Practice*, May 2008, p. 142.

8 ALRC, *For your information: Australian Privacy Law and Practice*, May 2008, p. 2392.

-
- (a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;
 - (b) how these two Acts interact with each other and with other legislation;
 - (c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;
 - (d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and
 - (e) whether the Telecommunications (Interception and Access) Act should be amended to provide for the role of a public interest monitor.⁹

1.6 The Rudd Labor Government released its first stage response to the ALRC's report on 14 August 2009. The response committed the government to first reforming the 'privacy foundations' and to enhancing the role of the Privacy Commissioner.¹⁰ Reform would be 'technology neutral' to ensure the protection of personal information held in any medium.¹¹ Although the first stage response addressed 197 of the ALRC's 295 recommendations, it did not address the matters set out in recommendation 71.2 or broader issues relating to reform of the TIA Act. Rather, the government stated that it would consider the remaining recommendations of the ALRC after the first stage

9 See: ALRC, *For your information: Australian Privacy Law and Practice*, May 2008, p. 2395.

10 In the response, the government committed to: creating a harmonised set of Privacy Principles; redrafting and updating the Privacy Principles; creating a comprehensive credit reporting framework; improving health sector information flows, and giving individuals new rights to control their health records, contributing to better health service delivery; requiring the public and private sector to ensure the right to privacy will continue to be protected if personal information is sent overseas; and strengthening the Privacy Commissioner's powers to conduct investigations, resolve complaints and promote compliance, contributing to more effective and stronger protection of the right to privacy. Source: Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108. October 2009. See: http://www.dpmc.gov.au/privacy/alrc_docs/stage1_au_govt_response.pdf (accessed 25 March 2014).

11 Source: Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108. October 2009. See: http://www.dpmc.gov.au/privacy/alrc_docs/stage1_au_govt_response.pdf (accessed 25 March 2014).

response reforms had progressed. Legislation giving effect to the government's first stage response was enacted in November 2012.¹²

The Parliamentary Joint Committee on Intelligence and Security—Inquiry into potential reforms of Australia's National Security Legislation

1.7 In May 2012, the then Attorney-General (the Hon Nicola Roxon MP) requested that the PJCIS conduct an inquiry into a package of potential reforms to Australia's national security legislation. The package of reforms put to the PJCIS was comprised of 'telecommunications interception reform, telecommunications sector security reform and Australian intelligence community reform'.¹³ Along with the referral of the PJCIS inquiry, the Attorney-General's Department (the department) released a discussion paper that canvassed issues covered by the ALRC's report, including matters set out in Part J (which, as noted above, included recommendation 71.2).

1.8 The PJCIS tabled its report in June 2013 making 43 recommendations. Recommendations 1–18 related to the TIA Act and recommendations 42 and 43 concerned data retention. These recommendations are listed at Appendix 1. It is noted by the committee that in February 2015 the PJCIS handed down its inquiry report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 which seeks to introduce a two year mandatory data retention regime in respect of telecommunications data (metadata) and implement recommendation 42 of the PJCIS's recommendations.

The current inquiry

1.9 The committee advertised the inquiry in *The Australian* newspaper on 5 February 2014. Details of the inquiry were published on the committee's website at www.aph.gov.au/senate/legalcon. The committee also wrote to over 110 organisations and individuals inviting submissions by 27 February 2014.

1.10 The committee received 46 submissions. Public submissions were published on the committee's website and are listed at Appendix 2. The committee held six public hearings: on 22 and 23 April 2014, 21 July 2014, 26 September 2014 and 2 February 2015 in Canberra, and on 29 July 2014 in Sydney. The committee also took

12 The *Privacy Amendment (Enhancing Privacy Protection) Amendment Act 2012* (Cth). See: <http://www.alrc.gov.au/inquiries/privacy/implementation> (accessed 25 March 2014). Among other things that Act amended the *Privacy Act 1988* (Cth) to replace the existing privacy principles for the public and private sectors with a single set of privacy principles (the Australian Privacy Principles (APPs)). The APPs came into effect on 12 March 2014. For further information about the first stage response reforms, see: http://www.dpmc.gov.au/privacy/alrc_docs/stage1_au_govt_response.pdf, and <http://www.alrc.gov.au/inquiries/privacy/implementation>.

13 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 3.

evidence in camera. A list of witnesses who appeared at the public hearings is at Appendix 3. The Hansard transcripts from the public hearings can be accessed on the committee's website.

Acknowledgement

1.11 The committee thanks all those organisations and individuals who made submissions and gave evidence at the public hearings.

Note on references

1.12 References in the report to the committee *Hansard* are to the proof committee Hansard. Page numbers between the proof committee *Hansard* and the official Hansard may differ.

Scope and structure of the report

1.13 During this inquiry the committee sought to address the matters referred to it by examining issues raised since the reviews of the ALRC and the PJCIS. The committee took the approach that the recommendations of the ALRC's report relating to the TIA Act (including recommendation 71.2) were, to some extent, realised by the then Labor Government's referral of a review of potential reforms of Australia's national security legislation to the PJCIS committee. In that referral, the PJCIS was asked to examine many of the considerations set out in the ALRC's recommendation 71.2.

1.14 The committee notes the breadth of the recommendations of the PJCIS that related to the TIA Act: recommendations 1 to 18 related specifically to the existing provisions of the TIA Act; and recommendations 42 and 43 considered the broader policy issue of mandatory data retention. This committee notes that although the PJCIS did not reach a consensus view on mandatory data retention in its 2013 report, it recommended considerations that should be had if the government were persuaded to implement such a regime.¹⁴ The committee acknowledges that the 2015 PJCIS report into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 examines issues relating to data retention with greater specificity and detail than does the 2013 report.

1.15 This report comprises three chapters. The current chapter outlines the inquiry process. Chapter 2 considers the need for reform to the TIA Act and chapter 3 discusses warranted access to telecommunications content.

1.16 The committee could not reach agreement in relation to access to data and mandatory data retention. The minority reports at the conclusion of this committee report outline committee members' views on these issues.

14 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, pp. 192–193.

Chapter 2

The Telecommunications (*Interception and Access*) Act 1979

2.1 This chapter of the report considers the need for reform of the *Telecommunication (Interception and Access) Act 1979* (TIA Act) and the possible approaches to reform.

Why is reform needed?

2.2 Legislation to protect the privacy of individuals was introduced in 1960 through the *Telephonic Communications (Interception) Act 1960*, which prohibited the interception of telephonic communications except where authorised in the interests of the security of the Commonwealth.¹ That Act was repealed and replaced by the *Telecommunications (Interception) Act 1979* on 1 June 1980.² In 2006, the *Telecommunications (Interception) Act 1979* was amended to change the name of the Act (amongst other things) to the current *Telecommunications (Interception and Access) Act 1979* (TIA Act).³ The Attorney-General's Department (the department) has advised that the objectives of the TIA Act are as follows:

- to protect the privacy of telecommunications by criminalising the interception or accessing of communications; and
- to enable law enforcement, anti-corruption and national security agencies to investigate serious wrongdoing by allowing those agencies to apply for warrants to intercept communications when investigating serious crimes and threats to national security.⁴

2.3 The objectives of the TIA Act remain largely the same as those in the 1960 legislation.⁵ Of course, the TIA Act dates well before the age of the internet, and

1 <http://www.comlaw.gov.au/Details/C1960A00027> (accessed 3 July 2014).

2 <http://www.comlaw.gov.au/Details/C1960A00027> (accessed 3 July 2014).

3 At the time that the Act was amended to change its name, it was also amended to implement a number of the recommendations of the Report of the Review of the Regulation of Access to Communications (the Blunn Report) which had concluded: '[T]here was inadequate regulation of access to stored communications, as well as insufficient protection of privacy during the access, storage, and disposal processes of stored communications [and that] the distribution of provisions between the Telecommunications Act and the Telecommunications (Interception) Act (as it was then known) dealing with access to telecommunications data security was complicated, confusing and dysfunctional'. See: ALRC, *For Your Information: Australian Privacy Law and Practice*, 2008, pp. 2478–2479.

4 Attorney-General's Department, *Submission 26*, pp 3–4.

5 Section 5 of the *Telephonic Communications (Interception) Act 1960* provided that telephone communications were not to be intercepted, the exception being by ASIO where the interception was in connection with the performance by ASIO 'of its functions or otherwise for the security of the Commonwealth'.

although written with the aim of remaining 'technology neutral', evidence taken by the committee indicated that it has failed to keep pace.

Support for reform

2.4 Although those who gave evidence during this inquiry had different views on how reform should progress, there was universal support for urgent reform of the telecommunications legislation.

Law enforcement and national security agencies

2.5 The committee heard that all law enforcement and national security agencies agreed that the current TIA Act was at risk of becoming ineffective without reform. For example, the Australian Crime Commission (ACC) advised the committee that advancements in technology and security had 'diminished the authority initially issued by Parliament in 1979 in relation to interception'. As a result, according to the ACC there is:

...a compelling need to modernise the TIA Act to ensure provisions keep pace with changes in technology...Because of changes in technology, the ACC is hindered in its investigation of serious and organised crime due to the restrictions on its ability to collect and share material obtained under the TIA Act.⁶

2.6 The ACC explained that, in its view, the TIA Act 'must be capable of overcoming technological advances which are deliberately used to prevent law enforcement from lawfully intercepting and accessing communications'.⁷

2.7 Similarly, the Australian Security Intelligence Organisation (ASIO) advised the committee that without modernisation not only will there be 'detrimental consequences' for Australia's national security and law enforcement capacities, but also for individual privacy.⁸

2.8 The Australian Federal Police (AFP) emphasised to the committee that the need for comprehensive reform to 'avoid further degradation of existing capability whilst ensuring transparency' was 'becoming increasingly pressing'.⁹

2.9 In addition to these Commonwealth agencies, state and territory law enforcement agencies also supported reform. For example, Victoria Police expressed the view that 'holistic reform of the TIA Act' was urgently needed 'if law enforcement agencies [were] to maintain an adequate investigative capability'.¹⁰ The Western Australian Police argued that the current legislative framework was 'not sufficient to adequately deal with technological change, and the attempt to address such

6 Australian Crime Commission, *Submission 23*, pp 3–6.

7 Australian Crime Commission, *Submission 23*, pp 3–6.

8 Australian Security Intelligence Organisation, *Submission 27*, p. 4.

9 Australian Federal Police, *Submission 25*, p. 3.

10 Victoria Police, *Submission 6*, p. 1.

advancements [through constant legislative amendments had] resulted in a complicated regime'.¹¹

Civil liberty and rule of law stakeholders

2.10 Support for reform was also expressed by stakeholder organisations that seek to promote and protect the right to privacy and the rule of law. For example, the Law Council of Australia (Law Council) gave its 'general support' for a comprehensive review that considered:

...how this legislation fits within the broader surveillance and interception legislative regime; whether the TIA Act can and should respond to emerging technological developments; and what safeguards and other provisions should be included in the TIA Act to ensure that it does not unduly burden individual rights, including the right to privacy.¹²

2.11 ThoughtWorks Australia also supported review. It observed that, as the TIA Act had 'been amended more than 45 times since September 2001, [it] requires an overhaul to bring it into the digital age, to properly integrate Australia's National Privacy Principles, and to uphold...[Australia's] obligations under international human rights law'.¹³

2.12 Blueprint for Free Speech similarly noted that it would be 'prudent to modernise the legislation to account for new technology and new challenges faced in gathering evidence for criminal investigations'.¹⁴

Approach to reform

2.13 The findings of the ALRC and PJCIS reports and evidence received throughout the inquiry indicate that legislative reform must seek to achieve administrative efficiencies, remain technology neutral and maintain adequate oversight and privacy protections. The then Secretary of the Attorney-General's department expressed this approach to reform succinctly:

The key driver for reform is the need to create a privacy and access regime that is fit for the modern telecommunications environment and that can withstand rapid technological change into the future...[R]eform of the TIA Act...also represent[s] an opportunity to modernise and strengthen protections afforded to Australian telecommunications, limit the range of agencies in accessing telecommunications data while also introducing

11 Western Australian Police, *Submission 20*, p. 4. Northern Territory (NT) Police also expressed support for reform of the TIA to 'provide greater simplicity, clarity and efficiency of operations under those acts'. See: NT Police, *Submission 21*, p. 10.

12 Law Council of Australia, *Submission 34*, p. 4.

13 ThoughtWorks Australia, *Submission 5*, p. [2]. The Australian Privacy Foundation (APF), made similar comments, stating its support for a holistic review to consider the cumulative effect of the many marginal changes over time. See: Mr Nigel Waters, Australian Privacy Foundation, Committee Hansard, 29 July 2014, p. 30.

14 Blueprint for Free Speech, *Submission 4*, p. 15.

stronger oversight mechanisms and improv[ing] the effectiveness and efficiency of the current accountability and reporting regimes.¹⁵

2.14 The department suggested that although the 'basic values underpinning the Act are probably sound and do not require revision or amendment':

[T]he law requires agencies and other users to navigate an incredibly complex modern communications environment using powers and procedures designed in the 1970s...The antiquated nature of the Act presents real and very pressing challenges for these agencies...The privacy protections and the oversight regimes established by the Act are in better shape, but even these protections are fragmented and, in places, internally inconsistent after 35 years of ad hoc amendment.¹⁶

2.15 This approach to reform was consistent with views expressed by the technology industry—the Internet Society of Australia (ISOC-AU) submitted that:

[A]ny legislative changes should adopt a technology neutral, principles based approach that would better withstand technological change and couple that with preservation of fundamental citizen rights. At least, any changes to the legislation should avoid wherever possible being unduly technology specific, as that obviously leads to endless amounts of specification that would need to be adjusted on a continuing basis.¹⁷

Balancing the right to privacy and national interests

2.16 Any programme of reform must balance individual and national interests with sensitivity and maturity. The need for balance was clearly expressed by the Australian Law Reform Commission (ALRC) following its 2006-8 review of the *Privacy Act 1988* (Cth):

As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. International instruments on human rights and growing international and domestic jurisprudence in this field all recognise that privacy protection is not an absolute. Where circumstances require, the vindication of individual rights must be balanced carefully against other competing rights.¹⁸

2.17 Although the view that the need for urgent reform of the telecommunications legislation was universal, the objective of protecting privacy was not diminished. The

15 Mr Roger Wilkins AO, Secretary, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 2.

16 Mr Roger Wilkins AO, Secretary, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 2.

17 Ms Narelle Clark, President, Internet Society of Australia (ISOC-AU), *Committee Hansard*, 23 April 2014, p. 32.

18 *For Your Information – Australian Privacy Law and Practice*, Australian Law Reform Commission (ALRC) Report #108, p. 104.

evidence received by the committee emphasised that the right to access telecommunications information should only be exercised when both proportionate and appropriate. For example, the Law Council explained:

...where a State seeks to restrict human rights, such as the right to privacy, for legitimate and defined purposes, for example in the context of telecommunications access and interception, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective.

In the context of telecommunications access and interception, this involves balancing the intrusiveness of the interference, against operational needs. Interception of, or access to communications, will not be proportionate if it is excessive in the circumstances or if the information sought could reasonably be obtained by other means.¹⁹

19 Law Council of Australia, *Submission 34*, p. 5.

Chapter 3

Warranted access to telecommunication content

3.1 The *Telecommunications (Interception and Access) Act 1979* (TIA Act) provides a legislative framework that criminalises the interception and accessing of telecommunications. However, the Act prescribes exceptions that enable law enforcement, anti-corruption and national security agencies to apply for warrants to intercept communications when investigating serious crimes and threats to national security. The warrant regime provides these agencies with lawful access to telecommunications content.

3.2 This chapter provides an overview of the existing warrant framework within the TIA Act and then discusses opportunities for legislative reform. The overview provides an insight into the complexity of the current legislation.

3.3 In examining the warranted access regime to telecommunications content, the committee was informed by the 2013 report of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) which recommended that the proportionality test within the TIA Act be revised and consideration be given to implementing a consistent proportionality test across interception and access to telecommunications content. The committee was also informed by the 2015 report of the PJCIS into mandatory data retention that re-considered the issue of proportionality in context of necessity, efficacy and the current risk environment.¹

An overview of the warrant regime

3.4 Chapters 2 and 3 of the TIA Act² provide for warranted access to telecommunications, including both communications passing across telecommunications services (that is, the interception of live communications), and stored telecommunications content.³

3.5 The Attorney-General's Department (the department) provided the following description of the four existing warrant regimes that enable law enforcement and anti-corruption agencies to lawfully access the content of communications:

1 PJCIS data retention report, paragraph 2.102, p. 37.

2 The TIA Act is comprised of five chapters.

3 The process which the Australian Security and Intelligence Organisation (ASIO) is required to follow for warrants, differs to those for anti-corruption agencies and law enforcement agencies and has not been specifically addressed in the body of the report. The sections relevant to ASIO are sections 9, 9A and section 109 of the TIA Act. By way of example, where ASIO has applied to the Attorney-General for a warrant under section 9 of the Act, the Attorney-General may issue a warrant where satisfied that the telecommunication service is being used, or is likely to be used in 'activities prejudicial to security' and interception will, or is likely to, assist the organisation in carry out its functions. 'Activities prejudicial to security' is defined in section 4 of the *Australian Security Intelligence Organisation Act 1979*.

The TIA Act contains four warrant regimes for lawful access to the content of communications by law enforcement and anti-corruption agencies. Three of these warrants relate to access to 'live' communications, and the fourth relates to access to 'stored' communications held by carriers.

The distinction between access to live and stored communications currently embodied in the TIA Act is based on an assumption that stored communications were generally more 'considered' and so less privacy sensitive.⁴

3.6 In addition, the Act provides for warrants to be issued for specific purposes, such as locating missing persons or locating a caller in an emergency.

Telecommunications service warrants and named person warrants

3.7 The provisions within Chapter 2 of the TIA Act enable 'agencies' to apply for telecommunications service warrants and named person warrants to an eligible judge or nominated member of the Administrative Appeals Tribunal (AAT). The Act prescribes that the judge or nominated member of the AAT may issue a warrant in the circumstances where they are satisfied that the information likely to be obtained under the warrant would be likely to assist in the investigation of a 'serious offence' and they have had regard to a number of factors to ensure that the issuing of a warrant is proportionate in the circumstances.⁵ This is referred to as a proportionality test.

3.8 For the purposes of Chapter 2 of the TIA Act, 'agencies' is defined as 'interception agencies' which is further defined as the Australian Federal Police (AFP), the Australian Crime Commission (ACC) or the Australian Commission for Law Enforcement Integrity (ACLEI); or an eligible authority of a state in relation to which a ministerial declaration under section 34 is in force. Section 34 of the TIA Act enables the Minister, by legislative instrument, at the request of the Premier of a State, to declare an 'eligible authority' of that State to be an 'agency' for the purposes of the Act. The Act defines an 'eligible authority' in relation to a state to mean:

- in any case—the police force of that state; or
- in the case of New South Wales—the Crime Commission, the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the Police Integrity Commission or the Inspector of the Police Integrity Commission; or
- in the case of Victoria—the Independent Broad-based Anti-Corruption Commission (IBAC) or the Victorian Inspectorate; or
- in the case of Queensland—the Crime and Misconduct Commission; or
- in the case of Western Australia—the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission; or

4 Attorney-General's Department, *Submission 26*, p. 17.

5 See sections 46 and 46A of the TIA Act which set out the factors to which the Judge or AAT member must have regard when considering an application for a telecommunications service interception warrant or a named person warrant.

- in the case of South Australia—the Independent Commissioner Against Corruption.

3.9 'Serious offence' is defined in section 5D of the TIA Act. The definition is complex but includes, among other things, murder, kidnapping, bribery, market misconduct and other offences that are punishable by imprisonment for life or for a period, or maximum period, of at least seven years.

Stored telecommunications warrants

3.10 In certain circumstances, 'enforcement agencies' (defined below) can require that a carrier preserve all stored communications the carrier holds that relate to the person or telecommunications service specified in a notice.⁶ The communications stored may then be accessed, by warrant, in prescribed circumstances.⁷ Like telecommunications service warrants, a proportionality test is also applied. The proportionality test applied in this circumstance involves 'serious contravention'.

3.11 Where an 'enforcement agency' has applied to an 'issuing authority' (defined below) for a stored telecommunications warrant, the TIA Act provides that the 'issuing authority' may issue the warrant if satisfied that the information likely to be obtained under the warrant would be likely to assist in the investigation of a 'serious contravention' and the 'issuing authority' has had regard to a number of matters to ensure that the issuing of a warrant is proportionate in the circumstances.⁸

3.12 'Enforcement agency' is defined in section 5 of the TIA Act. The definition includes: the AFP, a police force of a state, anti-corruption bodies, the ACLEI, the ACC, authorities prescribed by legislation, and, 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.

3.13 'Issuing authority' is defined in section 5 of the Act as 'a person in respect of whom an appointment is in force under section 6DB'.⁹ Certain judges, magistrates and AAT members who are also enrolled as legal practitioners may be appointed by the Minister to be an 'issuing authority'.¹⁰

3.14 'Serious contravention' is defined in section 5E of the TIA Act. Like the definition of 'serious offence' in section 5D of the Act, the definition of 'serious contravention' in section 5E is complex. It includes a Commonwealth, state or territory offence punishable by imprisonment for a period, or a maximum period, of at least three years. The definition also includes offences punishable by a maximum fine

6 The legislative framework governing stored telecommunications warrants is set out in Chapter 3 of the TIA Act.

7 See Chapter 3 of the TIA Act.

8 Subsection 116(2) of the TIA Act sets out the matters to which the issuing authority must have regard when considering an application for a stored communications warrant.

9 This definition presents particular issues in relation to access to telecommunications data which are examined in Part II of this report.

10 Sections 5, 5E and 6DB, TIA Act.

of at least 180 penalty units¹¹ or a contravention of the law which would make an individual liable to pay a pecuniary penalty of the same magnitude.

Removing legislative duplication in the warrant regime

3.15 Throughout this inquiry the committee received evidence regarding the complexity of the existing legislative framework that governs warranted access to telecommunications content.¹² Stakeholders consistently impressed upon the committee the need to remove legislative duplication from the warrant framework. Many proposed the introduction of a single warrant regime that authorised interception of content, whether live or stored, on the basis of prescribed attributes. This is referred to as 'attribute-based interception'. Proponents of this approach argued that it would reduce complexity by removing the distinction between a 'serious offence' and a 'serious contravention' while also providing a single clear proportionality test.¹³

3.16 Submitters identified an administrative burden associated with the complex duplication within the existing TIA Act. The then Director-General of Security explained:

[I]n order to look at a particular individual we may need to take out three or four different warrants, each of which requires a considered three- or four-page argument, and yet the argument is actually the same in all of the warrants. So to be able to combine a number of warranted activities together...is one such example. The ability to intercept according to a number of different selectors, rather than just the name of a person and a telephone number, for example, to be able to intercept on the basis of other attributes—call areas, time or whatever—would be a great help. It does not in any way change the level of intrusiveness but it simply makes the bureaucratic processes a lot simpler.¹⁴

3.17 ASIO noted however, that there would be instances where legislative duplication would remain both necessary and appropriate:

Over time, the many amendments to the TIA Act have resulted in duplication and complexity making the Act difficult to understand and apply. Conversely, there is intentional duplication for provisions that apply specifically to ASIO with separate provisions for enforcement agencies. For example, voluntary disclosure provisions for ASIO are covered under

11 One penalty unit is currently \$170.

12 Among others, the following organisations cited support for removal of legislative duplication: Victoria Police, *Submission 6*, p. 2; Western Australian Corruption and Crime Commission, *Submission 14*, p. 16; Northern Territory Police, *Submission 21*, p. 8; and New South Wales Government, *Submission 30*, p. 13.

13 These same matters were canvassed by the PJCIS throughout its inquiry which reported in June 2013 (see that committee's recommendations 6, 7 and 10) and are discussed further at paragraphs 3.27 and 3.28 of this chapter.

14 Mr David Irvine, Director-General of Security, Australian Security Intelligence Organisation (ASIO), *Committee Hansard*, 21 July 2014, p. 7.

section 174 whereas section 177 relate[s] to enforcement agencies. ASIO supports the recommendation to remove legislative duplication but notes it should not be applied in instances where there is a necessary distinction between ASIO's security intelligence role and law enforcement agencies.¹⁵

3.18 The Australian Federal Police (AFP) stated that in its view, '[r]emoving duplicative processes and complexity within the TIA Act [would] simplify the processes for agencies and may assist in achieving transparency by removing legislative intricacy'.¹⁶ The Australian Mobile Telecommunications Association (AMTA) and the Communications Alliance similarly supported removing legislative duplication; these organisations added that legislative duplication between the TIA Act and the *Telecommunications Act 1997* (Telecommunications Act) should also be considered.¹⁷

3.19 Although many submitters were strongly supportive of a single warrant regime, the Law Council of Australia (Law Council) cautioned that it would be important not to introduce such a regime at the expense of privacy safeguards:

The Law Council supports the removal of legislative duplication but not where this involves a single warrant regime which would make it difficult for issuing authorities to adequately assess the privacy impacts of the powers under the warrant. Given the particularly intrusive nature of telecommunications interception, legislative clarity must not be achieved to the detriment of privacy principles.¹⁸

A single attribute-based interception regime

3.20 The department explained that under the existing provisions of the TIA Act, warrants issued may only authorise the interception of 'services' or 'devices'—such as a particular internet connection or telephone:

The service or device identifiers are the technical means that the telecommunications industry uses to identify the communications for retrieval under a warrant. This approach is technologically-specific and reflects historic assumptions about how telecommunications operate. The diversification of the telecommunications industry, changing communications habits and changes to the technical operation of modern telecommunications networks mean that new ways of identifying communications are both available and required.¹⁹

3.21 The department stated that in its view '[w]ithout reform, technological change will make the current, service and device-based provisions obsolete'.²⁰ The department

15 ASIO, *Submission 27*, p. 34.

16 Australian Federal Police, *Submission 25*, Attachment E, p. 5.

17 Australian Mobile Telecommunications Association and Communications Alliance, *Submission 16*, pp 7–8.

18 Law Council of Australia, *Submission 34*, pp 39–40.

19 Attorney-General's Department, *Submission 26*, p. 17.

20 Attorney-General's Department, *Submission 26*, p. 17.

recommended the single attribute-based warrant regime as a more targeted and technologically-neutral approach:

[T]he reality is that this Act was very cleverly drafted in 1979 in that it was technologically neutral and it has been able to capture all communications as they have come along, without any need to consider the implications of that technology. The reality now is that people communicate with very smart phones...and they do allow you to communicate in many, many ways with one device. The Act really is just saying that law enforcement can intercept that device without any approach that allows you to target the kind of information that you want.

What the Act does not do at the moment is have any real way to define what kind of information should be collected by law enforcement for them to investigate crimes. What the Act currently says is you can collect evidence; however, you must do it in a very broad, crude way.²¹

3.22 The department explained that it was advocating for a change in the legislation to a single attribute-based warrant regime as such a regime would:

- better protect the privacy of communications 'because law enforcement and national security agencies [would] have to determine the kind of communications they want to collect'; and
- allow telecommunications providers 'to target a stream of traffic rather than volumes of traffic'.²²

3.23 ASIO echoed these views. According to ASIO, the TIA Act, as currently written, 'limits the technical means by which agencies can conduct interception by requiring interception be based on either a "service" identifier (for example, a telephone number or email address) or a piece of "equipment" (for example, a mobile telephone handset)'.²³ ASIO advocated the 'decoupling' of the techniques for interception from the authorisation to intercept and expressed its support for attribute-based interception:

"Attributes" are specific identifying characteristics that can be used in combination to identify unique communications of interest to ASIO. Attribute-based interception encompasses service-based or equipment-based interception. It also allows ASIO to target specific attributes to collect communications of interest more effectively and less intrusively.²⁴

3.24 ASIO provided some examples of attributes that could be used:

- ...some individual attributes that could be combined to enable better interception targeting could include:

21 Ms Katherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, *Proof Committee Hansard*, 22 April 2014, p. 3.

22 Ms Katherine Smith, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 3.

23 ASIO, *Submission 27*, p. 33.

24 ASIO, *Submission 27*, p. 33.

-
- the source and/or destination of the communication;
 - the type of communication (for example, a video call, email, SMS);
 - the equipment being used to convey the communication (for example mobile telephone handset, cell tower);
 - any identifier being used in connection with the communication (such as a number or username);
 - a time period in which a communication is made or received; or
 - the location of the person making or receiving the communication.

3.25 The selection of a combination of attributes in each particular case would involve a number of considerations, including the extent to which:

- the telecommunications provider had the ability to intercept the chosen attributes;
- attributes (singly or in combination) were sufficiently precise to give a high degree of certainty communications of interest are accessed; and
- certain components of a communication could be excluded on the basis they were likely to be irrelevant.²⁵

3.26 In ASIO's view the approach of 'attribute-based interception':

...would allow agencies to filter and limit the communications they intercept more efficiently, helping to minimise the collection of extraneous information. With this more specific method of targeting the telecommunications of interest, the more certain we can be that we are excluding from incidental interception the communications of persons who are not of interest and whose privacy should be protected.²⁶

3.27 In its 2013 report, the PJCIS observed that advancements in telecommunications technology were diminishing the effectiveness of the current interception framework. As a result, the PJCIS recommended that the interception of communications should be conducted on the basis of specific attributes of communications as a means of 'arresting the decline of interception capability, while also offering additional privacy protections by better targeting communications which are of particular relevance to the serious crime or national security threat which is being investigated'.²⁷

3.28 Submitters to this inquiry cited the PJCIS's recommendation of a single warrant regime and suggested that the introduction of such a regime would be a means by which telecommunications interception legislation could be simplified and also

25 ASIO, *Submission 27*, p. 33.

26 ASIO, *Submission 27*, p. 33.

27 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 34.

respond to advancements in technology. The ACC and AFP also expressed support for a single attribute-based interception regime.²⁸

How would it work?

3.29 The department explained how it anticipated 'attribute-based' interception would apply in practice. A warrant would still need to be issued to authorise access to a particular person's communications but, according to the department, that 'attribute-based' warrant:

...would describe the communications that the service provider is to access and provide to the agency by using a combination of technical features or 'attributes'—rather than just a service or device identifier. Those attributes could include a specific account, a time of day, a geographic location or a technical feature of the communication.²⁹

3.30 The department explained that, in its view, attribute-based interception would enable warrants to be more targeted and would also minimise the lawful collection of irrelevant communications.

Concerns raised in relation to attribute-based interception

3.31 Although there was wide-spread support for the introduction of an attribute-based interception warrant regime throughout the law enforcement community, some concern was expressed by other stakeholders.

3.32 The Law Council advised that its reservations in relation to attribute-based interception are based on the view that 'attribute-based' has not been sufficiently defined to allow the 'true privacy implications' associated with such a model to be assessed.³⁰

3.33 In raising its objections, the Law Council noted the challenges that 'existing and emerging telecommunications technologies pose for agencies attempting to accurately identify the communications they intend to intercept or access',³¹ and went on to express general support for:

...efforts to develop a warrant regime that focuses on better targeting the characteristics of a communication and enables it to be isolated from communications that are not of interest. However, the Law Council is keen to ensure this does not occur at the expense of specific provisions designed to ensure that each particular device or service to be intercepted or communication to be accessed is clearly identified and shown to be justifiable and necessary, and that it occurs in a manner that has the least intrusive impact on individual rights and privacy.³²

28 See: ACC, *Submission 23*, Attachment A, p. [3] and AFP, *Submission 25*, Attachment E, p. 4.

29 Attorney-General's Department, *Submission 26*, p. 18.

30 Law Council of Australia, *Submission 34*, pp 33–34.

31 Law Council of Australia, *Submission 34*, pp 33–34.

32 Law Council of Australia, *Submission 34*, pp 33–34. This view was shared by AMTA and the Communications Alliance. See: *Submission 16*, p. 6.

3.34 The department explained to the committee that a single attribute-based warrant would enable more targeted interception and, therefore, provide a higher level of privacy protection. To demonstrate this, the department noted how the current framework provides for a law enforcement agency to intercept a device without any approach to targeting the kind of information wanted:

[For example] [a]t the moment, a service warrant would allow you to collect against a particular service. If it is Joe Bloggs's smart phone, that actually is the service, and everything that sits on that smart phone—every bit of content, whether it be Candy Crush, Skype or their email—that service is all of that, and the warrant does not have the specificity at the moment to say, "Actually, we don't want their livestreaming of the cricket; we just want the particular communication".

...

The problem at the moment is that the warrant is quite broad in its approach, and what we want to do is have much better specificity. It may be that they will collect the voice, the email and the livestream of the cricket, but we want to be able to identify those as attributes of the whole communication channel rather than just saying, "Give it all to us, and we'll decipher it later".³³

3.35 In expressing support for the introduction of a single attribute-based warrant regime both ASIO and the ACC acknowledged the need to ensure the maintenance of 'the proportionality thresholds and accountability requirements...to deliver public confidence and assurance regarding the use of these powers'³⁴ in any new regime.

Senator Scott Ludlam Inquiry Chair

33 Ms Katherine Smith, Attorney-General's Department, *Committee Hansard*, 22 April 2014, p. 3.

34 ASIO, *Submission 27*, p. 35. See also: ACC, *Submission 23*, Attachment A, p. [6].

Chair's Minority Additional Comments

Access to telecommunications data

1.1 In addition to a regime that allows for warranted access to telecommunications content (as discussed in Chapter 3), the *Telecommunications (Interception and Access) Act 1979* (TIA Act) also provides for agencies to access telecommunications data (metadata). A key difference between the regimes is that access to this data does not require a warrant; instead an 'authorised officer' (defined below) within an 'enforcement agency' can authorise access.¹ In considering whether or not to grant an authorisation, an 'authorised officer' is required by law to give consideration to privacy.

1.2 These additional comments discuss the ability of 'enforcement agencies' to access telecommunications data via authorisation and considers whether there is a need for change. The terms 'telecommunications data' and 'metadata' are used interchangeably.

An overview of the telecommunications data access regime

1.3 Part 13 of the *Telecommunications Act 1997* (Telecommunications Act) imposes obligations on 'eligible persons' to protect the confidentiality of information relating to the contents of communications and the affairs and personal particulars of other persons.²

1.4 The term 'eligible person' is defined in section 271 of the Telecommunications Act. 'Eligible person' for the purposes of Part 13 of the Telecommunications Act is: a carrier; or a carriage service provider; or an employee of a carrier; or an employee of a carriage service provider; or a telecommunications contractor; or an employee of a telecommunications contractor.

1.5 If these provisions are breached, the 'eligible person' is guilty of an offence. However, the TIA Act sets out circumstances where the relevant sections in Part 13 of the Telecommunications Act³ will not prohibit the disclosure of information or a document.⁴ These circumstances are set out in Division 3 (in relation to ASIO), Division 4 (in relation to 'enforcement agencies') and Division 4A (in relation to foreign law enforcement) of Chapter 4 of the TIA Act.

1 'Enforcement agency' is defined in section 5 of the TIA Act. Notably it includes any body whose functions include: (i) administering a law imposing a pecuniary penalty; or (ii) administering a law relating to the protection of public revenue. See also: paragraph 3.10 of Chapter 3 which sets out the definition.

2 See sections 276, 277 and 278, Telecommunications Act.

3 Sections 276, 277 and 278, Telecommunications Act.

4 However, the TIA Act does not permit the disclosure of this information if it is the contents or substance of a communication, or a document to the extent that the document contains the contents or substance of a communication. See: section 172, TIA Act.

1.6 The Division 4 provisions specify that 'enforcement agencies' can access telecommunications data by prescribing that an 'authorised officer' of an 'enforcement agency' may authorise disclosure of specified information if the disclosure of the information would be 'reasonably necessary' for:

- enforcement of a criminal law;⁵ or
- enforcement of a law imposing a pecuniary penalty or for the protection of public revenue.⁶

1.7 Before making an authorisation under Division 4, the authorised officer is required, by section 180F of the TIA Act, to have regard to:

[W]hether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters: (a) the likely relevance and usefulness of the information or documents; (b) the reason why the disclosure or use concerned is proposed to be authorised.⁷

1.8 As set out in Chapter 3, submitters raised concerns in relation to the standardisation of the proportionality tests used across the TIA Act given that the proportionality test applied in authorising access to telecommunications data is significantly lower than the proportionality test involved in seeking to intercept live communications or access stored content. In the case of content, the proportionality test relates back to serious offence and serious contravention respectively. In the case of authorising access to telecommunications data, a much lower threshold can be established by linking necessity of accessing the information with 'enforcement of a law imposing a pecuniary penalty or for the protection of public revenue'.

What is telecommunications data?

1.9 The term 'telecommunications data', also referred to as metadata, communications data and communications associated data, is not defined in the TIA Act. However, the term is generally accepted as being 'information about the process of a communication, as distinct from its content'.⁸

1.10 The department explained that although 'telecommunications data' is not defined in the Act, the term has 'come to encompass a broad range of different types of information' and that the department uses a working definition.⁹ The working

5 Section 178, TIA Act.

6 Section 179, TIA Act. Division 4 of the TIA Act also provides for authorised officer of the Australian Federal Police or a state police force to authorise disclosure for the purposes of locating missing persons and for an authorised officer of a criminal law enforcement agency to authorise access to prospective information if satisfied that disclosure of the information is reasonably necessary for the investigation of: a serious offence; or an offence against the Commonwealth, a state or territory law punishable by imprisonment for at least three years.

7 Section 180F, TIA Act.

8 Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 Annual Report 2012-13*, p. 44.

9 Attorney-General's Department, *Submission 26*, p. 21.

definition is: information or documents that are not the content of a communication, and includes the following types of information, which fall into the following two categories and relate to communications for telephones (both fixed and mobile) and the internet:

- Information that allows a communication to occur:
 - the internet identifier (information that uniquely identifies a person on the internet) assigned to the user by the provider;
 - for mobile service: the number called or texted;
 - the service identifier used to send a communication, for example the customer's email address, phone number or VoIP number;
 - the time and date of a communication;
 - general location information, that is, cell tower; and
 - the duration of the communication.
- Information about the parties to the communications is information about the person who owns the service. This would include:
 - name of the customer;
 - address of the customer;
 - postal address of the customer (if different);
 - billing address of the customer (if different);
 - contact details, mobile number, email address and landline phone number; and
 - same information on recipient party if known by the service provider.¹⁰

1.11 Section 172 of the TIA Act makes it clear that access to telecommunications data is not intended to allow access to the content or substance of a communication. The committee heard, however, that what is now captured as telecommunications data is a far broader subset of information than was captured in 1979. Appendix 4 sets out an example, provided by iiNet Limited, of the telecommunications data that is generated by a website, a Facebook page and a tweet.

1.12 Electronic Frontiers Australia argued that this technological change has altered the nature of metadata to the extent that telecommunications metadata, in many circumstances, is more sensitive than the content of a communication:

In terms of looking at the current context of where we are compared to when this Act was written in 1979, obviously there have been a few changes in the way people communicate...In line with that, we reject pretty strongly the assertion that taking the powers of this Act from 1979, a

¹⁰ Attorney-General's Department, *Submission 26*, p. 46. The department expressly stated that the definition of telecommunications data 'does not include information relating to a person's web browsing or the contents or substance of their communications'. See: *Submission 26*, p. 46.

context where mobile phones did not exist and the internet was still a pipedream, and extending those powers into a context of ubiquitous mobile devices and internet usage is not in any way a logical extension of the law to, as it were, keep up with technology on a like-for-like basis. We strongly believe that in fact this represents a very dramatic escalation of surveillance deep into all aspects of people's lives and goes far beyond anything originally envisaged when this act was drafted.¹¹

1.13 Electronic Frontiers Australia provided the following example of the extent to which the volume of metadata had changed since 1979:

[W]hen this Act was originally drafted, the information that you would get would be the fact that a phone call was made from No. A to No. B at a certain time and lasted a certain duration. That is four pieces of information. As soon as you widen that into a mobile phone context, all of a sudden you have got a location at each point, which is an entirely new thing, where literally people's locations can be tracked. Then, if you go beyond that into non-telephonic communications, all of a sudden the amount of information that has been collected starts to explode. You start to have potentially dozens, if not hundreds, of different points of data that can tell all sorts of things about what is going on. It is really quite a different scale, a different scope, a different context, and it needs to have very different rules.¹²

1.14 The Internet Society of Australia (ISOC-AU) was of a similar view and stated that it could not agree with the argument that metadata is not content:

Over recent times much discussion has also taken place on metadata, with assertions that metadata does not include the content of communication. We contend that, without appropriate technological standards defined by an independent standards body, this claim is inherently untrue. Information gathered by existing mechanisms about the material that transits across an internet network—for example, by using the web page addresses visited by a user—inherently contains specific addresses for many, many elements within the page, even third-party elements in turn requested by the page, such as advertising.

Thus, the amount revealed about an individual, their family, workmates and broader community is potentially very large. In many cases also this data is dynamic and changes from moment to moment, and often today even depends on the types of other sites visited by users, with the advent of cookie correlation—none of which is under any control by the individual users. This is further complicated by the emergence of apps, where users

11 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 35.

12 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 38.

have extremely little knowledge of the level of security or the pervasiveness and the types of actions going on in the background.¹³

1.15 The department acknowledged that changes in technology did have implications for identifying the distinction between telecommunications data and content:

At times, the distinction between 'telecommunications data' and 'content of a communication' may become less clear. This is particularly the case for information that, while not obviously the 'substance' of a communication, could contain or reveal substantive information, such as:

- email subject lines—subject lines can be used to convey the substance of a communication, and
- Uniform Resource Locators (URLs)—the details of which web page a person visited can reveal the content that a person accessed.¹⁴

1.16 The department informed the committee that in situations where it is unclear, its advice to agencies, industry participants and the public, has been that:

[A]ny information that contains or reveals the content of a communication is protected by the prohibitions on interception and access to content under sections 7 and 108 of the TIA Act.¹⁵

Using telecommunications data

1.17 As set out in Division 4 of Chapter 4 of the TIA Act, access to telecommunications data by authorisation is intended to be used when disclosure is considered reasonably necessary for the enforcement of a criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.

1.18 Throughout its inquiry, the committee heard that the use of telecommunications data by law enforcement agencies is often vital in subsequently establishing the grounds for obtaining access to the content of a communication, via warrant, pursuant to Chapter 2 or 3 of the TIA Act. For example, the Australian Commission for Law Enforcement Integrity (ACLEI), explained the usefulness of metadata in the early stages of an investigation:

I would like to emphasise the importance of access to data at the preliminary stages of an investigation. Investigations such as Operation Heritage seek to uncover the full extent of a corrupt network, but often start with only snippets of information or credible allegations. Data about who a person of interest is talking to is often a critical first step that provides a foundation for further investigation including, at a much later stage, seeking

13 Ms Narelle Clark, President, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 32. ThoughtWorks expressed similar views explaining that technology has changed communications such that 'really there is no distinction between metadata and content'. See, Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 4.

14 Attorney-General's Department, *Submission 26*, p. 45.

15 Attorney-General's Department, *Submission 26*, p. 45. Sections 9 and 108 of the TIA Act prohibit access to communications and therefore access would require a warrant.

a warrant for interception. It also allows us to rule out at an early stage people who are unlikely to be complicit, thereby preventing the need for unnecessary investigation and deeper intrusion of privacy.¹⁶

1.19 Queensland Police expressed a similar view regarding the utility of telecommunications data:

The warrantless data we capture regularly is used to in order to assist you reaching the threshold to obtain the warrant, so in nearly all cases you would be using the warrantless information to assist you to gather the information which aided you to reach the threshold you needed to obtain the warrant for telephone interception. That is one of its most common uses. Obtaining data from your phone that is able to tell us about connections between people at different times, aids in painting the picture which, added with other intelligence and evidence, raises you to the threshold of being able to obtain a warrant. That is one of those distinctions I think we need to make between the warrantless and warrant based processes.¹⁷

1.20 The Board of the ACC similarly described to the committee how, in its view, accessing telecommunications data without a warrant enables law enforcement agencies to only seek access to content (via a warrant) where necessary:

[W]hat [telecommunications data] often does is confirm someone's involvement in crime. After that confirmation we often go to the next level, which is obtaining a warrant et cetera for content. So at a fundamental level what it often does for us is confirm that a person is involved with a group of people who are committing, for example, organised crime. Then we build on that as far as obtaining a warrant for content down the track. Fundamentally what it is used for is that confirmation of involvement. I think it was mentioned by one of my colleagues that it should not be underestimated how many citizens are excluded from ongoing intrusive law enforcement interests because of that fundamental check. It [is] still sensitive information—there is no question about that—but we do exclude a considerable number of people in that first-step process.¹⁸

1.21 The Board of the ACC emphasised that it understood the need to protect metadata and expressed its view that this data, although not content, is by no means 'innocuous':

We do not believe that this is innocuous. We accept that you can build a picture. What we are saying is that it is a building block in many ways for further, more intrusive powers which are, quite appropriately, warranted. It

16 Mr Philip Moss, Integrity Commissioner, Australian Commission for Law Enforcement Integrity, *Committee Hansard*, 23 April 2014, p. 6.

17 Assistant Commissioner Peter Crawford, Queensland Police Force, *Committee Hansard*, 22 April 2014, p. 15.

18 Mr Paul Jevtovic APM, Acting Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 22 April 2014, p. 16.

is not open for us to access that information without thresholds having been crossed. They are not inconsiderable thresholds that we have to cross.¹⁹

1.22 A similar view was expressed by Mr Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra. Mr MacGibbon, a former federal agent with the AFP:

...impress[ed] upon the committee the extreme and extraordinary importance of metadata to assist law enforcement investigations. However, anyone who accesses metadata from a law enforcement point of view understands the gravity and the granularity of the information that is provided.²⁰

1.23 The department explained to the committee that telecommunications data has a 'set of irreplaceable characteristics that often make it the most appropriate tool for agencies'. The department identified these characteristics as being:

- it is low risk—unlike the use of undercover officers, informants or physical surveillance, agencies can obtain valuable information without placing their officers, agents or operations at risk
- it is less resource intensive—many other investigative techniques would require agencies to deploy teams of specialist officers to obtain basic information about a target and their associates; lawful access to telecommunications data allows agencies to prioritise the use of these scarce resources for the most critical investigations, and
- it is less privacy intrusive—telecommunications data allows agencies to obtain factual information about communications, such as with whom, when and where a person was communicating, which is useful at the early stages of an investigation. However, as telecommunications data does not include the content of a communication it does not disclose more sensitive information about a person's motivations or intentions, such as what a person was talking about or why they were communicating.²¹

Growth in access to telecommunications data

1.24 Throughout the inquiry, the committee received evidence from submitters critical of the growing number of authorisations being issued to 'enforcement agencies'

19 Acting Commissioner Andrew Colvin, Australian Federal Police, *Committee Hansard*, 22 April 2014, p. 15.

20 Mr Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra, *Committee Hansard*, 26 September 2014, p. 26.

21 Attorney General's Department, *Submission 26*, p. 22. The department also explained that in the case of cybercrime investigations—such as, online fraud, identity theft and child exploitation investigations—law enforcement agencies rely heavily on telecommunications data. Cybercrime includes: crimes where computers or other communications technologies are integral to the offence, such as online fraud, identity theft and the distribution of child exploitation material, and crimes targeting computers, such as hacking or unauthorised access to data. See: *Submission 26*, p. 22.

for access to telecommunications data. Illustrating the extent of the use of authorisations, for the 2012-13 financial year the department reported that:

- law enforcement agencies²² authorised access to telecommunications data in 312,929 cases;
- Commonwealth enforcement agencies²³ made 6,254 authorisations for access to telecommunications data; and
- state and territory enforcement agencies²⁴ authorised access to telecommunications data on 691 occasions.²⁵

1.25 Given the growth in access to metadata the view that all telecommunications data should be accessed by warrant, making access subject to independent judicial oversight (for example, a judge or nominated Administrative Appeals Tribunal (AAT) member), was considered throughout the inquiry.²⁶

1.26 In response to this suggestion the department stated it considered:

...that a more holistic approach, including limiting the range of agencies permitted to access traffic data and requiring such access to be subject to independent oversight...would enable Parliament to strengthen the existing regime without degrading agencies' capabilities or imposing a disproportionate burden on agencies and issuing authorities.²⁷

-
- 22 Law enforcement agencies that accessed telecommunications data by authorisation in 2012-13 included (but is not limited to): the Australian Federal Police (AFP), Tasmanian Police, NSW Police, South Australia Police, Northern Territory Police, Victoria Police, Western Australia Police, the Australian Crime Commission, and the Australian Commission for Law Enforcement Integrity. See: p. 47
<http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf> (accessed 9 August 2014).
- 23 Some of the Commonwealth enforcement agencies that accessed telecommunications data by authorisation in 2012-13 included: the Australian Competition and Consumer Commission, Australian Securities and Investments Commission, Australian Taxation Office, Customs, Department of Health, and the Insolvency and Trustee Service of Australia (now known as the Australian Financial Security Authority). See:
<http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf> (accessed 9 August 2014).
- 24 Among the state and territory enforcement agencies that accessed telecommunications data by authorisation in 2012-13 were the Victorian Department of Environment and Primary Industries, Worksafe Victoria, RSPCA (Victoria), RSPCA (Queensland), Bankstown City Council, Corrective Services NSW and the Western Australia Department of Commerce. See:
<http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf> (accessed 9 August 2014).
- 25 <http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf> (accessed 9 August 2014). See: pp. 47–48.
- 26 See: Australian Privacy Foundation, *Submission 36*, pp. 5, 9; ThoughtWorks Australia, *Submission 5*, p. [2]; The Pirate Party, *Submission 10*, pp. 5–7.
- 27 Attorney General's Department, *Submission 26*, p. 22.

1.27 The department's suggestion that the threshold for access to telecommunications data be reviewed and some form of independent oversight be introduced into the regime was similar in some respects to recommendation 5 of the PJCIS's June 2013 report.

The need to review the threshold for access to telecommunications data

1.28 In its June 2013 report, the PJCIS recommended that the threshold for access to telecommunications data be reviewed with a 'focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated' as the threshold on which access is allowed.²⁸

1.29 The Corruption and Crime Commission of Western Australia supported this recommendation:

The Commission fully supports Recommendation 5 and further supports a stronger threshold for access to traffic data as opposed to a lower threshold for access to subscriber data. The Commission considers this will strengthen the privacy protections within the TIA Act.²⁹

1.30 Electronic Frontiers Australia suggested that thresholds for access to telecommunications data 'should be set taking into account the principle of proportionality' and:

...ensure that access is only available in relation to a reasonably serious offence—for example, a criminal offence attracting a certain maximum term of imprisonment or a civil offence attracting a predetermined minimum penalty—and where there is a reasonable suspicion of the people involved in such an offence.³⁰

1.31 ThoughtWorks Australia similarly argued that 'the number of agencies that can access this data needs to be confined to only those truly undertaking law enforcement and national security activities'.³¹

1.32 In its submission to the inquiry, the department expressed concern with the recommendation of the PJCIS to use 'gravity of conduct' as a threshold for access on the basis that to do so would be inconsistent with Australia's international legal obligations under the Council of Europe's Convention on Cybercrime.³² The department explained that instead of this approach it would prefer the 'imposition of

28 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 26.

29 Corruption and Crime Commission of Western Australia, *Submission 14*, p. 11.

30 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

31 ThoughtWorks Australia, *Submission 5*, p. [2].

32 Attorney General's Department, *Submission 26*, p. 21. The AFP raised similar concerns in relation to the Council of Europe Convention on Cybercrime. See: *Submission 25*, Attachment E, p. 3.

safeguards, including restricting the range of agencies permitted to access such data³³ and that options be explored to:

- create certainty about which agencies are permitted to access account-holder data or traffic data
- ensure that agencies accessing any type of telecommunications data have a demonstrated need to do so, and
- ensure that all agencies with data-access powers are subject to appropriate oversight...³⁴

1.33 The Australian Privacy Commissioner, Mr Timothy Pilgrim, however, in his evidence in respect of the mandatory data retention Bill currently before Parliament noted that if proportionality considerations are not considered in reviewing the threshold for access to telecommunications data, additional safeguards may be required in the legislation:

In my submission, I did not advocate for the imposition of warrants. I took this position on the proviso 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, since 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 investigation of minor offences.³⁵

1.34 Similar concerns were raised by the Parliamentary Joint Committee on Human Rights (PJCHR) during its examination of the Bill and led that committee to recommend that the Bill be amended:

...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...to limit disclosure authorisation for existing data to where it is 'necessary' for the investigation of specific serious crimes, or categories of serious crimes.³⁶

1.35 The committee heard from other stakeholders that were supportive of reviewing the threshold for access to telecommunications data as suggested by the PJCIS. For example, Blueprint for Free Speech expressed its support for a review stating:

33 Attorney General's Department, *Submission 26*, p. 21.

34 Attorney General's Department, *Submission 26*, p. 21.

35 Mr Timothy Pilgrim, Australian Privacy Commissioner, *House of Representatives Committee Hansard*, 29 January 2015, p. 47.

36 Parliamentary Joint Committee on Human Rights, *Fifteenth Report of the 44th Parliament*, pp. 16–17.

...there must be proper public consultation about the detail around which agencies should have continued access to telecommunications data, and...[the] proper description of the basis for this access and the threshold for same. This information should not be concealed from the broader Australian community, and Australians must have a say in this decision process.³⁷

1.36 In addition to calls for a review of the proportionality test involved in authorising access to telecommunications data, submitters also voiced support for refining the definition of 'enforcement agency' to reduce the number of agencies that could access the data without a warrant. For example, the Office of the Public Interest Monitor of Victoria supported calls for a reduction in the number of agencies accessing telecommunications data without a warrant, stating:

There has been recent media attention and significant criticism of the ability of agencies to obtain telecommunications data and the consequential implications on the privacy of those who utilise telecommunications services. Local councils can access telecommunications data under the TIA Act on the basis that disclosure of the said data is reasonably necessary for the enforcement of a law imposing a pecuniary penalty. The matters in respect of which telecommunications data is obtained by some agencies does not appear commensurate with the invasion of privacy occasioned by the disclosure of such data. A reduction in the number of agencies able to access telecommunications data by using the gravity of the conduct which may be investigated utilising telecommunications data as a threshold on which access is allowed is supported.³⁸

1.37 The Australian Mobile Telecommunications Association (AMTA) and the Communications Alliance advised the committee that there was a need for 'clarity around which agencies are eligible to have access to telecommunications data' and that this could result in cost efficiencies for industry.³⁹

1.38 The Internet Society of Australia (ISOC-AU) was of a similar view:

The existing provisions do not make clear which agencies have the right to gain access to metadata. Should metadata be defined then there must be a clear understanding of which agencies are eligible to access communications information, and the proportionality of [the] suspected crime must also be correspondingly high.⁴⁰

1.39 Electronic Frontiers Australia also suggested that the highly invasive nature of this information warranted tighter restrictions to access:

...and, ideally, a clearly defined list of agencies that are able to request access to data. As mentioned, there may be cases where agencies outside that list can apply via an approved agency, as it were, to do that, but we

37 Blueprint for Free Speech, *Submission 4*, pp. 3–4.

38 Office of the Public Interest Monitor Victoria, *Submission 17*, p. 5.

39 AMTA and the Communications Association, *Submission 16*, p. 6.

40 Ms Narelle Clark, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 33.

think that there do need to be some very tight restrictions around that. We also agree that there should be very tight, very stringent and very clearly defined thresholds for access to data.⁴¹

1.40 It is noted that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 which is currently before Parliament, seeks to limit the number of agencies that can access telecommunications data by redefining 'enforcement agency'. The Bill, however, does not address the need to review the proportionality test in respect of accessing telecommunications data.

Introduction of oversight for telecommunications data

1.41 In addition to calls for a review of the threshold for access to telecommunications data, the committee repeatedly heard concerns raised by stakeholders about the lack of oversight and transparency in the telecommunications data access regime.

1.42 Under the existing legislative framework, telecommunications data can be accessed by any agency that meets the definition of 'enforcement agency', (which includes 'a body whose functions include: (i) administering a law imposing a pecuniary penalty; or (ii) administering a law relating to the protection of public revenue'),⁴² where the disclosure is considered reasonably necessary for the enforcement of the law or the protection of public revenue and the authorised officer has had regard to the privacy implications of the disclosure.

1.43 Unlike the warrant regimes of Chapters 2 and 3 of the TIA Act, Chapter 4 of the TIA Act does not contain any legislative framework for direct oversight of the authorisation process. Similarly, the legislation does not require that information accessed must be destroyed when it is no longer necessary, unlike the Act's requirements for content⁴³ and as is required by Australian Privacy Principle (APP) 11.⁴⁴

41 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36. This suggestion was also made by Mr Alastair MacGibbon (see, *Committee Hansard*, 26 September 2014, p. 26) and Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy, Vodafone Hutchison Australia (see, *Committee Hansard*, 26 September 2014, p. 18).

42 Section 5, TIA Act.

43 Section 79 of the TIA Act and section 150 of the TIA Act prescribe that 'restricted records' (any information obtained by interception) and records or information obtained by accessing a stored communication are required to be destroyed if it is no longer likely to be required.

44 Australian Privacy Principle (APP) 11—security of personal information:

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.

1.44 There are reporting requirements for access to data. The TIA Act requires the 'enforcement agency' to keep a record of authorisations and report those to the Minister at the end of each year. Although the number of authorisations is published in an annual report tabled by the Minister, no further detail is provided. As the authorisation process occurs internally within each enforcement agency, there is no external oversight of or transparency about how agencies are complying with the obligations to balance access with privacy.

1.45 The Commonwealth Ombudsman, who has a role in overseeing warranted access to telecommunications content, commented on the lack of oversight of access to telecommunications data. The Ombudsman explained that his office did not have any inspection role in relation to metadata and agreed that the oversight and reporting regime for telecommunications data could be improved. He suggested that there may also be an educational role that his office could play.⁴⁵ The then Secretary of the Attorney-General's Department also explained that in his view there was a need for greater transparency in relation to the authorisation process for accessing telecommunications data.⁴⁶

1.46 The figures outlined at paragraph 4.24 indicate that, if the Commonwealth Ombudsman were to have a role in relation to inspecting access to metadata, his office would face an enormous workload. However, the Ombudsman suggested that the resourcing challenges presented by the number of authorisations for access to metadata that would need inspection could be met by an 'appropriate sampling program':

That would be the normal approach to a volume responsibility along those lines. And then, if we form some views, they would need to be couched in language which said we had done that which we could, in the circumstances with which we are confronted.⁴⁷

1.47 An officer from the Commonwealth Ombudsman added that in addition to a sampling program:

...we would have to look at the risks associated with that inspection regime. It may well be that the most appropriate means would be looking at processes rather than focusing on records per se, so looking at high-level

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 (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. Source: Part 4 of Schedule 1 to the *Privacy Act 1988*.

45 Mr Colin Neave, Commonwealth Ombudsman; Mr Simon Pomery, Assistant Director, Commonwealth Ombudsman, *Committee Hansard*, 23 April 2014, pp. 29–30.

46 Mr Roger Wilkins AO, Secretary, Attorney-General's Department, *Committee Hansard*, 23 April 2014, p. 4.

47 Mr Colin Neave, Commonwealth Ombudsman, *Committee Hansard*, 23 April 2014, p. 29.

processes in combination with doing a sample may alleviate some of the risks that would occur from not looking at a greater number.⁴⁸

1.48 Electronic Frontiers Australia expressed its support for the introduction of a better oversight and reporting regime in relation to access to telecommunications data:

We also support calls for more detailed reporting of access to data...We also see no reason why access to communications data by intelligence agencies should not be reported...at least on a statistical basis. We cannot see any harm in doing that. We agree that there needs to be more effective external and independent oversight of this process. We would also suggest that there need to be very clear rules about what happens to data that has been accessed through this process, how long it is retained by the agencies and how it is disposed of and so forth.⁴⁹

1.49 The Chair notes that the government has proposed changes to the oversight arrangements for accessing telecommunications data by authorisation in the Bill currently before Parliament. This is discussed in more detail later.

Should access to 'telecommunications data' require a warrant?

1.50 It is widely considered that there is a need to review the threshold for access to telecommunications data accessed without a warrant. Some witnesses suggested to the committee that the need for such a review in the context of a legislative framework mandating retention of defined data attributes has become even more important. For example, the Australian Privacy Foundation explained:

In terms of metadata, I think it is easy, when we say 'All metadata should be covered by warrants', for the law enforcement agencies to come back and say, 'That's completely ridiculous; it's administratively impossible for us to go for warrants for all of those 320,000 authorisations.' I think one of the questions that needs to be asked is: how many of those are just for customer name and address? I do not think any of us are suggesting that you should have to go for a warrant just to say to a telco, 'Do you have a customer Nigel Waters?' So, we could get rid of that sort of furphy and say that maybe 50 or 60 per cent of requests are in that category and that it is no different from any other business that the police might go to and ask for customer information. But when you get into the details of their billing records, their transactions and all the other associated metadata, then it is our position that that should be subject to the warrant regime.⁵⁰

1.51 This view was supported by Electronic Frontiers Australia:

We support the implementation of a warrant process for access to metadata in any substantive form...outside of simple customer information. We do

48 Mr Simon Pomery, Assistant Director, Commonwealth Ombudsman, *Committee Hansard*, 23 April 2014, p. 29.

49 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

50 Mr Nigel Waters, Australian Privacy Foundation, *Committee Hansard*, 29 July 2014, p. 31.

not think there is a need for wider access to that, but for anything involving any substantive amount of metadata we would certainly support that.⁵¹

1.52 The MEAA explained that it agreed with the extension of the warrant regime to data which is 'information that allows a communication to occur',⁵² on the basis that such an approach would provide valuable protections for journalists:

Clearly, being required to get a warrant—anything that raises the bar to access this information is obviously very valuable. It also would then require them [law enforcement agencies] to answer certain questions that a judge would have to ask under the Evidence Act in terms of confidentiality of sources. For example, if you are seeking a warrant to get metadata about a particular journalist's phone, then they [the agency] would also have to jump through the hoops under the shield laws.⁵³

1.53 Calls for requiring access to telecommunications data to be restricted via warrant or changes to the definition of 'enforcement agency' are largely the result of changes to metadata brought about by advancing technologies and the view of stakeholders that in many circumstances, metadata should be regarded as the equivalent of content.⁵⁴ As a result, it is in this context that the debate around accessing metadata via an authorisation, rather than warrant needs to be had.

1.54 This section outlined the existing legislative framework that provides for enforcement agencies to access telecommunications data by means of an authorisation. It discussed evidence received which indicated that information captured as telecommunications data today is far greater and more revealing than the information which was available when the Act was first introduced pointing to a need for reform. Reform of access to telecommunications data becomes even more important in light of calls for mandatory data retention, which is discussed in the next section of these additional comments.

51 Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

52 'Information that allows a communication to occur' would include: the internet identifier assigned to the user by the provider; for mobile phone services – the number called or texted; the service identifier used to send a communication; the time and date of a communication; general location information/cell tower; and the duration of the communication. See, paragraph 4.10.

53 Mr Christopher Warren, Media, Entertainment and Arts Alliance, *Committee Hansard*, 21 July 2014, p. 23.

54 For more discussion refer to paragraphs 4.11 to 4.14.

Chair's views and recommendations: existing regime for authorising access to telecommunications data

1.55 The Chair's views and recommendations set out below are made in respect of his findings on the current form of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

1.56 The Chair acknowledges the enormous complexity involved in updating telecommunications interception legislation and recognises that the issues involved are technical and challenging. In forming these recommendations, the Chair has been guided by the underlying premise that the individual right to privacy must be balanced with the need to ensure community safety and national security. However, there are difficult compromises to be struck between these competing rights, as well as a range of practical considerations affecting both law enforcement agencies and telecommunications providers. Notwithstanding these difficulties, the existing TIA Act is complex and difficult to navigate; it should be re-written.

1.57 The need for reform has arisen as a result of piecemeal amendments over a 35 year period. Although these legislative changes sought to respond to the needs of law enforcement and anti-corruption bodies, they have not sufficiently considered the impact of parallel advancements in technology.

1.58 Evidence to the committee clearly illustrated that ad-hoc reform in the absence of consideration of changing technologies has resulted in a regime characterised by complexity, duplication and, in some cases, inadequate oversight and privacy protections. Moreover, it has led to an inexorable creep in the range of agencies permitted to access intercepted material and the purposes for which they are permitted to do so. As a result, the Chair considers that comprehensive reform of the telecommunications legislation is required, particularly so the legislation is well-placed to deal with the continued evolution of telecommunications technology and usage. Continued piecemeal amendment of the existing TIA Act is not feasible.

1.59 The Chair sees merit in the introduction of a single attribute-based warrant regime for content and metadata that is 'information that allows a communication to occur', but notes that a carefully considered definition of the attributes included and an appropriate proportionality test is required.

1.60 The introduction of a single attribute-based warrant regime should be coupled with the introduction of a Commonwealth public interest monitor and a review of the oversight regime governing both warranted and warrantless access. The Law Council of Australia provided examples of specific legislative changes that could be incorporated which the Chair considers would address the concerns of stakeholders in respect of oversight of the warranted access regime.⁵⁵ The Chair recommends that consideration be given to the evidence taken during this inquiry regarding the design of a single attribute-based warrant regime.

55 Law Council of Australia, *Supplementary Submission 34*, p. 2.

1.61 The Chair agrees with calls for an objects clause clearly articulating the purpose of the Act and its dual objectives of providing access to communications content and data to enable the investigation of serious crime and threats to national security and protecting the privacy of communications.

1.62 The Chair was persuaded that the introduction of a Commonwealth Public Interest Monitor, serving a similar role to that played in Queensland and Victoria, would help ensure that the introduction of attribute-based warrants does not reduce privacy protections under the existing regime.

Recommendation 1

1.63 The Chair recommends that the *Telecommunication (Interception and Access) Act 1979* be amended to include an objects clause modelled on Article 17 of the International Convention on Civil and Political Rights and the privacy principles contained in the *Privacy Act 1988*.

Recommendation 2

1.64 The Chair recommends that the *Telecommunication (Interception and Access) Act 1979* be comprehensively redrafted to enact a single attribute-based warrant regime applying to content and data that is 'information that allows a communication to occur'. Warrants under that regime should be limited to the investigation by law enforcement, anti-corruption or national security agencies of:

- serious criminal activity; or
- activity that may have serious and immediate implications for national security.

1.65 'Basic subscriber data' would continue to be accessed by enforcement agencies via the authorisation regime.

Recommendation 3

1.66 The Chair recommends that the *Telecommunication (Interception and Access) Act 1979* should be amended to establish a Commonwealth Public Interest Monitor to have oversight of the warrant regime under the Act.

Mandatory data retention

This section examines the policy of mandatory data retention in the context of the government's proposed regime set out in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. The terms 'telecommunications data' and 'metadata' are used interchangeably.

Background

1.67 In 2012, when requesting that the Parliamentary Joint Committee on Intelligence and Security (PJCIS) undertake an inquiry into a package of potential reforms to Australia's national security legislation, the then Attorney-General directed the PJCIS to consider:

Applying tailored data retention periods for up to 2 years for part of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts.⁵⁶

1.68 In its June 2013 report, the PJCIS stated that it had 'grappled with the issue of how best to reconcile the important national security interests...and on the other hand...the very significant alteration of the relationship between the state and the citizen, which the introduction of such a regime would arguably involve'.⁵⁷ That committee did not form a view on the need for the introduction of mandatory data retention, but rather, stated that the matter should be left for government.⁵⁸

1.69 On 30 October 2014, the Abbott Government introduced the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Bill) into the House of Representatives.⁵⁹ On introducing the Bill, the Minister for Communications explained:

The bill contains a package of reforms to prevent the further degradation of the investigative capabilities of Australia's law enforcement and national security agencies. 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

⁵⁶ Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 139.

⁵⁷ PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, p. 190. The PJCIS noted in its report that its task was made more difficult in the absence of any draft legislation.

⁵⁸ In noting that mandatory data retention should be a decision for government, the PJCIS did recommend that if the government was persuaded to introduce a mandatory data retention regime, an exposure draft of the proposed legislation should be referred to the committee for examination. See: PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, pp. 192–193.

⁵⁹ The Hon Malcolm Turnbull MP, Minister for Communications, *Votes and Proceedings*, Thursday 30 October 2014, p. 951.

two years. The bill amends the *Telecommunications Interception and Access Act 1979*...and the *Telecommunications Act 1997*...⁶⁰

1.70 The proposed mandatory data retention regime set out in the Bill would introduce a requirement that telecommunication service providers in Australia retain telecommunications data (metadata) for a period of two years. Rather than define 'telecommunications data', the Bill would 'allow regulations to prescribe a consistent, minimum set of records that service providers who provide services in Australia must keep for two years'.⁶¹ Under the Bill, content and web browsing data would be specifically excluded from the retention requirement.⁶²

1.71 The Bill also proposes a new definition of 'enforcement agency' and 'criminal law enforcement agency' for the purposes of existing Chapter 4 (accessing telecommunications data) and Chapter 3 (in relation to preservation notices) of the TIA Act. The proposed definitions, which would seek to limit the number of agencies that can access this data, include the introduction of a ministerial discretion that would enable the Minister to declare an agency to be an 'enforcement agency' or 'criminal law enforcement agency' for the purposes of the Act.⁶³

1.72 In addition, the Bill proposes the introduction of a new oversight regime for the Commonwealth Ombudsman where the Ombudsman would oversee the authorisation regime, including an obligation to report annually on the regime to the Minister and the Parliament.⁶⁴

Why is mandatory data retention being proposed?

1.73 Telecommunications data is generally collected as a matter of course by carriers and carriage service providers in the provision of communication services. This information has traditionally been used for billing purposes. However, as technology and the way in which services are provided has changed, this data is no longer always required for business purposes and in some instances is not being retained at all. This has led to calls, primarily from national security and law enforcement agencies, for the introduction of a mandatory data retention regime. It also explains the view of those agencies that, what would be required is not the introduction of a new obligation, but rather the mandating of data to ensure consistency in the data set retained, both in terms of data and the period of retention. This is reflected in the Bill currently before Parliament.

1.74 In his second reading speech the Minister explained the government's view of the vital role of metadata to public and national security:

⁶⁰ The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12560.

⁶¹ The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12561.

⁶² Proposed new subsection 187A(4).

⁶³ Proposed new sections 110A and 176A.

⁶⁴ Proposed new sections 186A to 186J.

Access to metadata plays a central role in almost every counterterrorism, counterespionage, cybersecurity and organised crime investigation. It is also used in almost all serious criminal investigations, including investigations into murder, serious sexual assaults, drug trafficking and kidnapping. The use of this kind of metadata, therefore, is not new. However, as the business models of service providers are changing with technology they are keeping fewer records. And they are keeping those records for shorter periods of time because they do not need them any longer, in many cases, for billing. Many of the records that are still kept are kept because of legacy systems put in place years ago. In June 2013, the Parliamentary Joint Committee on Intelligence and Security concluded that this diminution in the retention of metadata is harming law enforcement and national security capabilities, and that these changes are accelerating.⁶⁵

1.75 Throughout its inquiry the committee received much evidence from law enforcement agencies indicating universal support for the introduction of mandatory data retention for the reasons cited by the Minister. For example, the Board of the Australian Crime Commission (ACC), in stating its support for a regime that required data to be retained for a 'uniform length of time across all telecommunication service providers', explained:

Telecommunications data is an effective and efficient tool used by law enforcement to identify and investigate organised criminal activity and serious crime and reveal the true extent of a criminal network which would otherwise remain unknown.⁶⁶

1.76 Victoria Police, another advocate for mandatory data retention, voiced strong support for the implementation of such a regime 'given the changes in the patterns of community usage of mobile phones (being that many persons use mobile phones daily and frequently for conversations or internet access) and changes in industry business practices'. Victoria Police added:

...in many instances, carriers only retain data for commercial purposes such as billing. Data which is of interest to law enforcement is often not retained. Where data is retained, it is for varying periods of time. The community expectation for criminal activity to be sufficiently investigated and prosecuted justifies data retention to mitigate the risk that evidence will be unavailable.⁶⁷

1.77 The Australian Commission for Law Enforcement Integrity (ACLEI) also supported calls for mandatory data retention:

ACLEI sees merit in a legislated data retention requirement on telecommunications service providers, which would provide clarity as to how long a period of time service providers will retain telecommunications

⁶⁵ The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12560.

⁶⁶ Mr Paul Jevtovic APM, Acting Chief Executive Officer, Australian Crime Commission' *Committee Hansard*, 22 April 2014, p. 9.

⁶⁷ Victoria Police, *Submission 6*, p. 4.

data, and ensure that such data can be properly accessed for law enforcement purposes. This data is already in the possession of service providers for their usual business practices, such as billing, which is generally destroyed after a short period of time.⁶⁸

1.78 ACLEI provided an example of how the lack of a mandatory data retention regime had affected its ability to investigate corruption:

In a recent ACLEI corruption investigation, it appeared that sensitive information about a law enforcement agency may have been unlawfully disclosed to a third party by use of an anonymous website contact form.

ACLEI was able to identify the IP address of the computer from which the alleged unlawful disclosure had been made, but when ACLEI sought to match the IP address to a particular internet user, the relevant internet service provider advised that—in accordance with usual business practices—the information had been destroyed when it was no longer necessary.

There were no other means available to ACLEI to match the IP address to a person. If the service provider had been under an obligation to keep its telecommunications data for more than a few months, the data might have been available to ACLEI for the purposes of the corruption investigation.⁶⁹

1.79 Despite widespread support among law enforcement and national security agencies for the introduction of mandatory data retention, concerns have been consistently raised since such a regime was first mooted, and again, following the release of the government's proposed legislation in late October 2014. Concerns are generally related to the following three themes:

- the scope of the proposed mandatory data retention regime;
- the cost involved; and
- the privacy implications of implementing a two year retention regime.

1.80 These matters are addressed below in the context of the government's proposed regime.

Scope of the proposed mandatory data retention regime

1.81 Part 1 of Schedule 1 of the Bill seeks to insert a new Part 5-1A into Chapter 5 of the TIA Act.⁷⁰ Proposed Division 1 of Part 5-1A sets out the scope of the proposed mandatory data retention regime.

1.82 Proposed new section 187A contains the obligation on service providers to keep 'information of a kind prescribed by regulations, or documents containing information of that kind'⁷¹ for the period prescribed by proposed new section 187C

⁶⁸ ACLEI, *Submission 11*, p. 5.

⁶⁹ ACLEI, *Submission 11*, p. 5.

⁷⁰ Explanatory Memorandum (EM), p. 34.

⁷¹ Proposed new subsection 187A(1).

and identifies that the kinds of information that would be required to be retained by regulations must relate to one or more of the following matters:

- (a) characteristics of any of the following:
 - (i) the subscriber of a relevant service;
 - (ii) an account relating to a relevant service;
 - (iii) a telecommunications device relating to a relevant service;
 - (iv) another relevant service relating to a relevant service;
- (b) the source of a communication;
- (c) the destination of a communication;
- (d) the date, time and duration of a communication, or of its connection to a relevant service;
- (e) the type of a communication, or a type of relevant service used in connection with a communication;
- (f) the location of equipment, or a line, used in connection with a communication.⁷²

1.83 The Explanatory Memorandum (EM) to the Bill sets out that telecommunications data would not be defined in the TIA Act so as to remain technology-neutral and that 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'.⁷³

1.84 The EM further explains 'data retention will create a consistent obligation for record-keeping across the telecommunications industry' and that although '[s]ome service providers may initially need to modify their systems to ensure they meet this minimum standard':

The minimum obligation imposed by this legislation is consistent with the types of data and subscriber information currently held by service providers for billing, quality assurance and other business purposes.⁷⁴

1.85 Proposed new section 187B identifies service providers that would be exempt from the data retention obligations proposed under section 187A(1). The purpose of proposed new section 187B:

...will be to ensure that entities such as governments, universities and corporations will not be required to retain telecommunications data in relation to their own internal networks (provided these services are not offered to the general public), and that providers of communications services in a single place, such as free Wi-Fi access in cafes and restaurants

⁷² Proposed new subsection 187A(2).

⁷³ EM, p. 36.

⁷⁴ EM, p. 34.

are not required to retain telecommunications data in relation to those services. However, the [Communications Access Co-ordinator] CAC can declare that data from such services must nevertheless be retained.⁷⁵

1.86 The mandatory data retention regime being proposed by the government's Bill has been criticised on the basis that the:

- term 'telecommunications data' remains unclear;
- costs of implementing such a regime remain unknown; and
- retention period being proposed is arbitrary and further undermines privacy.

1.87 There has, however, been widespread support for the inclusion in the Bill of a revised definition of 'enforcement agency' (which would have the effect of limiting the number of agencies who can access telecommunications data via authorisation), and the proposed introduction of an oversight regime in respect of telecommunications data.

What is telecommunications data?

1.88 Many submitters contended that due to changes in technology, metadata (telecommunications data) should now be regarded as content. They contend that the definition of 'telecommunications data' should take this into account. Mr Steve Dalby, the Chief Regulatory Officer at internet service provider iiNet Limited, explained how the analogy of the 'envelope and the letter' no longer holds up:

The complex, voluminous, often sensitive and private nature of the data sought under a mandatory data retention regime exposes the hollowness of the claim that communications data or metadata is 'just like the envelope without its contents'. The difficulty with such a poor analogy is that it attempts to compare a piece of paper, the envelope, with a chain of events and multiple links to myriad other data, meticulously described and recorded. In the case of Twitter, this may include who wrote the tweet, their biography, their location, when it was written, how many other tweets have been written on that user's account, where the author was when the tweet was posted, what time it was, whom it was sent to, where the author is normally based and, surprisingly in the case of Twitter, the 140 characters of the content of the tweet as well.⁷⁶

1.89 Mr Dalby further explained to the committee that as metadata 'underlies all communications':

It is fundamentally misleading to downplay the degree of intrusion of data retention regimes such as those that operate at the European directive level. A false assertion is that such regimes do not include the actual content of what our customers might be communicating. These inaccurate distinctions are dangerous and inappropriate. It is misleading to assert that such data is

⁷⁵ EM, p. 47.

⁷⁶ Mr Steve Dalby, Chief Regulatory Officer, iiNet Limited, *Committee Hansard*, 29 July 2014, p. 21.

'only metadata' or 'just metadata'. Metadata reveals even more about an individual than the content itself.⁷⁷

1.90 Blueprint for Free Speech raised similar concerns that it is:

...easy to try to triangulate information about a particular person, or to imply particular activities or conduct, purely from metadata. If you have enough of it you can build a story and then imply context, which is in itself dangerous.⁷⁸

1.91 Electronic Frontiers Australia agreed with the view that 'metadata is often a proxy for content':

We also strongly disagree with the assertion that metadata is less invasive than providing access to content. As the Attorney-General's Department itself admitted in its submission:...telecommunications data can contain particularly sensitive personal information justifying special legal protection. We completely and wholeheartedly agree with that. Clearly, it can be used to build a picture of a target, their network of associates, where they shop, where they eat, where they sleep...⁷⁹

1.92 Mr Lawrence also cited the following research by David Seidler who made the following point about data retention:

Although on its face, metadata might appear anonymised and trivial, the development of big data analysis techniques (for which metadata is "perfect fodder") means that the insights it provides after manipulation might well meet this definition—of being content, that is.⁸⁰

1.93 More dramatically, Ms Lindy Stephens, Global Director of People Operations at ThoughtWorks, cited former Central Intelligence Agency (CIA) and National Security Agency (NSA) Director General Michael Hayden as having said, 'We kill people based on metadata'.⁸¹ Ms Stephens also referred the committee to statements made by former NSA General Counsel Mr Stewart Baker that 'metadata absolutely tells you everything you need to know about somebody's life. If you have enough metadata, you don't really need content'.⁸²

1.94 Industry groups cautioned the committee in respect of the potential privacy impacts on consumers of data retention. AMTA submitted that:

[A] data retention scheme will involve an increased risk to the privacy of Australians and provide an incentive to hackers and criminals. Data

⁷⁷ Mr Steve Dalby, iiNet Limited, *Committee Hansard*, 29 July 2014, p. 20.

⁷⁸ Mr Simon Wolfe, Head of Research, Blueprint for Free Speech, *Committee Hansard*, 23 April 2014, pp. 50–51.

⁷⁹ Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

⁸⁰ Mr Jon Lawrence, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36.

⁸¹ Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 5

⁸² Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 5.

retention is at odds with the prevailing policy to maximise and protect privacy and minimise the data held by organisations.

Industry believes it is generally preferable for consumers that telecommunications service providers retain the least amount of data necessary to provision, maintain and bill for services.⁸³

1.95 The Media, Entertainment and Arts Alliance (MEAA) also outlined its opposition to mandatory data retention explaining that it was particularly apprehensive as to how such a regime would affect the free press:

The inevitable impact of collection, storage and surveillance through metadata is that it will be impossible for a journalist to liaise with a source, for a source to connect with a journalist or for a journalist to connect with a source without it being be able to be found and be identified, without them going through quite extraordinary encryption processes—and, even there, I think there is probably a question mark over how effective that would be.⁸⁴

The need for a definition of 'telecommunications data' in the primary legislation

1.96 Throughout the duration of the committee's 15 month inquiry, stakeholders consistently raised the need for a clear definition of 'telecommunications data' to be legislated, particularly in the event of the government seeking to implement mandatory data retention.

1.97 Dr Roger Clarke of the Australian Privacy Foundation identified the complexity of defining metadata, explaining to the committee:

The term 'metadata'...derives from the library sphere. It is data about data, and it has gradually been absorbed into discussions about the internet, because obviously librarianship has moved on to the internet during the last 20 years...It merely means data about data. That is the only consolidated meaning that it has. With respect to any given communication, your answer as to what is metadata and what is content will be different. There is not one answer to: what is metadata? There are 40 or 50 answers and, in fact, some of them can be disputed at length. That has been lost in this debate. Everybody is assuming that metadata is a thing that can be legislated for. It is not technologically neutral. It is absolutely unclear what metadata will mean in each of these different contexts.⁸⁵

⁸³ Australian Mobile Telecommunications Association and the Communications Alliance, *Submission 16*, pp. 12–13.

⁸⁴ Mr Christopher Warren, Federal Secretary, Media, Entertainment and Arts Alliance, *Committee Hansard*, 21 July 2014, p. 22.

⁸⁵ Dr Roger Clarke, Immediate Past Chair, Australian Privacy Foundation, *Committee Hansard*, 2 February 2015, p. 26. Similar concerns were raised by the Internet Society of Australia (ISOC-AU): At this point in time there are...no clear technical specifications for metadata in the internet protocol world. In [classic] telephony there were call detail records which are defined under International Telecommunications Union standards...It is clear, it is simple and it is available. In the internet world that type of description does not exist for the myriad of types of communications and communication services that we have. Source: Ms Narelle Clark, President, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 35.

1.98 Other submitters also acknowledged the complexity of defining 'telecommunications data', and they too cited the importance of clearly defining the term. Mr Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra, explained:

...defining metadata is...clearly the critical thing. What information do we consider to be metadata, in terms of the legislation, and what do we not? Once that distinction is made it becomes a much clearer picture, though it may not satisfy everyone. Metadata is anything and everything that you are really gathering; it is information from the use of technology.⁸⁶

1.99 Electronic Frontiers Australia was of a similar view:

It is clearly a pretty critical starting point that we get a clear definition of metadata. In the telephonic context it is fairly straightforward, but if we go beyond that into non-telephonic communications we have some very serious concerns that it is even technically feasible to effectively separate metadata from content, particularly in the case of email communications.⁸⁷

1.100 Although stakeholders explained the need for a clear definition of 'telecommunications data' on the basis that clarity is required to ensure certainty for industry, protect privacy, and enable the costs of mandatory data retention to be accurately forecast, the Bill currently before the Parliament, while identifying the categories of information that metadata might include, relies on regulations to set out the specific details.

1.101 The Attorney-General's Department (department) explained that this approach had been taken to ensure the legislation remains technology neutral:

The regulations provide an ability to update the dataset in the event that it is required due to changes in telecommunications services and the fundamental nature of those, and industry have told us consistently that the industries are evolving at a rapid rate and there is considerable change on the horizon. The inclusion of the dataset in regulations provides an ability to update the dataset whilst ensuring it is limited to the six key categories include on the face of the bill.⁸⁸

1.102 Despite the department's explanation, the approach of delegating the substance of the Bill to subordinate legislation has been criticised by many stakeholders, many reiterating the need for a definition to be included in the primary legislation.⁸⁹

⁸⁶ Mr Alastair MacGibbon, *Committee Hansard*, 26 September 2014, p. 35.

⁸⁷ Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, 29 July 2014, p. 36. See also: Ms Narelle Clark, ISOC-AU, *Committee Hansard*, 23 April 2014, p. 35.

⁸⁸ Ms Anna Harmer, Acting First Assistant Secretary, National Security Law and Policy Division, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, p. 46.

⁸⁹ The committee notes that Optus however 'consider[ed] the use of regulations to spell out more detail of the intended data set [was] appropriate'. Source: Optus, *Submission 86 to the PJCIS inquiry*, p. 7.

1.103 The Law Council of Australia (Law Council) stated that in its view, the delegation of the definition of telecommunications data to regulations was inappropriate:

The Law Council's Rule of Law Principles require that where legislation allows for the Executive to issue subordinate legislation in the form of regulations, the scope of that delegated authority should be carefully confined and remain subject to Parliamentary supervision. Such a requirement ensures that Executive powers are defined by law, such that it is not left to the Executive to determine for itself what powers it has and when and how they may be used. As a matter of good legislative practice, significant matters should be specified in primary legislation which generally undergoes extensive consultation, not potentially subject to change by Ministerial decision and regulation.⁹⁰

1.104 The Law Council further set out why it considered it inappropriate for the data set to be defined in regulations:

The categories of information which should be captured by the scheme will raise significant questions of policy and have very substantial financial, as well as privacy, implications. The 'kinds of information' (within defined categories) that might be required to be captured and kept are uncertain. Although the Government has provided an initial proposal (in the form of a draft Regulation) the data set is still in draft form and can be changed at any time. Given that service providers can be subjected to civil penalties for failing to comply with obligations under the scheme (see for example section 187M) and the impact of the scheme on individuals, the Law Council considers that it is inappropriate for the kind of telecommunications data to be prescribed by regulations. Both the categories of the data to be retained and the specific data set should be set out in the Bill itself.⁹¹

1.105 In addition, the Law Council cited the report of the Scrutiny of Bills Committee which stated that 'paragraph 187A(1)(a)...inappropriately delegate[d] legislative power'⁹² and accordingly, made the following recommendations:

- The Bill should clearly define the types of telecommunications data and the specific data set to be retained.
- The power to prescribe by way of regulation the mandatory data set should be removed from the Bill.
- The Bill should define the distinction between the 'content and substance' of a communication (referred to in clause 187(4)(a) of the Bill), as opposed to 'telecommunications data'.⁹³

⁹⁰ Law Council of Australia, *Submission 126 (Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014)*, p. 13.

⁹¹ Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 13.

⁹² Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 16 of 2014*, 26 November 2014, pp. 2–5. See also: Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 13.

1.106 A similar concern was raised by the Australian Human Rights Commission (AHRC) in its submission to the PJCIS inquiry. In its submission, the AHRC, while acknowledging the rationale for using regulations, stated that:

...the definition of telecommunications data is a critical feature of the Bill and should not be left to be described by Regulations. The Commission considers that the telecommunications data required to be retained by telecommunication services providers should be included in the legislation itself.⁹⁴

The cost of data retention

1.107 Throughout its inquiry the committee sought to establish the costs that would be involved should the government proceed with its plan to introduce mandatory data retention. At the committee's final public hearing on 2 February 2015 and after the introduction of the Bill, the department was unable to provide any indication to the committee of the possible cost of a mandatory data retention regime to taxpayers. In fact, in response to questioning as to whether or not the Parliament will know how much the scheme will cost before the Bill is debated, the department advised:

That will ultimately be a matter for the Attorney and the government...As with all budgetary matters, it is a matter for the budget process and the government and the cabinet.⁹⁵

1.108 On introducing the Bill, the Minister stated:

There has also been a great deal of conjecture about how much data retention may cost...the government is committed to ongoing, good faith consultation with industry and expects to make a substantial contribution to both the cost of implementation and the operation of this scheme.⁹⁶

1.109 On 18 February 2015, the Prime Minister, the Hon Tony Abbott MP, was quoted as saying that 'keeping the data would cost less than \$400 million a year'.⁹⁷ In its report tabled on 27 February 2015, the PJCIS set out that '[i]ndicative 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'.⁹⁸

⁹³ Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 14.

⁹⁴ Australian Human Rights Commission (AHRC), *Submission 42 to the PJCIS inquiry*, p. 7.

⁹⁵ Ms Katherine Jones, Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, p. 54.

⁹⁶ The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12561.

⁹⁷ Emma Griffiths, ABC News, 'Data retention plan could cost almost \$400 million a year, Tony Abbott says', 18 February 2015, <http://www.abc.net.au/news/2015-02-18/data-retention-plan-could-cost-almost-400-million-a-year/6139078> (accessed 3 March 2015).

⁹⁸ PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 182.

1.110 Throughout the course of its inquiry, the committee did however receive evidence from industry participants of the predicted costs associated with the implementation of such a regime. The committee heard that the lack of clarity around what was being proposed, and therefore the costs that the imposition of a mandatory data retention regime may have for industry participants, were of great concern. The Australian Mobile Telecommunications Association (AMTA) and Communications Alliance explained industry's apprehension and its views in relation to these matters as follows:

...the cost of retaining data beyond any period it would be retained in the normal course of business must be borne by the agencies that require it. Similarly, any costs in relation to security, storage and ability to search retained data must also be borne by the agencies that require it. The Associations note that keeping more data or keeping data for longer periods, may add to costs significantly whereas the added benefits may be incremental, at best.

...The costs of acquiring and retaining particular items of data will vary widely, as will the benefits to [law enforcement and national security agencies] LENSAs.⁹⁹

1.111 iiNet Limited (iiNet) advised the committee that the cost of implementing data retention to its organisation could be as high as '\$100 million and growing over time as data grows':

[\$60 million] was our first-year cost, which we calculated...18 months ago. We have done some maths since then and we have seen the proliferation of metadata on websites and other places doubling every 18 months to two years, so our costs would increase. I know the cost of storage is coming down, but we believe that doubling every two years of the volume of data that would need to be collected would mean that this would be an ongoing increase. We are now talking more in the order of \$100 million for that first two-year period of data collection...and growing over time as that data grows. And then there is another potential cost on top. If the suggestion is that content is not required—that somebody will be required to process the metadata that is collected to strip out the content—that would be petabytes of data a day for our own organisation. You would need supercomputers to extract that data ...The cost of storage might go down a fraction, but if we have to store it in the first place and then redact it it is just costs upon costs.¹⁰⁰

1.112 AMTA explained that it had previously identified the potential costs of data retention to industry as more than \$500 million for 'a new scheme around network infrastructure security and potentially high costs for industry around online copyright enforcement':

⁹⁹ Australian Mobile Telecommunications Association and the Communications Alliance, *Submission 16*, pp. 12–13.

¹⁰⁰ Mr Steve Dalby, iiNet Limited, *Committee Hansard*, 29 July 2014, pp. 26–27.

...in this day and age information flows are not only huge but increasing in some spaces exponentially. They are also borderless in the sense that all of us on a daily basis I am sure traverse many websites and destinations outside of Australia...To give you a picture: data volumes in the mobile space alone are predicted to increase by a factor of 10 between 2013 and 2019. Should we have to build a system to retain data for a lengthy period, it is not just as simple as pushing a button or tapping an existing resource; in actual fact we would have to duplicate the data. That duplication would be required because this data comes from a multitude of IT systems within carriers. To be helpful to law enforcement agencies, it would need to be duplicated and aggregated. Then we have to store it...Then we have to manage it and be able to interrogate it. There are the privacy and security issues that go with that. All of these things are very considerable issues to address.¹⁰¹

1.113 iiNet suggested that these costs could end up being passed on to customers, but added that until it is clear what the legislation would require it would be difficult to calculate the ultimate cost:

We originally calculated the \$60 million to be an increase of about \$5 per month per customer if we just passed the costs through...we are very confused about what is required so it is very difficult for us to calculate what the costs will be. If we are only required to keep routine metadata for telephone calls we can probably pack up today and not speak again. If, however, the confidential briefing paper that was provided by the Attorney-General's Department is to be interpreted the way we have then yes, there will be massive costs.¹⁰²

1.114 Mr Chris Althaus, Chief Executive Officer of AMTA made similar comments in relation to consumers:

[T]he costs issue remains a very significant one for industry. All of the matters that relate to interception, and the extension perhaps into a data retention regime, come at significant cost. Industry has to shoulder its burden in that respect, but so too will there be an impost through to consumers, and, we believe, a necessary impost on government. Schemes elsewhere around the world have frequently seen the role of government in funding the establishment of schemes and the national security and law-enforcement agencies paying to use those schemes. That is certainly an issue for consideration in this current debate.

We are going to incur significant costs. Data gathering through a range of currently disaggregated systems within service providers will need to be serviced by a new system, a new capacity. And of course there is significant and ongoing uncertainty around many aspects of that. A lot of those aspects are what we will perhaps describe as a work in progress.¹⁰³

¹⁰¹ Mr Chris Althaus, AMTA, *Committee Hansard*, 29 July 2014, pp. 11–12.

¹⁰² Mr Steve Dalby, iiNet Limited, *Committee Hansard*, 29 July 2014, pp. 26–27.

¹⁰³ Mr Chris Althaus, Chief Executive Officer, AMTA, *Proof Committee Hansard*, 2 February 2015, p. 6.

1.115 Industry submitters consistently explained to the committee that the costs from the introduction of a mandatory data retention regime would not be from storage of the data but rather the systems to extract the data and the security that would need to be built to protect the data once stored. For example, Mr James Shaw, Director of Government Relations at Telstra, explained:

...quite often the focus seems to be around the storage of the data...but that is only a very small part of it. In fact, in terms of the costs of the scheme, it is probably one of the lesser elements of it. There is the whole process of extracting the data from the network, and the data that is being looked at in the context of this regime comes from various network elements. It is not located in one central server within the network. There is a variety of platforms generating different types of data in different formats. That has to be extracted. It then has to be managed and stored, and at the same time it has to be secured. Then it has to be made available in a form that the agencies can usefully use. Then, finally, and most importantly, at the end it has to be disposed of in a way that satisfies the concerns of customers that this data is not hanging around for any longer than is required. So they are all steps in or elements of an overall data retention scheme. You cannot divorce one from the other, but they are separate considerations in how you go about building the scheme.¹⁰⁴

1.116 Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy at Vodafone Hutchison Australia, was of a similar view:

The storage component is relatively straightforward to expand. Where the costs are is in the capability to retrieve the information from a very large data set. That is where the costs will kick in as you lengthen the amount of time.¹⁰⁵

1.117 However, Mr Alastair MacGibbon suggested to the committee that in his experience, the 'cost argument is often overblown'. He explained:

Given the ability to compress information and the cost of the actual devices for storing information, the cost of storage has gone down exponentially and will continue to do so over the years. I think the biggest cost is probably in architecting their systems to collect information. In many respects they are compelled to at the moment anyway under the current telecommunications interception act requirements.

...The reason why cost should not be an argument in compelling some of these ISPs and telcos to store information is that, as I say, they are currently obliged to have themselves architected in certain ways...¹⁰⁶

¹⁰⁴ Mr James Shaw, Telstra, *Committee Hansard*, 26 September 2014, p. 39.

¹⁰⁵ Mr Matthew Lobb, Vodafone Hutchison Australia, *Committee Hansard*, 26 September 2014, p. 24.

¹⁰⁶ Mr Alastair MacGibbon, *Committee Hansard*, 26 September 2014, pp. 30–31.

1.118 ThoughtWorks raised the concern that data retention could in fact have more far-reaching impacts, directly affecting the bottom line of some businesses as consumers seek out companies that provide greater privacy protections:

As an Australian business we are concerned that we will see this impact on our industry here in Australia that the US has seen. Essentially, we are talking about customers choosing to store their information in another country because they are concerned about the laws in the US and the subversion of those laws in the US in order to access data.

We are also concerned that if we have stronger laws here that we will lose business. In particular, for things like cloud providers—organisations that store data for other companies—where there has been the biggest impact. But there were all sorts of impacts across the board. Cisco, who make routers and other things that direct internet traffic, saw a decline in their top markets of between 18 and 30 per cent. So we are seeing real impacts on business already, particularly in the US, and it comes from a lack of trust by customers.¹⁰⁷

Privacy implications of the proposed data retention period

1.119 In contrast to the calls by law enforcement agencies for the implementation of a mandatory data retention regime, many stakeholders raised concerns in respect of privacy and the proposed regime, particularly the prescribed retention period of two years. It was suggested that the introduction of such a regime ran directly counter to the application of Australian Privacy Principle 3, which codifies the long-standing principle that personal data should not be arbitrarily captured and stored:

The Australian privacy principles were updated and implemented just six months ago, yet mandatory data retention is a policy that would require the explicit rejection of these principles.¹⁰⁸

1.120 On introducing the Bill, the Minister explained that the two year retention period set out in the Bill had been determined on advice from law enforcement and security agencies, as well as by reference to the experiences of a number of foreign jurisdictions.¹⁰⁹

1.121 In its submission to the PJCIS committee, the department identified that '[m]ore than 35 Western countries worldwide have legislative data retention schemes' and that the 'most widely implemented data retention scheme is the former EU Data Retention Directive...which imposed an obligation on companies to retain specified data for up to [two] years'.¹¹⁰ The evidence provided by the department to the PJCIS

¹⁰⁷ Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 7.

¹⁰⁸ Mr Simon Breheny, Director, Legal Rights Project, Institute of Public Affairs, *Committee Hansard*, 26 September 2014, p. 8.

¹⁰⁹ The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12561.

¹¹⁰ Attorney-General's Department, *Submission 27 to the PJCIS inquiry*, p. 38.

identified that the proposed two year period is in fact at the upper limit for retaining data across jurisdictions.¹¹¹

1.122 The proposed period attracted much criticism: stakeholders were consistently of the view that the two-year period should be revised. In its review of the Bill, the Parliamentary Joint Committee on Human Rights (PJCHR) stated that:

A data retention period of two years raises the question of whether the period is disproportionate, and may go beyond the period necessary to achieve the scheme's legitimate objective. This question is resolved by reference to the purposes for which the data is accessed.

For example, despite the acknowledged low frequency of use of data that is more than six months old, and the stated requirement for older data for national security and complex criminal offences, the scheme does not limit access to data which is older than six months to the investigation of national security and complex criminal offences.¹¹²

1.123 This conclusion led the PJCHR to request 'further advice of the Attorney-General as to whether the two year retention period is necessary and proportionate in pursuit of a legitimate objective'.¹¹³

1.124 Similarly, the Australian Human Rights Commission (AHRC) raised concerns in respect of the two year retention period noting that:

In the landmark decision of the Court of Justice of the European Union [EU], which invalidated the EU Data Retention Directive, the Court identified several characteristics of the Directive that rendered the regime a disproportionate interference with the rights to privacy. Relevantly, the Court considered that retention periods should be limited to that which is 'strictly necessary'. Further, retention schemes should distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned.¹¹⁴

1.125 The AHRC drew attention to an evaluation report on the EU Data Retention Directive in 2011 that 'only 2 per cent of requested data was over [one] year old across

¹¹¹ See: Attorney-General's Department, *Submission 27 to the PJCIS inquiry*, Appendix A—Summary of data retention and access arrangements in Western countries, pp. 55–56.

¹¹² Parliamentary Joint Committee on Human Rights (PJCHR), *Fifteenth Report of the 44th Parliament*, p. 15. It is expected that the response of the Attorney-General together with the PJCHR's finding on the Bill's compatibility with human rights will be set out in the PJCHR's report of 17 March 2015.

¹¹³ PJCHR, *Fifteenth Report of the 44th Parliament*, p. 15.

¹¹⁴ Australian Human Rights Commission (AHRC), *Submission 42 to the PJCIS inquiry*, pp. 8–9. See also, Gilbert + Tobin Centre for Public Law, *Submission 5 to the PJCIS inquiry*, p. 2; Mr Bernard Keene, *Submission 37 to the PJCIS inquiry*, pp. 5–6; Australian Privacy Foundation, *Submission 75 to the PJCIS*, p. 2; Law Institute of Victoria, *Submission 117*, pp. 15–16; Civil Liberties Councils of Australia, *Submission 129 to the PJCIS inquiry*, p. 12; and Mr Jon Lawrence, Electronic Frontiers Australia, *Proof Committee Hansard*, 2 February 2015, p. 15.

the European Union' and noted that as the majority of EU countries (including the United Kingdom) have a one year retention period 'an initial retention period of [one] year would be a more proportionate interference with the right to privacy'.¹¹⁵

1.126 The Australian Privacy Commissioner stated that any data retention scheme 'should only require service providers to retain telecommunications data for the minimum amount of time necessary to meet those needs'.¹¹⁶ The Law Council made a similar recommendation stating that the 'data retention period should be reduced to no longer than the minimal period required by law enforcement and security agencies'.¹¹⁷

1.127 The Internet Society of Australia (ISOC-AU) outlined that in its view unless there is 'appropriate technology standards metadata should not be retained beyond strict business need':

Where metadata is retained there need to be the strictest standards around retention and access. I cannot reinforce that enough. Should access to metadata be granted, considerably higher standards of access and oversight of these processes need to be implemented, including penalties for the breaches of these sorts of standards...Certain things need to be built into the equipment and the application so that we can do this in a clear and consistent manner with appropriate levels of control.¹¹⁸

1.128 The telecommunications industry was also of the opinion that the case for a two year data retention period had not been made:

Industry is, however, far from convinced that a two year retention period for IP related data is either necessary, justifiable, cost-effective, or in the public interest...and 12 months. For internet-related data there is only one country – Poland – that appears to be heading down the path of a 2 year retention period – and that regime is under challenge.

We know that in UK, for example, over a recent 4 year period, 74%+ of disclosures to law enforcement agencies, where the age of data being sought was known, related to data that was less than 3 months old....

[communication service providers] CSPs report that the vast majority of warrantless requests they receive from Australian agencies relate to data that is 6 months old or younger...¹¹⁹

¹¹⁵ AHRC, *Submission 42 to the PJCIS inquiry*, pp. 8–9. A similar study was cited by the Australian Privacy Commissioner in his submission to the PJCIS inquiry and the Law Council of Australia. See, Office of the Australian Information Commissioner (OAIC), *Submission 92 to the PJCIS inquiry*, p. 15; Law Council of Australia, *Submission 126 to the PJCIS inquiry*, pp. 16–17.

¹¹⁶ OAIC, *Submission 92 to the PJCIS inquiry*, p. 14.

¹¹⁷ Law Council of Australia, *Submission 126 to the PJCIS inquiry*, p. 17.

¹¹⁸ Ms Narelle Clark, ISOC-AU, *Committee Hansard*, 23 April 2014, pp. 33, 38.

¹¹⁹ AMTA and Communications Alliance, *Submission 6 to the PJCIS inquiry*, p. 7.

1.129 AMTA and the Communications Alliance suggested that rather than the two year period proposed by the Bill, a '[six] month period would be an appropriate minimum time to require the retention of internet-related data' and:

It might be useful to incorporate within the Bill a requirement for agencies to periodically report to Parliament the number of requests (including distinguishing between a request relating to an individual and requests relating to groups of people) that have been placed with CSPs for retained data that was generated in the preceding 3 month period, 3-6 month period, 6-12 month period, 12-18 month period and 18-24 month period.¹²⁰

No destruction requirement

1.130 Concerns were also raised in relation to the absence of a legislative requirement for data captured by the proposed regime to be destroyed.

1.131 On 12 March 2014, the updated Australian Privacy Principles (APP's) came into force, binding government agencies and other organisations to uphold high-level privacy practices.

1.132 Notably, for the purposes of data retention, APP 3 states, in part, that an:

[E]ntity must not collect personal information... unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.¹²¹

1.133 APP 11 prescribes that an entity must:

[T]ake such steps as are reasonable in the circumstances to protect the [personal] information [it holds] from misuse, interference and loss; and from unauthorised access, modification or disclosure [and that if an entity holding personal information about an individual] no longer needs the information for any purpose for which the information may be used or disclosed by the entity...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.¹²²

1.134 Although the existing TIA Act contains a destruction requirement for restricted records and telecommunications content¹²³ it does not contain a destruction requirement in respect of telecommunications data. The department confirmed that there is no destruction requirement proposed in the Bill currently before the Parliament:

¹²⁰ AMTA and Communications Alliance, *Submission 6 to the PJCIS inquiry*, pp. 7–8.

¹²¹ <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles> (accessed 20 August 2014). See also: APP 3, Schedule 1 to the *Privacy Act 1988*.

¹²² APP 11, Schedule 1 to the *Privacy Act 1988*.

¹²³ See sections 79 and 150 of the TIA Act.

...in relation to the two-year detention period is that there is no obligation in the bill to destroy that information after two years.¹²⁴

1.135 Throughout its inquiry, this aspect of the existing legislation and the proposed Bill was identified as an area needing reform.

1.136 The Law Council raised this gap in the Bill as a concern given the obligations imposed by the APP's.¹²⁵ Telstra also drew attention to its obligations under the Privacy Act suggesting that clarification was required:

[W]e also operate under a requirement in the Privacy Act to destroy or de-identify data once no longer required for purposes for which they were collected. This could be interpreted as meaning we are legally required to immediately destroy or make amendments to the data retained under the Bill as soon as the two year retention period has ended thereby creating a further rolling obligation and additional cost on industry unrelated to commercial purposes that we have not yet factored into our assessment of the Bill. To help limit this impact, we believe that if there are to be different data retention periods across technologies as part of this scheme, we would recommend that telecommunication service providers be given the option of retaining data for the longest permitted period without breaching the law.¹²⁶

1.137 This section examined the government's announcement to introduce mandatory data retention and the main concerns that have been raised in relation to the government's proposal. The next section looks briefly at the international experience of those jurisdictions which have pursued mandatory data retention.

¹²⁴ Ms Anna Harmer, Attorney-General's Department, *Proof Committee Hansard*, 17 December 2014, p. 7.

¹²⁵ Law Council of Australia, *Submission 126 to PJCIS inquiry*, pp. 25–26.

¹²⁶ Telstra, *Submission 112 to the PJCIS*, p. 5.

International developments

1.138 Australia is not the only jurisdiction considering data retention and related privacy issues. However, several data retention regimes in other countries have recently been wound back. This section reflects on the international experience with mandatory data retention.

Is international practice moving away from mandatory data retention?

1.139 On 15 March 2006, the European Parliament and the Council of the European Union issued Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.¹²⁷ Directive 2006/24/EC also amended Directive 2002/58/EC.¹²⁸ In part, it required the European Union (EU) to:

- retain certain categories of data¹²⁹ (Article 3) for a period of 'not less than six months and not more than two years from the date of the communication' (Article 6);
- ensure access to data is provided only 'to the competent national authorities in specific cases and in accordance with national law' and that the procedures and conditions followed to access the data accord with the requirements of necessity and proportionality as defined in each Member State's national law subject to EU law, public international law and 'in particular the ECHR as interpreted by the European Court of Human rights' (Article 4); and
- ensure the protection and security of the data, including destroying the data at the end of the retention period (Article 7).¹³⁰

1.140 In an April 2014 ruling, the Court of Justice of the European Union (ECJ) found that the European Data Retention Directive was invalid. The regime was overturned by the ECJ on the grounds that it 'entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the

127 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> (accessed 26 February 2015). A copy of Directive 2006/24/EC is set out in Appendix 5.

128 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> (accessed 26 February 2015). Directive 2002/58/EC concerned the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). See: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML> (accessed 3 March 2015).

129 The categories of data required to be retained are set out in Article 5 of Directive 2006/24/EC. The definitions for the purposes of the directive are set out in Article 2.

130 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF> (accessed 26 February 2015).

protection of personal data, without that interference being limited to what is strictly necessary'.¹³¹

1.141 In a statement advising of its decision, the ECJ stated that 'by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interfere[d] in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data' and that 'the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance'.¹³²

1.142 The Court went on to explain that it was then for it to examine 'whether such an interference with the fundamental rights at issue [was] justified' and that it was of the opinion that:

...by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.

In that context, the Court observe[d] that, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by the directive, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

1.143 The Court also set out that:

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.

Firstly, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have access to the data and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime'

131 <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (accessed 26 February 2015). See also: Ms Lindy Stephens, Global Director of People Operations, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 1.

132 <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (accessed 26 February 2015).

as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.

Thirdly, so far as concerns the data retention period, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

The Court also finds that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data. It notes, *inter alia*, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.

Lastly, the Court states that the directive does not require that the data be retained within the EU. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.¹³³

1.144 The Law Council explained that it shared the concerns of the ECJ and highlighted similarities with the proposed Australian scheme:

I note with interest the decision of the Court of Justice of the European Union this month that struck down the data retention directive and did so really because of the sorts of concerns that exist in the legal profession here in Australia. The directive there would be similar to a law here that would require data to be kept for perhaps two years. One of the reasons the directive was struck down was that there was no real differentiation of what sort of data was to be kept. Data that was entirely innocent needed to be kept, along with data that might be likely to impact on national security issues or serious crime investigation issues. There was a problem about the length of time that data was to be kept; the proposal in each case considered

133 <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> (accessed 26 February 2015).

by the court there was six months. The risk of abuse inherent in that scheme seemed to be at the heart of the decision.¹³⁴

1.145 Despite the decision of the ECJ, the committee also received evidence from Australian law enforcement agencies that in their view, the decision does not necessarily have implications for Australia. The then Acting Chief Executive Officer of the Australian Crime Commission (ACC) addressed some, but not all the issues raised by the ECJ:

I am aware of the Court of Justice decision. I think what is important is the basis of that decision. There were about four key points that they referenced and my reading of it is that it does differentiate a little from the environment we have here in Australia. I would argue that in a number of those cases we already mitigate some of the risks that were identified. For example, one of the bases that the Court of Justice identified was that there was no protection against the risk of abuse. From my perspective, our oversight regime does protect from the risk of abuse. Whilst I am aware of the Court of Justice decision, I would equally argue that our oversight regime both from a legislative perspective and even a policy perspective differentiates from what the European Union appears to have discovered in their Court of Justice decision.¹³⁵

1.146 The department argued, that '[t]he Court's finding was not because data retention was inherently unconstitutional... Instead, the Court's judgment was based on the lack of appropriate safeguards and limits within the Directive itself...'¹³⁶ and that although the invalidation of the Directive had resulted 'in the annulment of a number of data retention laws in member States where the Directive was implemented... many European countries [were] actively working to address the issued identified by the Court. For example, the then Director-General of ASIO told the committee:

Notwithstanding the decision of the [European Court of Justice], Britain decided just a couple of weeks ago that they would implement that regime. They made no bones about why they need it. The court said it did not contain sufficient safeguards for implementation across EU member-states and the way it was framed violated the principle of proportionality under EU law. But it did acknowledge that data retention genuinely satisfies an objective of general interest, mainly the fight against serious crime and ultimately public security.¹³⁷

1.147 The then Director-General of ASIO added that:

I suspect the debate, discussion and, indeed, legal processes in Europe are not yet completed. It would be wrong of us to jump to one judgement of the

134 Mr Phillip Boulten SC, Law Council of Australia, *Proof Committee Hansard*, 23 April 2014, p. 3.

135 Mr Paul Jevtovic APM, Australian Crime Commission, *Committee Hansard*, 22 April 2014, p. 10.

136 Attorney-General's Department, *Submission 27 to the PJCIS inquiry*, p. 39.

137 Mr David Irvine, ASIO, *Committee Hansard*, 21 July 2014, p. 16.

European court in relation to one aspect of data retention to rule it out as a gross violation of human rights across the board.¹³⁸

1.148 iiNet Limited (iiNet) explained that, in its view, the shift internationally is away from mandatory data retention and provided examples of how various European jurisdictions had responded to the decision of the ECJ.¹³⁹ The Attorney-General's Department (department) provided a concise summary of the data retention regimes in the European Union as they currently stand: the summary indicates those jurisdictions that have annulled mandatory data retention since the decision of the EU Court of Justice:

138 Mr David Irvine, ASIO, *Committee Hansard*, 21 July 2014, p. 16.

139 iiNet Limited, answer to a question taken on notice, received 11 August 2014, p. 1.

Country	Retention period	Access method
Latvia	18 months	Judicial authorisation for traffic data. Police authority for subscriber information.
Liechtenstein	6 months	
Lithuania	6 months	Internal authorisation
Luxembourg	6 months	
Malta	Between 6 and 12 months	Internal authorisation
Netherlands	6 months for IP address allocation 12 months for telephony	Hybrid – Internal authorisation for security agencies and less-intrusive law enforcement requests; prosecutorial warrant for more intrusive law enforcement requests.
Norway	6 months Entered into force on 1 January 2015	
Poland	2 years	Internal authorisation
Portugal	12 months	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Romania	Previously 12 months Annulled as a result of the annulment of the EU Data Retention Directive	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Serbia	12 months	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Slovakia	Between 6 and 12 months Temporarily suspended while under judicial consideration	
Slovenia	Previously 12 months Annulled as a result of the annulment of the EU Data Retention Directive	Internal authorisation
South Africa	3 years	
Spain	Between 6 months and 2 years	Internal authorisation
Sweden	6 months	
Switzerland	6 months Laws before Parliament to increase to 12 months	
Turkey	Between 6 months and 2 years	
United Kingdom	12 months, with extraterritorial application	Internal authorisation for most agencies. However, local authorities require a warrant from a judicial officer.
United States	18 months (telephony only)	Internal authorisation

Country	Retention period	Access method
Austria	Previously between 8 and 14 months Annulled following the annulment of the EU Data Retention Directive	Internal authorisation
Belgium	Between 12 months and 3 years	Warrant issued by a judicial officer or a public prosecutor
Brazil	6 months for web browsing history 12 months for IP address allocation	
Bulgaria	12 months	Warrant issued by a judicial officer
Cyprus	Previously 6 months Annulled in 2011	Warrant issued by a judicial officer
Czech Republic	Previously between 6 and 12 months. Annulled as a result of the annulment of the EU Data Retention Directive Currently drafting new laws	Internal authorisation
Denmark	12 months Denmark previously required internet service providers to also retain web-browsing information for 1 in every 500 packets sent over the internet. This requirement was removed in mid-2014, following advice from agencies and prosecutors that there were technical difficulties in obtaining useful information from only 0.2% of such traffic. Annulled but will reintroduce in January 2015	Warrant issued by a judicial officer
Estonia	12 months	Prosecutor authorisation
Finland	12 months	No authorisation required for subscriber information. Judge's authority for traffic data.
France	12 months	Authorisation from the Interior Ministry (from 1 January 2015)
Germany	Previously 6 months Annulled in 2010 Draft amendments to Telemedia Act for limited data retention	Internal authorisation
Greece	12 months	Warrant issued by a judicial officer
Hungary	12 months	Internal authorisation
Iceland	6 months	
Ireland	Between 12 and 24 months	Internal authorisation
Italy	12 months for IP address allocation 2 years for telephony	Hybrid – public prosecutor or, in the case of organised crime or counter-terrorism, an internal authorisation.

Source: Attorney-General's Department, *submission 27 to the PJCIS inquiry*, pp. 55–56.

1.149 The department was unable to point to any jurisdiction where the winding back of data retention or the requiring a warrant to access metadata had caused law enforcement activities to 'grind to a halt':

CHAIR: Ms Jones, are you aware that law enforcement has not ground to a halt in Belgium, Bulgaria, Denmark, Greece, Latvia, the Netherlands, Portugal, Romania and Serbia, which are all countries that, according to your very helpful appendix to your submission, have some form of judicial oversight of telecommunications authorisations? Why do you think it would grind to a halt in Australia? What evidence do you have to back that up?

Ms Jones: We have obviously been discussing this with agencies in terms of their operational experience of the importance of being able to access data information as quickly as possible early in the process.

I note that you have listed a number of countries, but we have also looked at the experience in the United Kingdom, where they have recently had to look at the regime that they had in relation to warrants because essentially their operational experience was that it became virtually unworkable and that the number of successful authorisations was significantly reduced. There was a report to the UK Parliament by the Interception of Communications Commissioner that noted that it was causing significant delay in the progress of many investigations.

CHAIR: Do you have any evidence that in any of the countries I just listed law enforcement has ground to a halt or that there has actually been any impact at all on the efficiency of law enforcement?

Ms Jones: We have not discussed the specifics with those countries. Is there anything further you can add?

Ms Harmer: No, we have not engaged directly.

CHAIR: It is a pretty big deal to come in here and make sweeping statements like, 'Law enforcement will grind to a halt unless we are allowed to continue vast, warrantless access to telecommunications data.' It is a pretty big call and you have no evidence that in any of those countries that has been the case.

Ms Jones: We are focused on the experience in the Australian context, on talking with agencies in Australia, and this is an issue that we have discussed before the Parliamentary Joint Committee on Intelligence and Security.

CHAIR: Yes, but you are here now with us. What evidence do you have either in the countries that have a standing data retention regime or in those in Europe that had one that was then annulled—Germany being one example—of improvements in the rate of clearance of crimes? Is there any evidence from any country at all that you could point to where data retention has led to an improvement in the rate of crime clearance?

Ms Harmer: I think one of the challenges in that regard is the extent to which data as a single investigative resource can be said by itself to improve clearance rates. I expect you may have in mind a German report which suggests that there was a limited improvement or what has perhaps been characterised as negligible improvement in clearance rates as a result

of the introduction of data retention there. What the clearance rate reflects, of course, is the number of crimes solved as opposed to the number of crimes on hand. What access to data does is to provide the starting point for investigations and allow them to proceed further, or indeed to commence at all. In that regard, while there is that German report, I think it was only a fortnight ago that German Chancellor Merkel indicated her intention to lobby the EU for a new data retention directive, noting the very significant importance of data retention from her perspective to German investigations.

CHAIR: You have still managed to avoid the question. Do you have any evidence from any jurisdiction at all that mandatory data retention either reduces crime or improves the rate at which crimes are solved? You may not have it at the table, but is there anything at all that you could point me to?

Ms Harmer: The evidence in support of data retention is not cast in terms of clearance rates; it is cast in terms of—

CHAIR: Or crime rate? I will take any metric you care to name.

Ms Harmer: Perhaps in that regard I could refer you to some of the evidence of the law enforcement agencies who appeared last Friday. From an investigative perspective, it is the case that it is extremely difficult to point to data as one investigative tool having a direct and quantifiable impact on the number of prosecutions and convictions. The way in which law enforcement agencies apply metrics to assess their effectiveness and their prosecutions and convictions is not able to hinge back to a single data point. Accordingly—

CHAIR: I am not talking about a single data point but the whole category of data retention or metadata access in general. It is the opposite of evidence based policy; it is anecdote based policy.

Ms Jones: It is policy based on very strong advice from the agencies who have responsibilities in relation to law enforcement and national security.

CHAIR: Of course they want more power. It is your job and ours to balance that power against proportionality and whether it is useful or not. I am just asking for evidence as to whether it is useful. All right—we will move on.¹⁴⁰

1.150 In fact, the committee heard that Germany has moved in the opposite direction to mandatory data retention, implementing a policy known as 'datensparsamkeit' or 'data austerity' which places the onus on government agencies, departments and business to 'collect only that data which is necessary and proportionate'.¹⁴¹

140 Ms Katherine Jones, Deputy Secretary, National Security and Criminal Justice Group, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, pp. 52–53; and Ms Anna Harmer, Acting First Assistant Secretary, National Security Law and Policy Division, Attorney-General's Department, *Proof Committee Hansard*, 2 February 2015, pp. 52–53.

141 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 2.

1.151 ThoughtWorks expressed the view that what is 'necessary and proportionate' is a difficult concept to define and 'does depend on the individual circumstances'.¹⁴² ThoughtWorks cautioned however that as 'technology moves at a pace that is ahead of business and ahead of decisions and laws':

...people are doing things because they are technologically possible, not because they are a good idea. So we are asking that businesses—and this is what we do ourselves—actually stop and think and make a decision: do they need that particular piece of data in order to serve their customers, in order to provide the services they provide, or is it just something they think they might need in the future?

It is really more about stopping and asking whether you are collecting data just for the sake of it or whether you really need it to do business.¹⁴³

1.152 During its inquiry the committee also received evidence that in a 30 June 2014 report of the United Nations (UN) High Commissioner for Human Rights titled 'The right to privacy in the digital age', the High Commissioner 'strongly emphasis[ed] the complicity of business in mass surveillance and in violating the right to privacy'.¹⁴⁴ ThoughtWorks further explained the concerns of the UN High Commissioner:

The former high commissioner outlined a few key points in her report...The first one is that she asserts that states have a positive obligation under international law to protect citizens from surveillance by private or state entities and that bulk collection and the very existence of mass surveillance, whether the information is used or not, interferes with the right to privacy. She also asserted that mandatory third-party retention is surveillance and that it is neither necessary nor proportionate and insists that a distinction between content and metadata is no longer persuasive. In other words, there is no longer any real distinction between metadata and content. The crucial finding applies the effective control doctrine under international law to internet infrastructure. So, states are obliged to extend human rights protections to whoever's privacy is interfered with by internet infrastructure on their territory.¹⁴⁵

1.153 The Chair also noted the similarly titled June 2014 Report of the Australian Law Reform Commission (ALRC) *Serious Invasions of Privacy in the Digital Era*, in which the ALRC advised:

...privacy has been said to lie at the heart of liberty, and will often support other fundamental rights and freedoms, sometimes it must be balanced with other important interests... [however] privacy should not be casually 'traded off' for the sake of other important interests.¹⁴⁶

142 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 3.

143 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 3.

144 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 1.

145 Ms Lindy Stephens, ThoughtWorks, *Committee Hansard*, 26 September 2014, p. 2.

146 ALRC Report 123, June 2014, p. 35.

Alternatives to mandatory data retention

1.154 Submitters to the inquiry also suggested that mandatory data retention should not be pursued before alternatives are considered.

1.155 The Australian Privacy Foundation explained that, in its view, mandatory data retention is not necessary as the existing preservation notice regime set out in the TIA Act 'should be sufficient to provide agencies with what they need'.¹⁴⁷

1.156 iiNet shared this view stating that '[t]argeted preservation notices used together with stored communications warrants provide an alternative framework to mass data retention that is designed to ensure that any retention and access to private data is necessary and legitimate'.¹⁴⁸ The Institute of Public Affairs (IPA) was of a similar view. In evidence to the committee, the IPA expressed that:

It is also worth noting that it has not been adequately shown that preservation orders are not adequate to achieve the aims of the law enforcement. Stored preservation orders are targeted, proportional data retention schemes that offer a flexible and privacy-protecting mechanism to law enforcement agencies. It is striking to us how rarely the existence of this mechanism is discussed in the data retention debate when it would seem to resolve all the problems with the TIA act that have been identified by law enforcement agencies.¹⁴⁹

1.157 This view however was specifically discounted in the Minister's second reading speech when he explained that the '[e]xisting powers and laws are not adequate to respond to this challenge'.¹⁵⁰ The department further explained the government's view that the often cited alternative of the existing preservation regime was insufficient:

[T]he Department's view, supported by international experience, is that expanding the existing preservation notice regime would not address the capability challenges faced by agencies.

Preservation and data retention are complementary tools, but are aimed at different objectives. 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. For example, a preservation

147 Mr Nigel Waters, Australian Privacy Foundation, *Committee Hansard*, 29 July 2014, p. 31. The preservation notice regime, set out in Part 3-1A of the TIA Act, establishes a system of preserving certain stored communications that are held by a carrier. The purpose of the preservation is to prevent the communications from being destroyed before they can be accessed under certain warrants issued under the Act.

148 iiNet Limited, Answers to questions taken on notice, received 11 August 2014, p. [5].

149 Mr Simon Breheny, Director, Legal Rights Project, Institute of Public Affairs, *Committee Hansard*, 26 September 2014, p. 8.

150 The Hon Malcolm Turnbull MP, Minister for Communications, Second Reading Speech, *House of Representatives Hansard*, 30 October 2014, p. 12560.p.

notice issued 9 months after a criminal event cannot assist an investigation if the data sought was destroyed after just 1 month's existence.

Preservation notices will not, therefore, address the fact that service providers are not retaining critical types of telecommunications data, or are retaining that data for shorter periods of time. In addition, as the current data authorisation provisions in Chapter 4 of the TIA Act already facilitate timely access to telecommunications data for legitimate investigative purposes, the Australian Government did not need to include preservation notices for telecommunications data in the Cybercrime Act.

By comparison, the purpose of data retention is to introduce a consistent record-keeping requirement across industry to ensure that certain telecommunications data are consistently available. As such, data retention is in fact a prerequisite to preservation of data, rather than preservation offering an alternative to retention.¹⁵¹

1.158 This section has looked briefly at the European experience with data retention. The final section sets out the Chair's view and recommendations in respect of the proposed mandatory data retention regime.

151 Attorney-General's Department, *Submission 27* (to the PJCIS inquiry), p. 17.

Chair's views and recommendations: mandatory data retention

Introduction

1.159 The Chair's views and recommendations set out below are made in respect of the policy of mandatory data retention in the context of the government's proposal set out in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Bill).

1.160 The Chair notes that, at the time of tabling its report, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) had finalised its inquiry into the Bill and the government had issued a response. The Chair is heartened by the government's announcement that it supports all 39 recommendations put forward by the PJCIS. However, although the Chair agrees with some of the recommendations of the PJCIS, he considers that others must go further and hopes that the government responds with similar speed and timeliness to this report and recommendations.

Broader reform is required

1.161 The Chair takes the view that the government's announcement that it will seek to implement mandatory data retention makes the need for the rationalisation and updating of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to be considered holistically more pressing. The Chair trusts that this inquiry will assist in moving towards a TIA Act which is more adapted both to contemporary technology and to the public's more evolved expectations in relation to privacy.

1.162 The Chair is opposed to the introduction of a mandatory data retention regime and draws attention to the failed pursuit of such regimes internationally. It is particularly concerning that the government is considering requiring the retention of data even if it serves no business purpose and would therefore only be retained as a result of this new regime. The Chair references the international experience and suggests that the German approach of retaining only that which is both necessary and proportionate, 'datensparsemkeit', should guide policy and law makers.

1.163 The Chair is critical of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 currently before Parliament. The regime being proposed equates to mass surveillance. It should not proceed. The grounds for implementing a policy of mandatory data retention have not been established to the Chair's satisfaction.

1.164 The implications for the right to privacy and freedom of the press must not be traded away without careful consideration or in the absence of adequate legislative safeguards.

1.165 Throughout its inquiry, the committee received evidence clearly illustrating that what was collected as telecommunications data in 1979 was a small fraction of what is collected as telecommunications data in 2015. The evidence illustrated the difficulties of defining 'telecommunications data' yet clearly showed that telecommunications data today provides a much fuller picture of a person's social connections, values, personal preferences and habits. It is clear to the Chair that the

analogy of the envelope and the letter no longer describes the distinction between content and metadata in the digital age.

Recommendation 4

1.166 The Chair recommends that the government not proceed with a mandatory data retention regime and that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be withdrawn.

The need for a definition

1.167 The Chair considers that a definition of 'telecommunications data' or 'metadata' must be settled and incorporated into a redrafted *Telecommunications (Interception and Access) Act 1979* (TIA Act). A definition should be developed by industry, together with government and privacy advocates. Until a definition is settled, the scope, cost and privacy implications of any proposed data retention regime remain unquantifiable.

1.168 The Chair does not support the proposed definition of 'telecommunications data' set out in the Bill currently before the parliament. The Chair agrees with Recommendation 2 of the PJCIS that the Bill should be amended to include the proposed data set in primary legislation.¹⁵² However, the Chair suggests that revisions to the definition of the data set go further and identify those elements within the data set that constitute the 'information that allows a communication to occur'¹⁵³ and 'basic subscriber data'¹⁵⁴ and identify that any change to the parameters of the data set must occur through the legislative process.

1.169 The Chair considers that the evidence received by the PJCIS that industry will find it 'very challenging' to separate the content from the metadata for some types of data further supports its view that different elements of the data set have greater privacy implications than others and adds weight to calls for the introduction of a warranted access regime for data that is 'information that allows a communication to occur'.¹⁵⁵

152 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 79.

153 Data that is 'information that allows a communication to occur' includes for example: the internet identifier (information that uniquely identifies a person on the internet) assigned to the user by the provider; for mobile service: the number called or texted; the service identifier used to send a communication, for example the customer's email address, phone number or VoIP number; the time and date of a communication; general location information, that is, cell tower; and the duration of the communication.

154 Data that is 'basic subscriber data' would include for example: name of the customer; address of the customer; postal address of the customer (if different); billing address of the customer (if different); contact details, mobile number, email address and landline phone number; and same information on recipient party if known by the service provider.

155 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 100.

Access to telecommunications data

1.170 The Chair acknowledges that 'basic subscriber data'¹⁵⁶ should be able to be accessed without a warrant but maintains that access to data that is 'information that allows a communication to occur'¹⁵⁷ should occur via warrant.

1.171 The Chair notes that evidence received by the PJCIS during its inquiry into the proposed mandatory data retention regime was overwhelmingly supportive of the introduction of warranted access to metadata yet the PJCIS dismissed that evidence on the basis that it would 'impede the operational effectiveness of agencies...to the detriment of the protection of the Australian community'.¹⁵⁸ The Chair disagrees with this assessment and suggests that differentiating between 'basic subscriber data' and data that is 'information that allows a communication to occur' and requiring the latter category of data to be accessed only via warrant, would in fact better balance the important public interests of privacy and security.

1.172 The Chair notes the government's proposal to amend the definition of 'enforcement agency' for the purposes of accessing telecommunications data and supports the principle of restricting access to telecommunications data through tightening the definition of 'enforcement agency' for the purposes of Chapter 4 of the TIA Act. However, the Chair is opposed to proposed new subsections 176A(3) and 176A(4) which would provide the Attorney-General with a discretion to declare an authority or agency to be an 'enforcement agency' for the purposes of accessing telecommunications data. Furthermore, the Chair considers that access to metadata should also be limited through a revision of the associated proportionality test. The Chair acknowledges Recommendation 25 of the PJCIS report¹⁵⁹ but maintains that it does not go far enough.¹⁶⁰ In the absence of a concurrent revision of the

156 For example, data identifying information such as the name, address and contact details of a customer.

157 For example, data including the internet identifier, service identifier, and geo-location data.

158 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 245.

159 Recommendation 25 of the PJCIS report stated:

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 of 4A of Part 4-1 of the Act, the authorised officer 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.

160 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 251.

proportionality test to restrict access to metadata to situations where it is 'necessary' for the investigation of specified serious crimes or categories of serious crimes, reform will be neutered.

1.173 The Chair also notes that throughout this inquiry the government has stated that calls for a revision of this proportionality test would be inconsistent with Australia's obligations under the European Union Convention on Cybercrime. The Chair does not agree with this position and is frustrated by the government's willingness to preference a minor Council of Europe convention over Australia's obligations under international human rights law and the fundamental right to privacy of its citizens.

The proposed retention period

1.174 The Chair is concerned by the data retention period proposed in the Bill of two years. The Chair disagrees with Recommendation 9 of the PJCIS report which recommends that the two-year retention period specified in the Bill be maintained and its finding that two years is 'the minimum amount of time that would be acceptable from a national security and law enforcement perspective'.¹⁶¹ The Chair believes that the proposed retention period of two years is out of step with international jurisdictions, many of which are moving in the opposite direction. The Chair notes the evidence that both this committee and the PJCIS received, which identified that in the majority of cases where metadata is used for law enforcement purposes, it is less than 12 months old.

A destruction requirement

1.175 The Chair is very concerned by the absence in the Bill of a destruction requirement when data is no longer required. In the Chair's view the absence of a destruction requirement directly contradicts the Australian Privacy Principles (APP's), particularly APP 11. The Chair notes Recommendation 28 of the PJCIS 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 [TIA Act] and held by enforcement agencies and ASIO'.¹⁶² The Chair believes that this recommendation does not go far enough and the Bill should be amended to include an express requirement to destroy data after the data retention period has expired or the information is no longer needed. The Chair does, however, support Recommendation 35 of the PJCIS which calls for the APP's to apply to all service providers regardless of their turnover.¹⁶³

161 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, pp. 145–147.

162 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 262.

163 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 297.

Oversight

1.176 The Chair supports the proposed new oversight and inspection regime set out in Schedule 3 of the Bill. The Chair considers however, that Schedule 3 of the Bill should be further strengthened by the inclusion of a requirement that enforcement agencies also retain records in relation to:

- the type and age of metadata requested;
- the offences to which a request relates; and
- any outcomes following the request.

1.177 This data should be included in the annual report of the Attorney-General's department.

1.178 The Chair notes that the requirement for the Commonwealth Ombudsman to inspect records in proposed Chapter 4A, does not identify a timeframe for inspection. The Chair considers that this should be addressed through the inclusion of a provision requiring the Commonwealth Ombudsman to examine the records of each agency which has access to metadata every six months.

1.179 The Chair acknowledges that the introduction of a comprehensive inspection and oversight regime will have significant resourcing implications for the Commonwealth Ombudsman and therefore echoes Recommendation 29 of the PJCIS which calls for additional financial resources for the Commonwealth Ombudsman to ensure it can carry out a broader role of overseeing access to telecommunications data. However, the Chair suggests that the resources sought by the PJCIS in Recommendation 32 would be better allocated to assist the Commonwealth Ombudsman and the Inspector General of Intelligence and Security with the independent statutory oversight functions of those offices.

Protection of press freedom

1.180 In its report on the Bill, the PJCIS recommended that further inquiry is needed before recognition of 'the principle of press freedom and the protection of journalists' sources' in the Bill is finalised.¹⁶⁴ Although the Chair supports this recommendation, he is of the view that this inquiry extend to other professions, for example, medical professionals and lawyers, where the integrity of the profession depends upon privacy and confidentiality. The Chair suggests that this issue be resolved and protections for these classes of professions be included in the Bill before it is considered by the Parliament.

Mandatory data breach notification scheme

1.181 The Chair expresses his support for the PJCIS's recommendation (Recommendation 38) to implement a mandatory data breach notification scheme by the end of 2015 and agrees with the PJCIS that 'there must be a [mandatory data breach notification] scheme in place prior to the implementation of the Bill' as it

164 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 258.

'would provide a strong incentive for service providers to implement robust security measures to protect data retained under the data retention regime'.¹⁶⁵

Recommendation 5

1.182 If the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 is not withdrawn the Chair recommends that the Bill be amended to:

- **include a definition of 'telecommunications data' in the primary legislation;**
- **identify in the definition of 'telecommunications data' the elements of the data set as either 'information that allows a communication to occur' or 'basic subscriber information';**
- **delete proposed subsections 176A(3) and 176A(4) which provide the Minister with the ability to declare an authority or agency to be an enforcement agency for the purposes of accessing metadata;**
- **amend the proportionality test set out in existing sections 177, 178 and 179 of the *Telecommunications (Interception and Access) Act 1979*. The Australian Privacy Commissioner, Law Council of Australia and the Australian Human Rights Commission are to be consulted in amending the proportionality test associated with accessing telecommunications data;**
- **include a requirement for data that is 'information that allows a communication to occur' to be accessed only via warrant;**
- **reduce the mandatory data retention period from two years to three months;**
- **include a requirement that all data be stored in Australia;**
- **include a requirement to destroy telecommunications data after the mandatory retention period or when it is no longer needed;**
- **include protections for sensitive classes of professionals including journalists and their sources, medical professionals, and lawyers;**

165 PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, pp. 298–299.

- **amend proposed section 186A to include a requirement that the following information also be kept by an agency:**
 - **the type of metadata requested;**
 - **the age of the metadata requested;**
 - **the offence(s) which the request related to;**
 - **the outcome following the request;****and include a requirement in proposed section 187P that this information be reported in the Attorney-General's annual report to the Parliament;**
- **amend proposed section 186B to include a requirement that the Commonwealth Ombudsman examine the records of each agency which has access to metadata every six months;**
- **amend proposed section 187N (Review of operation of Part) to require both the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor to review the data retention regime on a triennial basis; and**
- **introduce a mandatory data breach notification regime.**

Recommendation 6

1.183 The Chair recommends that the government introduce a statutory right to privacy, similar to that which exists in the United Kingdom, rather than relying on international human rights instruments.

Divergent views on '5 Eyes' collaboration

1.184 The Chair notes that there is significant variance between the evidence presented by Australian law enforcement agencies and oversight bodies, and the revelations about international surveillance and information sharing provided by whistleblowers and some elements of the media.

1.185 WikiLeaks publisher Mr Julian Assange, who has been instrumental in publishing a large volume of information from within many governments, told the committee in WikiLeaks' submission¹⁶⁶ that the nature of information-sharing among the so-called "5 Eyes" countries (the United States, Canada, the UK, Australia and New Zealand) had been 'fundamentally misrepresented'. Mr Assange said:

When asked about the information sharing practices of the 5 Eyes, the Committee heard on 23 April 2014 from Assistant Inspector General Blight from the Office of the IGIS that "... data sharing about Australian persons for ASD is regulated tightly by the Intelligence Services Act and the privacy rules made under that act and that data about Australian persons is subject to quite strict oversight .

In fact, the revelations of Edward Snowden have documented shared and integrated 5 Eyes databases, and that untargeted, bulk interception,

166 WikiLeaks, *Submission 46*.

collection and sharing of algorithmic analysis of private communications are routine among the 5 Eyes intelligence agencies.

It is absurd that Australian government agencies continue to misrepresent the nature of interception and their access to intercepted data via 5 Eyes sharing arrangements when their equivalents in the UK have acknowledged their role in mass surveillance, including through convenient interpretations of domestic laws to absorb "external communications" which includes all communications transiting Internet platforms and services such as Google, Skype, Facebook, Yahoo not based in the UK.

1.186 Mr Assange particularly drew the committee's attention to documents submitted to the UK Investigatory Powers Tribunal by Mr Charles Blandford Farr, the Director-General of the UK Government's Office for Security and Counter-Terrorism. Mr Blandford Farr's attendance at the Tribunal attracted attention in June 2014 particularly for his comments that UK intelligence services could legally intercept communications through social media and webmail services operated by companies such as Google and Facebook.

1.187 Mr Assange also drew the committee's attention to the US NSA XKEYSCORE surveillance program, the UK Tempora program. He wrote:

This [XKEYSCORE] program includes a Five Eyes Defeat checkbox that allows analysts to filter out data from one or more of the Five Eyes countries. Such a check box makes sense only in the context of a default sharing of information among the 5 Eyes that inevitably and necessarily circumvents the [Telecommunications (Interception and Access) Act].

[IGIS] Dr. Thom confirmed that the "quite strict oversight" also applied to Australian citizens abroad. The Tempora program also revealed by Snowden refutes this simplistic assumption. Under that program, all 5 Eyes nations access data and metadata resulting from British tapping of fibre optic cable; there are no protections provided to Australians under such indiscriminate collection and sharing arrangements.

Amendments made to the Intelligence Services Act in 2011, including the "WikiLeaks Amendment" so dubbed by employees of the Attorney General's Department, greatly reduced the scope or meaning of protections for Australians overseas and greatly increased the surveillance of their communications permitted.

By expanding the scope of surveillance overreach to anyone that was "in the interest of Australia's national security, Australia's foreign relations or Australia's economic wellbeing," almost anyone could be caught, rendering the 'strict oversight' a gesture, a meaningless gesture in the context of mass surveillance, collection and sharing of intelligence.

Senator Scott Ludlam
Inquiry Chair

Additional Remarks from Government Senators

1.1 The government members of the committee acknowledge universal support for reform of the legislative scheme governing telecommunications interception and access.

1.2 Government members agree with the findings of the recent inquiry conducted by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 ('Data Retention Bill'), and support the PJCIS inquiry's recommendation that the Data Retention Bill be passed.¹

1.3 Government Senators acknowledge the tension that persists between the interests of individual privacy, and national security and note that this tension has been exacerbated by irresponsible public commentary and reporting around the issue of reform of the scheme governing telecommunications interception and access.

1.4 Government members of the committee prefer to view these so-called 'competing' interests—personal/professional privacy, and national security—as inherently complementary interests, and urge a consensus approach to reform.

1.5 The government members of the committee reject the Chair's Report on data access and data retention as an over-simplification of the complex relationship between the complementary interests of national security and individual privacy. The Chair's report examines data retention from a highly biased perspective, and irresponsibly recommends additional layers of tax-payer-funded oversight that duplicate existing protective frameworks and are of limited or no utility.

The Reform Agenda

1.6 The current scheme governing telecommunications interception and access pre-dates mobile telephony and both mobile and fixed data services. It is no longer practicable to rely upon successive amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to accommodate the pace and breadth of technological change.

1.7 The committee's inquiry revealed a wide range of views regarding the preferable characteristics for reform of the TIA Act. These views overwhelmingly focused on protecting national security, protecting individual rights to privacy, and enhancing administrative efficiencies.

1 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p.xxv.

1.8 Any programme of reform must balance individual interests and national interests with sensitivity, maturity and common sense. The need for balance was clearly expressed by the Australian Law Reform Commission (ALRC) following its 2006-8 review of the *Privacy Act 1988* (Cth):

As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. International instruments on human rights and growing international and domestic jurisprudence in this field all recognise that privacy protection is not an absolute.²

Streamlining the Warrant Regime

1.9 Compelling evidence was received during the inquiry regarding the complexity of the existing scheme governing warranted access to telecommunications content and metadata. The administrative burden created by intricate process requirements was described *inter alia* by the Director-General of Security:

Over time, the many amendments to the TIA Act have resulted in duplication and complexity making the Act difficult to understand and apply.³

1.10 Government members of the committee support recommendations from law-enforcement and national security agencies calling for the introduction of a single attribute-based warrant scheme for content retrievals and interceptions.⁴ Government Senators are persuaded that the targeted nature of attribute-based warrants will lend efficiency and expedience to investigative practices, as well as protecting individual rights to privacy through the observance of proportionality thresholds.

1.11 In supporting the introduction of a single attribute-based warrant scheme ASIO and the ACC noted the need to maintain 'proportionality thresholds and accountability requirements...to deliver public confidence and assurance regarding the use of these powers'.⁵ The Law Council of Australia (Law Council) explained:

...where a State seeks to restrict human rights, such as the right to privacy, for legitimate and defined purposes, for example in the context of telecommunications access and interception, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective. In the context of

2 *For Your Information – Australian Privacy Law and Practice*, Australian Law Reform Commission (ALRC) Report #108, p. 104.

3 ASIO, *Submission 27*, p. 34.

4 For example ASIO, *Submission 27*, p. 26; Attorney-General's Department (AGD), *Submission 26*, pp. 16-19.

5 ASIO, *Submission 27*, p. 35. See also: ACC, *Submission 23*, p. 14.

telecommunications access and interception, this involves balancing the intrusiveness of the interference, against operational needs.⁶

1.12 The government members are satisfied that proportionality thresholds are satisfactorily maintained by relevant agencies, through existing procedural and oversight functions, to a standard that may reasonably be anticipated by the community-at-large.

1.13 The government members of the committee are strongly of the view that the utility of a single attribute-based warrant scheme should not be compromised through the imposition of cumbersome and unnecessary limitations or exceptions.

1.14 The protections that are currently conferred upon citizens' in relation to metadata will be substantially improved by the passage of the government's Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

1.15 Government members of the committee acknowledge the privacy implications of changes to warranted access however they are reassured by the government's unambiguous commitment to the preservation of individual privacy within the imperatives of the contemporary risk environment.

Oversight and the Commonwealth Public Interest Monitor

1.16 There is a range of existing oversight mechanisms for access to data and content, including in certain circumstances warrant regimes. These oversight functions protect the public interest in the preservation of individual privacy, as well as the public interest in the protection of national security.

1.17 The government members of the committee are satisfied that existing oversight functions are sufficient and that the introduction of a Commonwealth Public Interest Monitor would unnecessarily duplicate existing processes at the tax-payers' expense. Government members of the committee do not consider that this would reflect the public interest.

Metadata – Definition

1.18 The need for reform to the TIA Act is substantially due to the existing scheme's inability to accommodate the pace and breadth of technological change. The government members of the committee are mindful that inclusion of a prescriptive definition of 'metadata' in the legislative scheme could limit investigative scope in future, thus requiring amendments of the type and frequency that have led to the complexity found in the existing scheme.

6 Law Council of Australia, *Submission 34*, p. 5.

1.19 Government members encourage further consultation regarding the technology-neutral definition of all terms across any proposed reform of the TIA Act.

Mandatory Data Retention

1.20 Government Senators fully support the mandatory data retention scheme that is contemplated by the Data Retention Bill that is presently before the Parliament as fundamental to Australia's national security and law enforcement priorities.

1.21 National security and law enforcement agencies have unanimously and unambiguously identified the value derived from telecommunications data in the conduct of investigative activities.⁷

1.22 The Attorney-General's Department has stated that the increasing need for data retention has resulted from technological developments and consequential changes in the business practices of service providers:

Historically, service providers have generated and retained telecommunications data for their business purposes. However, as providers shift to modern, IP-based networks and services, they are tending to retain a narrower range of data, and to retain that data for shorter periods.⁸

1.23 The government members of the committee acknowledge evidence that mandatory data retention has the potential to provide greater privacy to individuals who may otherwise fall under the gaze of law enforcement investigations where such investigations would be required to cast a wider net in the absence of retained data. For example, the ACC submitted that accessing retained data enabled it to conduct investigations without needing to intercept or access the content of a wider range of communications.⁹

1.24 The ACC noted however that the retention of telecommunications content and data by service providers in Australia is variable and subject to the storage capacity of the service provider in question. The resultant lack of a consistent national standard:

...results in uncertainty for law enforcement and can jeopardise the outcome of operations. These differences in retention periods create difficulties for the ACC in its ability to undertake investigations into federally relevant criminal activity, as valuable telecommunications data is not always available when needed. When it comes to conducting ACC investigations on long-term federally relevant criminal activity, access to retrospective telecommunications data is critical for the ACC to understand the scope and nature of the threat.¹⁰

7 AGD, *Submission 26*, pp. 3, 4; ASIO, *Submission 27*, pp. 5, 33, 39.

8 AGD, *Submission 26*, p. 30.

9 ACC, *Submission 23*, p. 15.

10 ACC, *Submission 23*, p. 15.

1.25 ASIO explained that it considered that a data retention period of 'at least two years in some cases' is required for it to effectively discharge its functions.¹¹

1.26 The Australian Federal Police also supported calls for a mandatory data retention regime, explaining that this would ensure a 'national and systematic approach is taken to safeguarding the ongoing availability of telecommunications data for legitimate purposes'.¹²

Objects Clause

1.27 Government Senators are of the view that the privacy interests of individual citizens are comprehensively protected by a range of existing legislated and regulated oversight functions.

1.28 The protection of individual personal privacy is also implicit in the operation of the TIA Act itself which was enacted to provide a scheme of regulation for the interception of and access to the communications of private individuals. Government Senators are mindful that a prescriptive statement of objectives could have the same limiting effect on this scheme as a prescriptive definition of 'metadata'.

1.29 The inclusion of an objects clause in the TIA Act as an additional clarification of privacy protections would be of limited utility.

Destruction requirement

1.30 Government members of the committee are of the view that service providers are likely to be sufficiently motivated by commercial considerations to purge stored data once any statutory retention period has elapsed and do not believe prescriptive destruction parameters would impact the frequency, immediacy or completeness of the destruction of stored data.

1.31 In addition, the *Privacy Act 1988* (Cth) provides a framework for the destruction of personal information where the information is no longer required under law or for a legitimate business purpose.¹³

Conclusions and Recommendations

1.32 The government members of the committee acknowledge the sensitivity and complexity of debate around the complementary interests of national security and individual rights to privacy. Technological developments such as the proliferation of data mobility have contributed to the intricacies of this debate.

11 ASIO, *Submission 27*, p. 27.

12 Australian Federal Police, *Submission 25*, p. 10.

13 *Privacy Act 1988* (Cth), ss 4 and 11.

1.33 Any scheme of reform of the TIA Act must measure the individual interest against the national interest as well as accommodating the interests of commercial operators. The government members of the committee support a considered approach that will focus on consultation in exploring all facets of reform of the TIA Act.

1.34 Government Senators agree with the findings of the PJCIS inquiry into the Data Retention Bill and acknowledge that the government has announced its support for all 39 of the PJCIS report's recommendations. Government members of the committee wholeheartedly support the passage of the Data Retention Bill, and the implementation of a mandatory data retention scheme, as a matter of national urgency.

Recommendation 1

1.35 The government members of the committee recommend the instigation of a single attribute-based warrant scheme to apply to telecommunications content.

Recommendation 2

1.36 The government members of the committee recommend that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be passed by the Senate.

**Senator the Hon Ian Macdonald
Deputy Chair**

Comments from Opposition Senators

The Opposition notes the earlier inquiries into the telecommunications interception regime in Australia, referred to in Chapter 1 of this report. In particular, the Opposition notes that following a year of extensive consultation and detailed consideration, in June 2013 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) tabled a unanimous report recommending wide-ranging reforms to Australia's national security legislation. In particular, the PJCIS conducted a comprehensive review of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), and in Chapter 2 of its 2013 Report made 18 recommendations for improvements to that legislative framework.

Labor members of this Committee endorse Recommendation 18 of the 2013 PJCIS Report, which states:

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.

Although the 2013 Report of the PJCIS was unanimous, and included the current Attorney-General as one of its members at the time, the Abbott Government has still not responded to the recommendations in Chapter 2, let alone commenced the considerable work outlined in Recommendation 18 above. Labor is also concerned that the Abbott Government chose to ignore the recommendations for a

comprehensive review of the TIA Act while pressing ahead with the introduction of a new data retention regime in the form of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Data Retention Bill). It is clear to Labor members of this Committee that improving the legislative framework for telecommunications interception and access should have been undertaken prior to the introduction of a mandatory data retention regime, which necessarily relies on the existing, and now outdated, TIA Act framework.

Labor Members of this Committee also note that in its February 2015 *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, the PJCIS recommended 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'. Labor members of this Committee endorse this recommendation of the PJCIS, noting that eighteen of the nineteen outstanding recommendations referred to relate to reform of the TIA Act. We have reproduced below the 18 recommendations of the PJCIS from the June 2013 Report relating to the TIA Act, and call on the Government to formally accept all of these recommendations and to commence as soon as practicable the revision of that Act.

Labor members of this Committee also take this opportunity to express our disappointment at the chaotic and unnecessarily rushed manner in which the Abbott Government approached the Data Retention Bill. The Abbott Government did nothing to progress data retention laws during its first year in office, preferring to instead focus its energies on campaigns such as its failed attempt to repeal the race hate provisions in section 18C of the *Racial Discrimination Act 1975*. Despite failing to act on data retention laws for over a year in office, when it finally decided to act on data retention the Abbott Government claimed that the matter was suddenly of great urgency. The Government then chose to ignore the unanimous 2013 recommendation of the PJCIS to release an exposure draft of the proposed legislation for consultation, and instead introduced a significantly flawed bill into the Parliament. Now infamous attempts by senior members of the Government to explain the Bill in the weeks after its introduction only created confusion that exacerbated public concern about the effects of the proposed legislation.

The Government then sought to rush the review of the Data Retention Bill by the PJCIS, pressing for the Bill to be reviewed with an urgency that would have precluded proper public scrutiny. However, Labor insisted that the Government allow time for proper consideration of the Bill by the PJCIS, including adequate time for the public, legal bodies and key stakeholders to make submissions, and for public hearings to be held.

The review of the Data Retention Bill by the PJCIS revealed how flawed the Government's proposed legislation was. In its 2015 report the PJCIS made 38 substantive recommendations for changes to the Bill to improve the efficacy of the proposed regime, while at the same time introducing significant improvements to the data security, oversight and accountability mechanisms under which the proposed

regime would operate. Those recommendations were all accepted by the Government, and required numerous amendments to the Bill.

Labor members of this Committee strongly suggest that the Government take a more sensible, measured and consultative approach to reform of the TIA Act. Specifically, Labor recommends that the Government does not again ignore the bipartisan recommendations of the PJCIS, and follows the recommendation to revise the TIA Act in consultation with relevant stakeholders and to release an exposure draft of a revised TIA Act for public consultation and for consideration by the PJCIS.

Recommendations of the 2013 PJCIS Report with respect to 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.

Conclusion

Labor will always work to keep our nation safe, and at the same time to uphold the rights and freedoms enjoyed by all Australians. Getting this balance right can be a challenging task, and it is clear that there is still work to do to ensure that Australia's national security and law enforcement legislation meets the needs of our agencies while at the same time incorporating robust and effective oversight mechanisms and safeguards.

For example, Labor will continue to press for improvements to data security through the Telecommunications Sector Security Reform (TSSR) process. The TSSR aims to identify, manage and mitigate national security risks associated with Australia's telecommunications infrastructure, including matters such as the physical location of stored telecommunications data. This was also the subject of the PJCIS's 2013 report, which included at 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.

These PJCIS also recommended that the TSSR be subject to a comprehensive regulatory impact assessment.

In addition to the TSSR process, Senator John Faulkner, who retired from the Parliament in February this year, advocated for further improvements to the transparency and accountability mechanisms in our national security frameworks. It was Senator Faulkner's view that it is the Parliament to which our police and national security agencies are ultimately accountable, and it is the Parliament's responsibility to oversee their priorities and effectiveness, and to ensure that our agencies meet the requirements and standards that Parliament sets.

To this end Senator Faulkner developed a set of reforms designed to ensure that the effectiveness of Parliamentary oversight of intelligence and security agencies keeps pace with any enhanced powers being given to those agencies. A key reform

recommended by Senator Faulkner was for the PJCIS to have oversight of certain operational matters of the security agencies. Progress towards that reform is evident in the Data Retention Bill, which Labor pressed to be amended so that the PJCIS could oversight aspects of the data retention scheme.

Labor will bring forward legislation this year to give effect to the wider reforms proposed by Senator Faulkner.

Labor believes that ensuring the ongoing efficacy and integrity of our national security architecture is an ongoing responsibility of all parliamentarians, and Labor will continue to engage constructively in this important process.

Senator Jacinta Collins
Labor Senator for Victoria

Appendix 1

Recommendations 1 to 18, 42 and 43 of the PJCIS Report of the Inquiry into Potential Reforms of Australia's National Security Legislation

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. xxvi

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.

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 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.

Appendix 2

Public submissions

- 1 Australian Law Reform Commission
- 2 Mr Brett Hedger
- 3 Independent Broad-based Anti-corruption Commission (IBAC)
- 4 Blueprint For Free Speech
- 5 ThoughtWorks Australia Pty Ltd
- 6 Victoria Police
- 7 Australian Racing Board
- 8 Australian Communications and Media Authority (ACMA)
- 9 Commonwealth Ombudsman
- 10 Pirate Party Australia
- 11 Australian Commission for Law Enforcement Integrity
- 12 Inspector-General of Intelligence and Security
- 13 NSW Ombudsman
- 14 Corruption and Crime Commission
- 15 Media, Entertainment and Arts Alliance
- 16 Australian Mobile Telecommunications Association
- 17 Public Interest Monitor (Victoria)
- 18 Independent Commissioner Against Corruption
- 19 Mr Johann Trevaskis
- 20 Western Australia Police
- 21 Northern Territory Police
- 22 Electronic Frontiers Australia
- 23 Australian Crime Commission
- 24 Office of the Australian Information Commissioner
- 25 Australian Federal Police (AFP)
- 26 Attorney-General's Department
- 27 Australian Security Intelligence Organisation (ASIO)

- 28 Information and Privacy Commission NSW (ipc)
- 29 Mr Arthur Marsh
- 30 NSW Government
- 31 Confidential
- 32 Name Withheld
- 33 Telecommunications Industry Ombudsman
- 34 Law Council of Australia
- 35 Confidential
- 36 The Australian Privacy Foundation
- 37 Mr Philip Dorling
- 38 iiNet Limited (PDF 399 KB)
- 39 Office of the Inspector of the Independent Commission Against Corruption
- 40 Guardian Australia
- 41 Confidential
- 42 NSW Council for Civil Liberties
- 43 Confidential
- 44 Civil Liberties Australia
- 45 Free TV Australia

Appendix 3

Public hearings and witnesses

Tuesday, 22 April 2014—Canberra

COLVIN, Acting Commissioner Andrew, Australian Federal Police

CRAWFORD, Assistant Commissioner Peter, Queensland Police Service

JEVTOVIC, Mr Paul APM, Acting Chief Executive Officer, Australian Crime Commission

JEVTOVIC, Mr Paul, APM, Acting Chief Executive Officer, Australian Crime Commission

KELLY, Ms Wendy Anne, Director, Telecommunications and Surveillance Law Branch, Attorney-General's Department

LIND, Ms Judith, Executive Director, Strategy and Specialist Capabilities, Australian Crime Commission

MCMULLAN, Ms Kathryn, National Manager, Specialist Capabilities, Australian Crime Commission

SMITH, Ms Catherine Lucy, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department

STEVENS, Deputy Commissioner Grant John, Deputy Commissioner of Police, South Australia Police

TANZER, Mr Greg, Commissioner, Australian Securities and Investments Commission

WILKINS, Mr Roger, AO, Secretary, Attorney-General's Department

WILLIAMS, Mr Gregory, Deputy Commissioner, Australian Taxation Office

Wednesday, 23 April 2014—Canberra

BAKER-GOLDSMITH, Ms Sarah, Principal Lawyer, Australian Commission for Law Enforcement Integrity

BIBBY, Dr Martin, Member, Executive Committee, NSW Council for Civil Liberties

BLANKS, Mr Stephen, President, NSW Council for Civil Liberties

BLIGHT, Mr Jake, Assistant Inspector-General, Office of Inspector-General of Intelligence and Security

BOULTEN, Mr Phillip, SC, Member, National Criminal Law Committee, Law Council of Australia

CLARK, Mr Nick, Education Coordinator, Rule of Law Institute of Australia

CLARK, Ms Narelle, President, Internet Society of Australia

MARSHALL, Ms Sarah, Acting Executive Director Operations, Australian Commission for Law Enforcement Integrity

McMILLAN, Professor John Denison, Australian Information Commissioner, Office of the Australian Information Commissioner

MOLT, Dr Natasha, Policy Lawyer, Criminal Law and Human Rights Division, Law Council of Australia

MOSS, Mr Philip, Integrity Commissioner, Australian Commission for Law Enforcement Integrity

MOULDS, Ms Sarah, Acting Co-Director, Criminal Law and Human Rights Division, Law Council of Australia

NEAVE, Mr Colin, Commonwealth Ombudsman

POMERY, Mr Simon, Assistant Director, Commonwealth Ombudsman

ROGERS, Mr Jackson, Assistant Secretary, NSW Council for Civil Liberties

SELLARS, Mr Nicholas, Acting Executive Director Strategic and Secretariat, Australian Commission for Law Enforcement Integrity

STEWART, Mr Malcolm, Vice-President, Rule of Law Institute of Australia

THOM, Dr Vivienne, Inspector-General, Office of Inspector-General of Intelligence and Security

WOLFE, Mr Simon, Head of Research, Blueprint for Free Speech

Monday, 21 July 2014—Canberra

ARNOLD, Associate Professor Bruce Baer, Law School, University of Canberra

HARTLAND, Ms Kerri, Deputy Director-General, Australian Security Intelligence Organisation

IRVINE, Mr David Taylor, Director-General of Security, Australian Security Intelligence Organisation

WARREN, Mr Christopher, Federal Secretary, Media, Entertainment and Arts Alliance

Tuesday, 29 July 2014—Sydney

ALTHAUS, Mr Chris, Chief Executive Officer, Australian Mobile Telecommunications Association

BAKER, Mr Stewart Abercrombie, Private capacity

DALBY, Mr Steve, Chief Regulatory Officer, iiNet Limited

FROELICH, Mr Peter, Industry member, Australian Mobile Telecommunications Association and Communications Alliance Ltd

KELLOW, Mr Philip John, Registrar, Administrative Appeals Tribunal

LAWRENCE, Mr Jon, Executive Officer, Electronic Frontiers Australia

O'DONNELL, Ms Leanne, Regulatory Manager, iiNet Limited

RYAN, Mr Michael, Industry member, Australian Mobile Telecommunications Association and Communications Alliance Ltd

STANTON, Mr John, Chief Executive Officer, Communications Alliance Ltd

VULKANOVSKI, Mr Alexander, Member, Policy and Research Standing Committee

WATERS, Mr Nigel, Australian Privacy Foundation

YERRAMSETTI, Mr Roger, Operations Manager, iiNet Limited

Appendix 4

Examples of telecommunications data generated by a website, a Facebook page and a tweet

Source: Document tabled by iiNet Limited at public hearing on 29 July 2014

Follow us on **twitter**

iiNet
connect better

... and here's the metadata.

Here's a Tweet ...

GuardianUS
@GuardianUS

Need to catch up? Our complete #NSAFiles coverage is here: trib.al/qHVziUm

```
{
  "created_at": "Mon Jun 10 21:03:19 +0000 2013",
  "id": "344199622916448260",
  "text": "Need to catch up? Our complete #NSAFiles coverage is here: http://t.co/iZPkknopxk",
  "source": "<a href='\"http://www.socialflow.com\"' rel='nofollow'>socialflow</a>",
  "truncated": false,
  "user": {
    "id": "16042794",
    "id_str": "16042794",
    "name": "GuardianUS",
    "screen_name": "GuardianUS",
    "location": "New York",
    "description": "Featuring the Guardian's US coverage, conversations and reporters.",
    "url": "http://t.co/eqPi0NU5me",
    "protected": false,
    "followers_count": 55597,
    "friends_count": 509,
    "listed_count": 2114,
    "created_at": "Fri Aug 29 14:52:08 +0000 2008",
    "favourites_count": 800,
    "utc_offset": -18000,
    "time_zone": "Eastern Time (US & Canada)",
    "geo_enabled": true,
    "verified": true,
    "statuses_count": 41567,
    "lang": "en",
    "contributors_enabled": false,
    "is_translator": false,
    "is_translation_enabled": false
  }
}
```

The content of the Tweet is in the metadata

Comprehensive revision of Telecommunications (Interception and Access) Act 1979 – Attachment

29 July 2014

Note the links to picture files, which are content

... and here's the metadata.

1 ABC web page

2 Webpage metadata

Here's the ABC website ...

Comprehensive revision of Telecommunications (Interception and Access) Act 1979 – Attachment

29 July 2014

Here's the iiNet Facebook page...

1 iiNet Facebook page

2 Facebook metadata

3 Content

4 Author's Facebook profile

5 Author's Facebook page

... and here's the metadata.

Comprehensive revision of Telecommunications (Interception and Access) Act 1979 – Attachment

29 July 2014

Appendix 5

Tabled documents, answers to questions on notice and additional information

Answers to questions on notice

- 1 Attorney-General's Department - answers to questions taken on notice (received 12 May 2014)
- 2 iiNet Limited – answer to a question taken on notice at a public hearing on 29 July 2014 (received 11 August 2014)

Additional information

- 1 Additional Information received from Geoff Taylor – Document 1
- 2 Additional Information received from Geoff Taylor – Document 2
- 3 Document tabled by the Australian Crime Commission at public hearing held 22 April 2014 - Telecommunications Interception and Access Compliance
- 4 Additional Information received from Geoff Taylor – Document 3
- 5 Additional Information received from Geoff Taylor – Document 4
- 6 Document tabled by iiNet Limited, at public hearing on 29 July 2014

Appendix 6

**Directive 2006/24/EC of the European Parliament and of
the Council of 15 March 2006**



Press and Information

Court of Justice of the European Union

PRESS RELEASE No 54/14

Luxembourg, 8 April 2014

Judgment in Joined Cases C-293/12 and C-594/12
Digital Rights Ireland and Seitlinger and Others

The Court of Justice declares the Data Retention Directive to be invalid

It entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary

The main objective of the Data Retention Directive¹ is to harmonise Member States' provisions concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks. It therefore seeks to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism. Thus, the directive provides that the abovementioned providers must retain traffic and location data as well as related data necessary to identify the subscriber or user. By contrast, it does not permit the retention of the content of the communication or of information consulted.

The High Court (Ireland) and the Verfassungsgerichtshof (Constitutional Court, Austria) are asking the Court of Justice to examine the validity of the directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data.

The High Court must resolve a dispute between the Irish company Digital Rights Ireland and the Irish authorities regarding the legality of national measures concerning the retention of data relating to electronic communications. The Verfassungsgerichtshof has before it several constitutional actions brought by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants. Those actions seek the annulment of the national provision which transposes the directive into Austrian law.

By today's judgment, the Court declares the directive invalid².

The Court observes first of all that the data to be retained make it possible, in particular, (1) to know the identity of the person with whom a subscriber or registered user has communicated and by what means, (2) to identify the time of the communication as well as the place from which that communication took place and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.

The Court takes the view that, **by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.** Furthermore, the fact that data are retained and subsequently used without the

¹ 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 (OJ 2006 L 105, p. 54).

² Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the directive entered into force.

subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance.

The Court then examines whether such an interference with the fundamental rights at issue is justified.

It states that **the retention of data** required by the directive **is not such as to adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data**. The directive does not permit the acquisition of knowledge of the content of the electronic communications as such and provides that service or network providers must respect certain principles of data protection and data security.

Furthermore, the retention of data for the purpose of their possible transmission to the competent national authorities **genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security**.

However, the Court is of the opinion that, by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.

In that context, the Court observes that, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by the directive, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, **the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary**.

Firstly, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without **any differentiation, limitation or exception** being made in the light of the objective of fighting against serious crime.

Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have **access to the data** and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.

Thirdly, so far as concerns **the data retention period**, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

The Court also finds that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the **risk of abuse** and against any unlawful access and use of the data. It notes, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.

Lastly, the Court states that the directive does **not** require that the data be **retained within the EU**. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Unofficial document for media use, not binding on the Court of Justice.

The [full text](#) of the judgment is published on the CURIA website on the day of delivery.

Press contact: Christopher Fretwell ☎ (+352) 4303 3355

Pictures of the delivery of the judgment are available from "[Europe by Satellite](#)" ☎ (+32) 2 2964106

**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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee ⁽¹⁾,

Acting in accordance with the procedure laid down in Article 251 of the Treaty ⁽²⁾,

Whereas:

- (1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽³⁾ requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.
- (2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ⁽⁴⁾ translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.
- (3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be

erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

- (4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.
- (5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.
- (6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.
- (7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.
- (8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

⁽¹⁾ Opinion delivered on 19 January 2006 (not yet published in the Official Journal).

⁽²⁾ Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

⁽³⁾ OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

⁽⁴⁾ OJ L 201, 31.7.2002, p. 37.

- (9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, *inter alia*, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.
- (10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.
- (11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.
- (12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.
- (13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.
- (14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.
- (15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.
- (16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.
- (17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.
- (18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive. Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems ⁽¹⁾ provides that the intentional illegal access to information systems, including to data retained therein, is to be made punishable as a criminal offence.
- (19) The right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC to receive compensation, which derives from Article 23 of that Directive, applies also in relation to the unlawful processing of any personal data pursuant to this Directive.

⁽¹⁾ OJ L 69, 16.3.2005, p. 67.

- (20) The 2001 Council of Europe Convention on Cybercrime and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of this Directive.
- (21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.
- (22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.
- (23) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those providers, there is no obligation to retain them. This Directive is not intended to harmonise the technology for retaining data, the choice of which is a matter to be resolved at national level.
- (24) In accordance with paragraph 34 of the Interinstitutional agreement on better law-making ⁽¹⁾, Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public.
- (25) This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community

law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.
2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) ⁽²⁾, and in Directive 2002/58/EC shall apply.
2. For the purpose of this Directive:
 - (a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

⁽¹⁾ OJ C 321, 31.12.2003, p. 1.

⁽²⁾ OJ L 108, 24.4.2002, p. 33.

- (b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;
- (c) 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);
- (d) 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;
- (e) 'cell ID' means the identity of the cell from which a mobile telephony call originated or in which it terminated;
- (f) 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance

with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

- (a) data necessary to trace and identify the source of a communication:
- (1) concerning fixed network telephony and mobile telephony:
 - (i) the calling telephone number;
 - (ii) the name and address of the subscriber or registered user;
 - (2) concerning Internet access, Internet e-mail and Internet telephony:
 - (i) the user ID(s) allocated;
 - (ii) the user ID and telephone number allocated to any communication entering the public telephone network;
 - (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
- (b) data necessary to identify the destination of a communication:
- (1) concerning fixed network telephony and mobile telephony:
 - (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
 - (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

- (2) concerning Internet e-mail and Internet telephony:
- (i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;
 - (ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;
- (c) data necessary to identify the date, time and duration of a communication:
- (1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;
 - (2) concerning Internet access, Internet e-mail and Internet telephony:
 - (i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;
 - (ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;
- (d) data necessary to identify the type of communication:
- (1) concerning fixed network telephony and mobile telephony: the telephone service used;
 - (2) concerning Internet e-mail and Internet telephony: the Internet service used;
- (e) data necessary to identify users' communication equipment or what purports to be their equipment:
- (1) concerning fixed network telephony, the calling and called telephone numbers;
 - (2) concerning mobile telephony:
 - (i) the calling and called telephone numbers;
 - (ii) the International Mobile Subscriber Identity (IMSI) of the calling party;
 - (iii) the International Mobile Equipment Identity (IMEI) of the calling party;
- (iv) the IMSI of the called party;
- (v) the IMEI of the called party;
- (vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;
- (3) concerning Internet access, Internet e-mail and Internet telephony:
- (i) the calling telephone number for dial-up access;
 - (ii) the digital subscriber line (DSL) or other end point of the originator of the communication;
- (f) data necessary to identify the location of mobile communication equipment:
- (1) the location label (Cell ID) at the start of the communication;
 - (2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.
2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

- (a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

- (b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
- (c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;
- and
- (d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

- Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.
- The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10

Statistics

1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

- the cases in which information was provided to the competent authorities in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,

— the cases where requests for data could not be met.

- Such statistics shall not contain personal data.

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

'1a. Paragraph 1 shall not apply to data specifically required by 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 (*) to be retained for the purposes referred to in Article 1(1) of that Directive.

(*) OJ L 105, 13.4.2006, p. 54.'

Article 12

Future measures

- A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.
- The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.
- Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14

Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or

shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the *Official Journal of the European Union*.

Article 16

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 17

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 15 March 2006.

For the European Parliament
The President
J. BORRELL FONTELLES

For the Council
The President
H. WINKLER

Declaration by the Netherlands
pursuant to Article 15(3) of Directive 2006/24/EC

Regarding the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC, the Netherlands will be making use of the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period not exceeding 18 months following the date of entry into force of the Directive.

Declaration by Austria
pursuant to Article 15(3) of Directive 2006/24/EC

Austria declares that it will be postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period of 18 months following the date specified in Article 15(1).

Declaration by Estonia
pursuant to Article 15(3) of Directive 2006/24/EC

In accordance with Article 15(3) of the Directive of the European Parliament and of the Council 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, Estonia hereby states its intention to make use of use that paragraph and to postpone application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

Declaration by the United Kingdom
pursuant to Article 15(3) of Directive 2006/24/EC

The United Kingdom declares in accordance with Article 15(3) of the Directive 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 that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Cyprus
pursuant to Article 15(3) of Directive 2006/24/EC

The Republic of Cyprus declares that it is postponing application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until the date fixed in Article 15(3).

Declaration by the Hellenic Republic
pursuant to Article 15(3) of Directive 2006/24/EC

Greece declares that, pursuant to Article 15(3), it will postpone application of this Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 18 months after expiry of the period provided for in Article 15(1).

Declaration by the Grand Duchy of Luxembourg
pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the Directive of the European Parliament and of the Council 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, the Government of the Grand Duchy of Luxembourg declares that it intends to make use of Article 15(3) of the Directive in order to have the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Slovenia**pursuant to Article 15(3) of Directive 2006/24/EC**

Slovenia is joining the group of Member States which have made a declaration under Article 15(3) of the Directive of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, for the 18 months postponement of the application of the Directive to the retention of communication data relating to Internet, Internet telephony and Internet e-mail.

Declaration by Sweden**pursuant to Article 15(3) of Directive 2006/24/EC**

Pursuant to Article 15(3), Sweden wishes to have the option of postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Lithuania**pursuant to Article 15(3) of Directive 2006/24/EC**

Pursuant to Article 15(3) of the draft Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC (hereafter the 'Directive'), the Republic of Lithuania declares that once the Directive has been adopted it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).

Declaration by the Republic of Latvia**pursuant to Article 15(3) of Directive 2006/24/EC**

Latvia states in accordance with Article 15(3) of Directive 2006/24/EC 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 that it is postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

Declaration by the Czech Republic**pursuant to Article 15(3) of Directive 2006/24/EC**

Pursuant to Article 15(3), the Czech Republic hereby declares that it is postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

Declaration by Belgium**pursuant to Article 15(3) of Directive 2006/24/EC**

Belgium declares that, taking up the option available under Article 15(3), it will postpone application of this Directive, for a period of 36 months after its adoption, to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Poland**pursuant to Article 15(3) of Directive 2006/24/EC**

Poland hereby declares that it intends to make use of the option provided for under Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC and postpone application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in Article 15(1).

Declaration by Finland**pursuant to Article 15(3) of Directive 2006/24/EC**

Finland declares in accordance with Article 15(3) of the Directive 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 that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Germany**pursuant to Article 15(3) of Directive 2006/24/EC**

Germany reserves the right to postpone application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in the first sentence of Article 15(1).
