

---

The Parliament of the Commonwealth of Australia

# Report of the Inquiry into Potential Reforms of Australia's National Security Legislation

Parliamentary Joint Committee on Intelligence and Security

May 2013  
Canberra

---

© Commonwealth of Australia 2013

ISBN 978-1-74366-083-6 (Printed version)

ISBN 978-1-74366-084-3 (HTML version)

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/>.



# Contents

Foreword .....	vii
Membership of the Committee .....	xi
Terms of reference .....	xiii
List of abbreviations .....	xix
List of recommendations .....	xxiii
Glossary .....	xxxv
<b>1 Introduction .....</b>	<b>1</b>
Background to the inquiry.....	1
Conduct of the inquiry .....	2
Structure of the report .....	3
Chapter Two.....	4
Chapter Three .....	4
Chapter Four .....	5
Chapter Five.....	6
Appendices .....	7
<b>2 Telecommunications Interception.....</b>	<b>9</b>
Strengthening the safeguards and privacy protections .....	10
The legislation's privacy protection objective .....	10
The proportionality tests for issuing warrants .....	14
Mandatory record-keeping standards.....	16
Oversight arrangements by the Commonwealth and State Ombudsmen.....	19
Reforming the lawful access regime for agencies .....	22
Reducing the number of agencies eligible to access communications information .....	22

Standardise warrant tests and thresholds .....	26
Expanding the basis of interception activities.....	30
<b>Streamlining and reducing complexity .....</b>	<b>35</b>
Simplifying the information sharing provisions that allow agencies to cooperate .....	36
Removing legislative duplication .....	41
A single warrant with multiple telecommunications interception powers .....	43
<b>Modernising the cost sharing framework .....</b>	<b>48</b>
Align industry interception assistance with industry regulatory policy .....	49
Clarify ACMA's regulatory and enforcement role .....	50
Requirements for industry interception obligations.....	52
Clarify that the interception regime includes ancillary service providers.....	54
Industry participation model .....	56
An offence for failure to assist in the decryption of communications .....	59
Institute industry response timelines .....	64
Revision of the interception regime .....	66
<b>3 Telecommunications security .....</b>	<b>69</b>
Issues raised in evidence .....	72
Is there a need for an industry wide obligation to protect telecommunications?.....	72
Information sharing and compliance auditing .....	76
Remediation powers and a penalty regime .....	78
Other considerations .....	79
Committee comment.....	82
<b>4 Australian Intelligence Community Legislation Reform.....</b>	<b>85</b>
Proposals the Government wishes to progress.....	86
ASIO Act – Computer access warrants.....	86
ASIO Act warrant proposals .....	96
ASIO Act employment provisions.....	104
Intelligence Services Act – Clarifying the authority of the Defence Imagery and Geospatial Organisation.....	106
<b>Matters the Government is considering.....</b>	<b>108</b>
Creation of an authorised intelligence operations scheme .....	108
Named person warrants .....	112

Surveillance devices – use of optical devices .....	115
Person searches .....	116
Authorisation lists for warrants .....	120
Clarifying ASIO's ability to co-operate with private sector .....	122
Identifying ASIO officers.....	124
<b>Matters on which the Government expressly seeks the Committee's views – ASIO Act amendments.....</b>	<b>125</b>
Incidental entry onto premises .....	125
Use of force.....	128
Evidentiary certificates .....	130
<b>Matters on which the Government expressly seeks the Committee's views – Intelligence Services Act amendments.....</b>	<b>132</b>
Section 9 – Ministerial authorisations.....	133
Section 13A – Co-operation with intelligence agencies.....	134
ASIS co-operation on self-defence and weapons training.....	136
Concluding comment .....	138
<b>5 Data Retention .....</b>	<b>139</b>
Introduction .....	139
The current regime.....	141
The international experience .....	142
Responses to data retention.....	147
Privacy and civil liberties .....	150
Security .....	167
Feasibility and efficacy .....	175
Cost.....	185
Committee comment.....	189
<b>Appendix A – List of submissions .....</b>	<b>195</b>
<b>Appendix B – List of exhibits .....</b>	<b>203</b>
<b>Appendix C – Witnesses who appeared at public hearings.....</b>	<b>205</b>
Melbourne, 5 September 2012.....	205
Canberra, 14 September 2012.....	206

Sydney, 26 September 2012.....	207
Sydney, 27 September 2012.....	208
Canberra, 2 November 2012.....	208
<b>Appendix D – Witnesses who appeared at private hearings.....</b>	<b>209</b>
Canberra, 14 September 2012.....	209
Canberra, 21 September 2012.....	209
Canberra, 29 October 2012.....	210
Canberra, 2 November 2012.....	210
<b>Appendix E – Discussion paper .....</b>	<b>211</b>
<b>Appendix F – Letter from Attorney-General the Hon Nicola Roxon MP to the Hon Anthony Byrne MP .....</b>	<b>273</b>
<b>Appendix G – Letter from Mr Roger Wilkins AO, Secretary of the Attorney- General’s Department, to the Hon Anthony Byrne MP .....</b>	<b>279</b>
<b>Appendix H – Telecommunications data provided to law enforcement and national security agencies by Telstra .....</b>	<b>283</b>



# Foreword

## **Introduction**

The environment in which Australia's Security and Intelligence Agencies operate is a complex and rapidly evolving one.

Recent events such as the Boston bombings and the murder of a British Soldier on the streets of London remind us of the impact of terrorist attacks and the continued need for the Government and its Security and Intelligence Agencies to maintain vigilance, preparedness for and defence against terrorist attacks.

The Committee recognises the need for our Security and Intelligence Agencies to be appropriately resourced and to be granted powers, which are often intrusive, to carry out their work.

However, these intrusive powers must always be balanced by appropriate safeguards for the privacy of individuals and the community recognising that Australia is a democratic nation which values personal freedom and places limits on the Power of the State.

The Inquiry into the reforms proposed by the Attorney General was one of the most complex and controversial inquiries ever undertaken by the Parliamentary Joint Committee on Intelligence and Security (the Committee).

## **Conduct of Inquiry**

In May 2012, the then Attorney-General the Hon Nicola Roxon MP asked the Committee to inquire into a package of potential reforms to Australia's national security legislation.

Subsequent to this request, the Committee was provided with a discussion paper outlining the reforms the Australian Government was considering, as well as some on which the Government expressly sought the views of the Committee.

This discussion paper contained the terms of reference for this Inquiry which canvassed reforms in three areas: interception of communications and access to data under the *Telecommunication (Interception and Access) Act 1979*; reform of the telecommunications security aspects of the *Telecommunications Act 1997* and other relevant legislation; and reform of the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*. The terms of reference contained 18 specific reform proposals containing 44 separate items across three different reform areas.

Letters inviting submissions were sent to over 130 stakeholders in both federal and state government, the telecommunications industry, civil liberties and privacy non-government organisations, and peak legal bodies and associations with an expected interest in the reforms canvassed.

The Committee received 240 submissions and 29 exhibits. Three submissions were received in largely identical terms from some 5,300 individual members of the public. These submitters expressed opposition to the reform proposals, particularly the proposed mandatory data retention proposal.

### **Inquiry Challenges**

At the outset the Committee was faced with three key difficulties. Firstly, the terms of reference were very wide ranging as they contained 18 specific reform proposals containing 44 separate items across three different reform areas.

Secondly, the lack of any draft legislation or detail about some of the potential reforms was a major limitation and made the Committee's consideration of the merit of the reforms difficult. This also made it hard for interested stakeholders to effectively respond to the terms of reference.

Thirdly, that one of the most controversial topics canvassed in the discussion paper – data retention – was only accorded just over two lines of text.

This lack of information from the Attorney-General and her Department had two major consequences. First, it meant that submitters to the Inquiry could not be sure as to what they were being asked to comment on. Second, as the Committee was not sure of the exact nature of what the Attorney-General and her Department was proposing it was seriously hampered in the conduct of the inquiry and the process of obtaining evidence from witnesses.

Importantly the Committee was very disconcerted to find, once it commenced its Inquiry, that the Attorney-General's Department (AGD) had much more detailed information on the topic of data retention. Departmental work, including discussions with stakeholders, had been undertaken previously. Details of this work had to be drawn from witnesses representing the AGD.



In fact, it took until the 7<sup>th</sup> November 2012 for the Committee to be provided with a formal complete definition of which data was to be retained under the data retention regime proposed by the AGD.

## **In Conclusion**

The Committee welcomed the public response to the proposed reforms and evidence provided to the Committee was an important factor in its determinations.

This report is undoubtedly comprehensive, given the number of reforms proposed. However, given the lack of detail and the absence of draft legislation, the Committee's conclusions are often qualified or suggest areas where further work is needed.


I would like to thank my colleagues on the Parliamentary Joint Committee on Intelligence and Security for their work on this Inquiry and in particular their commitment under enormous constraints to produce a unanimous report.

Additionally, this Inquiry would not have been possible without the tireless work of the Committee Secretariat particularly the Committee Secretary Jerome Brown, Inquiry Secretary Robert Little and Senior Research Officer James Bunce.

Additionally I would thank Mr Cameron Gifford and Mr Simon Lee who were seconded to the Committee's Secretariat from the Attorney-General's Department.

The Hon Anthony Byrne MP  
Chair





## Membership of the Committee

**Chair**            The Hon Anthony Byrne MP

**Deputy Chair**   The Hon Philip Ruddock MP

<b>Members</b>	Mr Michael Danby MP (to 02/04/13)	Senator Mark Bishop (from 01/07/11)
	Mr John Forrest MP (from 06/07/11)	Senator the Hon George Brandis SC (from 06/07/11)
	Mr Daryl Melham MP (to 14/03/12)	Senator the Hon John Faulkner
	The Hon Kevin Rudd MP (from 14/03/12)	Senator Michael Forshaw (until 30/06/11)
	Mr Andrew Wilkie MP	Senator the Hon David Johnston (from 06/07/11)
		Senator Julian McGauran (until 30/06/11)
		Senator the Hon Ursula Stephens (from 06/07/11)
		Senator Russell Trood (until 30/06/11)

## Committee Secretariat

Secretary	Mr Jerome Brown
Inquiry Secretary	Mr Robert Little
Research Officers	Mr James Bunce
	Mr Simon Lee
	Mr Cameron Gifford
Administrative Officers	Ms Jessica Butler
	Ms Sonya Gaspar
	Ms Lauren McDougall



# Terms of reference

Having regard to:

- the desirability of comprehensive, consistent and workable laws and practices to protect the security and safety of Australia, its citizens and businesses,
- the need to ensure that intelligence, security and law enforcement agencies are equipped to effectively perform their functions and cooperate effectively in today's and tomorrow's technologically advanced and globalised environment, and
- the fact that national security brings shared responsibilities to the government and the private sector:

1. The Parliamentary Joint Committee on Intelligence and Security is to inquire into potential reforms of National Security Legislation, as set out in the attachment and which include proposals relating to the:

- *Telecommunications (Interception and Access) Act 1979*
- *Telecommunications Act 1997*
- *Australian Security Intelligence Organisation Act 1979*
- *Intelligence Services Act 2001*

2. The inquiry should consider the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet:

- the challenges of new and emerging technologies upon agencies' capabilities
- the requirements of a modern intelligence and security agency legislative framework, and to enhance cooperation between agencies, and

- the need for enhancements to the security of the telecommunications sector.
3. The Committee should have regard to whether the proposed responses:
    - contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector
    - apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the telecommunications sector and the potential for follow on effects to consumers, the economy and international competition, and
    - will address law enforcement reduction of capabilities from new technologies and business environment, which has a flow-on effect to security agencies.
  4. The Committee should take account of the interests of the broad range of stakeholders including through a range of public, in camera and classified hearings.
  5. The Committee should provide a written report on each of the three elements of the National Security Legislation referral to the Attorney-General.

The National Security Legislation the subject of the inquiry has three different elements and Objectives. They relate to:

- modernising lawful access to communications and associated communications data
- mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers, and
- enhancing the operational capacity of Australian intelligence community agencies.

The proposals across the three different packages are separated into three different groupings:

- A. those the Government wishes to progress
- B. those the Government is considering progressing, and
- C. those on which the Government is expressly seeking the views of the PJCIS.

**A - Government wishes to progress the following proposals:***Telecommunications (Interception and Access) Act 1979*

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the Telecommunications (Interception and Access) Act 1979 (the TIA Act). This would include the examination of:
  - the legislation's privacy protection objective
  - the proportionality tests for issuing of warrants
  - mandatory record-keeping standards
  - oversight arrangements by the Commonwealth and State Ombudsmen
2. Reforming the lawful access to communications regime. This would include:
  - reducing the number of agencies eligible to access communications information
  - the standardisation of warrant tests and thresholds
3. Streamlining and reducing complexity in the lawful access to communications regime. This would include:
  - simplifying the information sharing provisions that allow agencies to cooperate
  - removing legislative duplication
4. Modernising the TIA Act's cost sharing framework to:
  - align industry interception assistance with industry regulatory policy
  - clarify ACMA's regulatory and enforcement role

*Australian Security Intelligence Organisation Act 1979*

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions
  - to update the definition of 'computer' in section 25A
  - Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.
6. Modernising ASIO Act employment provisions by:
  - providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'
  - Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent

- Modernising the Director-General's powers in relation to employment terms and conditions
- Removing an outdated employment provision (section 87 of the ASIO Act)
- Providing additional scope for further secondment arrangements

Intelligence Services Act 2001

7. Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies.

**B. Government is considering the following proposals:**

Telecommunications (Interception and Access) Act 1979

8. Streamlining and reducing complexity in the lawful access to communications regime – this would include:
  - Creating a single warrant with multiple TI powers
9. Modernising the Industry assistance framework –
  - Implement detailed requirements for industry interception obligations
  - extend the regulatory regime to ancillary service providers not currently covered by the legislation
  - implement a three-tiered industry participation model

Australian Security Intelligence Organisation Act 1979

10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.
11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:
  - Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.
  - Align surveillance device provisions with the Surveillance Devices Act 2007



- Enable the disruption of a target computer for the purposes of a computer access warrant
  - Enable person searches to be undertaken independently of a premises search
  - Establish classes of persons able to execute warrants
12. Clarifying ASIO's ability to cooperate with the private sector.
  13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.

**C. Government is expressly seeking the views of the Committee on the following matters:**

14. Telecommunications (Interception and Access) Act 1979
  - Reforming the Lawful Access Regime
  - expanding the basis of interception activities
15. Modernising the Industry assistance framework
  - establish an offence for failure to assist in the decryption of communications
  - institute industry response timelines
  - tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

Telecommunications Act 1997

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:
  - by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference
  - by instituting obligations to provide Government with information on significant business and procurement decisions and network designs
  - Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers
  - Creating appropriate enforcement powers and pecuniary penalties

Australian Security Intelligence Organisation Act 1979

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:
- Using third party computers and communications in transit to access a target computer under a computer access warrant.
  - Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant
  - Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.
  - Introducing an evidentiary certificate regime.

Intelligence Services Act 2001

18. Amending the Intelligence Services Act to:
- Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.
  - Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required.
  - Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.



## List of abbreviations

ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACMA	Australian Communications and Media Authority
AGD	Attorney-General's Department
AFP	Australian Federal Police
AMTA	Australian Mobile Telecommunications Association
ASIO	Australian Security Intelligence Organisation
ASIC	Australian Securities and Investment Commission
ASIS	Australian Secret Intelligence Service
ASP	Application service provider
CAD	Call associated data
C/CSP	Carriers/Carriage Service Providers
CMC	Queensland Crime and Misconduct Commission
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DPI	Deep packet inspection
DSD	Defence Signals Directorate
ECHR	European Covenant on Human Rights
EU	European Union

GATT	General Agreement on Tariffs and Trade
ICCPR	International Covenant on Civil and Political Rights
IGIS	Inspector-General of Intelligence and Security
IIA	Internet industry association
IMEI	International Mobile Equipment Identifier
IP	Internet protocol
IPA	Institute of Public Affairs
IS Act	<i>Intelligence Services Act 2001</i>
ISP	Internet Service Provider
IT	Information Technology
LENSA	Law enforcement and national security agencies
NPP	National Privacy Principles
NSW	New South Wales
NSW CCL	New South Wales Council for Civil Liberties
OAIC	Office of the Australian Information Commissioner
ONA	Office of National Assessments
OTT	Over the top services
PIC	Police Integrity Commission
PJCIS	Parliamentary Joint Committee on Intelligence and Security
RSPCA	Royal Society for the Prevention of Cruelty to Animals
SD Act	<i>Surveillance Devices Act</i>
SMS	Short message service
TI	Telecommunications Interception
TIA Act	<i>Telecommunications (Interception and Access) Act 1997</i>
ToR	Terms of reference
UK	United Kingdom
UN	United Nations
URL	Uniform resource locator

US	United States
VPN	Virtual private network
WA	Western Australia
WTO	World Trade Organisation





# List of recommendations

## 2 Telecommunications Interception

### Recommendation 1

The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:

- expresses the dual objectives of the legislation –
  - ⇒ to protect the privacy of communications;
  - ⇒ to enable interception and access to communications in order to investigate serious crime and threats to national security; and
- accords with the privacy principles contained in the *Privacy Act 1988*.

### Recommendation 2

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the:

- privacy impacts of proposed investigative activity;
- public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and
- availability and effectiveness of less privacy intrusive investigative techniques.

The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.

### Recommendation 3

The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

### Recommendation 4

The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*.

Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.

The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.

### Recommendation 5

The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

### Recommendation 6

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- privacy impact of the threshold;
- proportionality of the investigative need and the privacy intrusion;
- gravity of the conduct to be investigated by these investigative means;
- scope of the offences included and excluded by a particular threshold; and
- impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.



### Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications.

The Committee further recommends that the Government model ‘attribute based interception’ on the existing named person interception warrants, which includes:

- the ability for the issuing authority to set parameters around the variation of attributes for interception;
- the ability for interception agencies to vary the attributes for interception; and
- reporting on the attributes added for interception by an authorised officer within an interception agency.

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

- attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;
- oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and
- reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.

### Recommendation 8

The Committee recommends that the Attorney-General’s Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure:

- protection of the security and privacy of intercepted information; and
- sharing of information where necessary to facilitate investigation of serious crime or threats to national security.

### Recommendation 9

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.

### Recommendation 10

The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunications (Interception and Access) Act 1979* be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features:

- a single threshold for law enforcement agencies to access communications based on serious criminal offences;
- removal of the concept of stored communications to provide uniform protection to the content of communications; and
- maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;
- rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;
- reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and
- Parliamentary oversight of the use of interception.

### Recommendation 11

The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.

### Recommendation 12

The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.

### Recommendation 13

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include provisions which clearly express

the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.

#### **Recommendation 14**

The Committee recommends that the *Telecommunications (Interception and Access Act) 1979* and the *Telecommunications Act 1997* be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.

#### **Recommendation 15**

The Committee recommends that the Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions.

#### **Recommendation 16**

The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.

#### **Recommendation 17**

The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority.

The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.

### Recommendation 18

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:

- clear protection for the privacy of communications;
- provisions which are technology neutral;
- maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;
- clearly articulated and enforceable industry obligations; and
- robust oversight and accountability which supports administrative efficiency.

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:

- Independent National Security Legislation Monitor;
- Australian Information Commissioner;
- ombudsmen and the Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

## 3 Telecommunications security

### Recommendation 19

The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide:

- a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference;
- a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and

- powers of direction and a penalty regime to encourage compliance.

The Committee further recommends that the Government, through a Regulation Impact Statement, address:

- the interaction of the proposed regime with existing legal obligations imposed upon corporations;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
- impacts on competition in the market-place, including:
  - ⇒ the potential for proposed requirements to create a barrier to entry for lower cost providers;
  - ⇒ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
  - ⇒ any other relevant effects.

## 4 Australian Intelligence Community Legislation Reform

### Recommendation 20

The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words "and includes multiple computers operating in a network".

The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.

### Recommendation 21

The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee

further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

#### Recommendation 22

The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*.

#### Recommendation 23

The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.

#### Recommendation 24

Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.

#### Recommendation 25

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.

#### Recommendation 26

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.

#### Recommendation 27

The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.

#### Recommendation 28

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.

**Recommendation 29**

The Committee recommends that should the Government proceed with amending the *Australian Security Intelligence Organisation Act 1979* to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.

**Recommendation 30**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004*, in particular by optical devices.

**Recommendation 31**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.

**Recommendation 32**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.

**Recommendation 33**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.

**Recommendation 34**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.

**Recommendation 35**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.

**Recommendation 36**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.

**Recommendation 37**

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code.

The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.

**Recommendation 38**

The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.

**Recommendation 39**

The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the *Australian Security Intelligence Organisation Act 1979* should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.

**Recommendation 40**

The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.



#### Recommendation 41

The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

## 5 Data Retention

#### Recommendation 42

There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- any mandatory data retention regime should apply only to meta-data and exclude content;
- the controls on access to communications data remain the same as under the current regime;
- internet browsing data should be explicitly excluded;
- where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
- the data should be stored securely by making encryption mandatory;
- save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;
- the costs incurred by providers should be reimbursed by the Government;
- a robust, mandatory data breach notification scheme;

- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
- oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

#### Recommendation 43

The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:

- there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;
- there should be an annual report on the operation of this scheme presented to Parliament; and
- the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.



## Glossary<sup>1</sup>

Communications data	Information about a communication event, and not the content or substance of a communication. For landlines, this includes such data as the time and date calls were made and received. For mobile phones, it also includes the location of the communication event. For internet communications, it also includes the username, account name and in some cases the internet protocol addresses allocated to a user. A list of what constitutes communications data is included at Appendix G.
Carriage service provider	A company that supplies a carriage service to the public. This can refer to companies that resell time on a carrier network for telephony and internet access, as well as over the top content and service providers.
Carrier	The owner of a telecommunications network that supplies carriage services to the public.
Content	The content or substance of a particular communication, as opposed to the data relating to that communication.
Data	See Communications data.
Data retention	The storage of communications data.
Encryption	The encoding of data to prevent unauthorised access.
Internet protocol	A standard protocol for transmission of data from source to destination.

---

<sup>1</sup> All definitions are drawn from Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012; and UK Intelligence and Security Committee, *Access to Communications Data by the Intelligence and Security Agencies*, UK Parliament, February 2013.

Internet telephony	See Voice over the internet protocol.
Internet service provider	Any entity that provides access to the internet.
Meta-data	See Communications data
Over the top providers	A service or content on the internet that is not under the administrative control of a carrier or carriage service provider. This includes such services as voice over the internet protocol.
Telecommunications data	See Communications data
Voice over the internet protocol	Technology that allows real-time voice conversations over the internet.

## Introduction

### Background to the inquiry

- 1.1 In May 2012, Attorney-General the Hon. Nicola Roxon MP asked the Parliamentary Joint Committee on Intelligence and Security (the Committee) to inquire into a number of potential reforms to Australia's national security legislation. Subsequent to this request, the Committee was provided with a discussion paper outlining the reforms the Australian Government was considering, as well as some on which the government sought the views of the Committee.
- 1.2 This discussion paper contained the terms of reference for this inquiry which canvassed reforms in three areas: interception of communications and access to data under the *Telecommunication (Interception and Access) Act 1979*; reform of the telecommunications security aspects of the *Telecommunications Act 1997* and other relevant legislation; and reform of the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*. The terms of reference contained 18 specific reform proposals.
- 1.3 The Committee formally adopted the proposed terms of reference on 6 July 2012.
- 1.4 The Committee was faced with two key difficulties in its conduct of this inquiry. Firstly, the terms of reference were very wide-ranging, containing 44 separate items across three different reform agenda. Secondly, the lack of any draft legislation or detail about the potential reforms was a major limitation and made the Committee's consideration of the merit of the reforms difficult. This also made it hard for interested stakeholders to effectively respond to the terms of reference.

## Conduct of the inquiry

- 1.5 The Chair of the Committee, the Hon. Anthony Byrne MP announced the inquiry via media release on 9 July 2012, and the inquiry was subsequently advertised in *The Australian* on 11 July 2012. The Attorney-General's Department discussion paper was published on the Committee website. Letters inviting submissions were sent to over 130 stakeholders in both federal and state government, the telecommunications industry, civil liberties and privacy non-government organisations, and peak legal bodies and associations with an expected interest in the reforms canvassed.
- 1.6 The Committee received 240 submissions and 29 exhibits. These are outlined in Appendices A and B. Three submissions were received in largely identical terms from some 5,300 individual members of the public. These submitters expressed opposition to the reform proposals, and to a mandatory data retention regime in particular. The Committee thanks these members of the public for contributing to the inquiry and making their concerns known.
- 1.7 At all times it was the Committee's preference for submission to be made public. Confidentiality was granted by the Committee where the information had a national security classification such as SECRET or where a submitter made a special request for such confidentiality to the Committee.
- 1.8 Whilst it is the Committee's preference to be open and transparent the use of classified evidence has meant this has not always been possible.
- 1.9 The Committee is grateful to ASIO and ASIS for providing unclassified submissions. This was particularly helpful in the writing of this report.
- 1.10 The Committee held six public hearings, three private classified hearings and a further private hearing. The witnesses who appeared at these hearings are outlined in Appendices C and D.
- 1.11 In addition to its public and classified hearings, the Committee received private briefings from the Attorney-General on two occasions, and received a further private briefing from the Secretary and officials of the Attorney-General's Department.
- 1.12 As the Committee commenced its inquiry, the Government of the United Kingdom issued a draft Communications Data Bill which has similarities to potential reforms in the Australian Government's proposals. The Bill was examined by the British Intelligence and Security Committee (ISC) and a Joint Select Committee of the UK Parliament. The Committee held a private meeting with the ISC where the reform proposals in each country were canvassed. The

Committee appreciated the observations and assistance provided by ISC members and their Secretariat.

- 1.13 Finally, the Committee visited Telstra's Global Operations Centre and received useful briefings from Telstra's staff.
- 1.14 Having commenced the inquiry at the beginning of July 2012, the Committee was asked to report if at all possible by the end of the calendar year. This afforded the Committee a highly compressed and unachievable time frame of less than six months to examine what is an extensive list of potential reforms, some of which are far reaching.
- 1.15 The Committee thanks all submitters and witnesses, including the large number of members of the public who submitted, for their contributions to the Committee's examination of this package of potential reforms of national security legislation.
- 1.16 While the evidence submitted was heavily focussed on data retention, the Committee carefully examined each proposal within the Terms of Reference. In its recommendations the Committee has outlined a strategy for the further development of the potential reforms to national security legislation. Specifically, the Committee believes that detailed consideration of any draft legislative provisions will be necessary. Public consultation must be part of this consideration. As part of this consultation the Committee sees merit in expressly seeking the views of key stakeholders including the Independent National Security Legislation Monitor, oversight bodies, privacy advocates, the telecommunications sector, law enforcement and national security agencies.

## Structure of the report

- 1.17 This report focuses around the terms of reference, and thus comprises four chapters. The following chapters discuss:
- Chapter Two – reform of the government's ability to intercept telecommunications content and data via the *Telecommunications (Interception and Access) Act 1979*;
  - Chapter Three – reform of telecommunications sector security and relevant legislation such as the *Telecommunications Act 1997*; and
  - Chapter Four – reform of the legislation governing the functions and activities of Australia's intelligence community, including the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*.

- Chapter Five – data retention.

1.18 The Terms of Reference group the proposed reforms into three broad categories:

- Matters the Government wishes to progress;
- Matters the Government is considering; and,
- Matters on which the Government expressly seeks the views of the Parliamentary Joint Committee on Intelligence and Security.

1.19 Due to the complexity and number of issues raised in the Terms of Reference it has not always been possible or logical for the Committee to address its comments in accordance with the three broad groupings noted above.

## Chapter Two

1.20 Chapter two looks at a series of proposed reforms to the telecommunications interception regime that are designed to better reflect the 'contemporary communications environment'.<sup>1</sup>

1.21 In particular, the AGD identified four aspects of the legislation as requiring reform:

- Strengthening the safeguards and privacy protections in line with contemporary community expectations;
- Reforming the lawful access regime for agencies;
- Streamlining and reducing complexity; and
- Modernising the cost sharing framework.<sup>2</sup>

1.22 Chapter two deals with each of these areas in detail.

## Chapter Three

1.23 Chapter three looks at emerging challenges to the security of telecommunications data:

Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental misconfiguration, external hacking and even trusted insiders.<sup>3</sup>

---

1 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 22.

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29.



- 1.24 The implications of these risks are significant, especially given that Australian businesses, individuals and public sector actors rely on telecommunication carriers and carriage service providers' (C/CSPs) ability to store and transmit their data safely and securely, and to protect it from potential national security threats. The discussion paper notes that:
- Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.<sup>4</sup>
- 1.25 The chapter looks at the proposed package of reforms to the *Telecommunications Act 1997* and associated legislation to establish this regulatory framework.

## Chapter Four

- 1.26 Chapter four deals with a number of practical difficulties with the legislation governing the operation of the Australian Intelligence Community which is comprised of the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), and the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO) and the Office of National Assessments (ONA).<sup>5</sup>
- 1.27 In relation to these difficulties, the discussion paper canvasses a number of reforms to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act). According to the discussion paper, these reforms are necessary to:
- ...maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.<sup>6</sup>

---

4 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29. An externality refers to a cost or benefit that accrues to actors which are not directly involved in a transaction.

5 On 3 May 2013 the Government announced its intention to rename the DSD and DIGO as the Australian Signals Directorate (ASD) and the Australian Geospatial-Intelligence Organisation (AGO) respectively. <<http://www.minister.defence.gov.au/2013/05/03/prime-minister-and-minister-for-defence-joint-media-release-2013-defence-white-paper-renaming-the-defence-signals-directorate-and-the-defence-imagery-and-geospatial-organisation/>>, viewed on 6 May 2013.

6 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

- 1.28 Chapter 4 of the report looks into these matters and make recommendations where appropriate.

## Chapter Five

- 1.29 The Government sought the Committee's views on a mandatory data retention regime.<sup>7</sup> The Committee did not have access to draft legislation. Furthermore, the inadequate description of data retention in the terms of reference and discussion paper also impaired both the public discussion and the Committee's consideration of the data retention issue.
- 1.30 By far the most controversial topic on which the Committee was asked to provide comment, data retention took up much of the Committee's time. The number of submissions on this issue far exceeded those received on any other topic in the terms of reference.
- 1.31 In correspondence to the Committee, the Attorney-General defined what could potentially be included in a data set for retention. The Attorney-General put forward the European Union data retention directive, which can be found at Appendix F, as an appropriate model.
- 1.32 Many submitters to this inquiry expressed their concerns about content being retained under any mandatory data retention regime. However, by the conclusion of the evidence gathering phase of the inquiry, the Attorney-General and the AGD had categorically stated that it was not the Government's intention to propose a regime that retains content, such as the substance of text messages and emails. However as Chapter Five reveals, there was conflicting evidence from expert witnesses as to whether this was technically possible. Indeed, one of the issues the Committee confronted was the uncertain definitional boundaries between data and content. For completeness, the definitional issue of what constitutes 'data' and 'content' is included in chapter five.
- 1.33 The issue with which the Committee has grappled arises not primarily from a changed threat environment, but from the increasingly rapid development of technological capability which has in many cases outpaced the security services' capacity to respond.
- 1.34 There is no doubt that the enactment of a mandatory data retention regime would be of significant utility to the national security agencies in the performance of their intelligence, counter-terrorism and law enforcement functions. The Committee takes very seriously the security services' concerns for public safety.

---

<sup>7</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

- 1.35 However, a mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed
- 1.36 Ultimately, the reconciliation of these two fundamental public values is a decision for Government to make.
- 1.37 The Committee would have been in a better position to assess the merits of such a scheme, and the public better placed to comment, had draft legislation been provided to it.

## Appendices

- 1.38 In addition to the appendices mentioned above, appendices with relevant information have been provided to assist the reader of the report. They are as follows:
- Appendix E: Discussion paper, *Equipping Australia against emerging and evolving threats*.
  - Appendix F: Correspondence from the Attorney-General regarding data retention.
  - Appendix G: Correspondence from the Secretary of the Attorney-General's Department further clarifying data retention.
  - Appendix H: Telecommunications data provided to law enforcement and national security agencies by Telstra.



## Telecommunications Interception

- 2.1 In its discussion paper, the Attorney-General's Department (AGD) notes that the current *Telecommunications (Interception and Access) Act 1979* (TIA Act):
- ...reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act.<sup>1</sup>
- 2.2 Therefore, the Australian Government has proposed a series of reforms to the telecommunications interception regime that are designed better reflect the 'contemporary communications environment'.<sup>2</sup>
- 2.3 In particular, the AGD identified four aspects of the legislation as requiring reform:
- Strengthening the safeguards and privacy protections in line with contemporary community expectations;
  - Reforming the lawful access regime for agencies;
  - Streamlining and reducing complexity; and
  - Modernising the cost sharing framework.<sup>3</sup>
- 2.4 This chapter will examine each of those proposals. Before doing so, the Committee notes the evidence from interception agencies and the AGD that these

---

1 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 22.

proposals should be considered in the context of a holistic revision of the TIA Act:

The magnitude of current and anticipated change to the telecommunications landscape means it is now timely to consider whether the privacy needs of Australians and the investigative needs of law enforcement and national security agencies are best served through continuous ad-hoc change or whether the time is right to put in place a new interception framework that squarely focuses on the contemporary communications environment. The Department considers that holistic reform would establish a new foundation for the interception regime that enables users and participants, as well as the broader Australian community to understand their powers, rights and obligations.<sup>4</sup>

- 2.5 The Committee's view on whether a new interception regime is necessary will be provided following the consideration of the individual proposals for reform of the TIA Act.

## **Strengthening the safeguards and privacy protections**

- 2.6 The AGD discussion paper expresses a desire to examine the 'safeguards and privacy protections under the lawful access to communications regime' in the TIA Act. In particular, the discussion paper seeks to examine:

- The legislation's privacy protection objective;
- The proportionality tests for issuing warrants;
- Mandatory record-keeping standards; and
- Oversight arrangements by Commonwealth and State Ombudsmen.<sup>5</sup>

### **The legislation's privacy protection objective**

- 2.7 As the discussion paper notes, the interception of telecommunications is 'a powerful and cost effective tool' for law enforcement and intelligence agencies. However, the discussion paper also notes that the ability to intercept telecommunications data and content must be balanced with the protection of privacy:

The primary objective of the current legislation governing access to communications is to protect the privacy of users of telecommunications

---

4 Attorney-General's Department, *Submission No. 218*, pp. 2-3

5 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 7-8.

services in Australia by prohibiting covert access to communications except as authorised in the circumstances set out in the TIA Act.<sup>6</sup>

- 2.8 The discussion paper proposes that the safeguards and privacy protections of the interception regime be strengthened ‘in line with contemporary community expectations’.
- 2.9 Many of the submissions and much of the testimony provided to the Committee focused upon the privacy impact of proposals for reform of the TIA Act, with submitters and witnesses noting that one of the primary objectives of the telecommunications interception regime is to protect the privacy of people against the intrusion of interception.
- 2.10 The proposal for a privacy objective drew broad support, from privacy advocates, private submitters, law enforcement and investigative agencies alike. The Western Australian Police stated:

It is recognised that the privacy protection objective is a fundamental principle which underlies the TIA Act. It is important to protect the privacy of users of telecommunications services by prohibiting covert access to communications except as authorised by the TIA Act.

...

The introduction of a privacy focus objective clause into the TIA Act is appropriate, and would ensure that privacy protection is a consideration in the interpretation and application of the law.<sup>7</sup>

- 2.11 The Law Council of Australia expressed strong support for the introduction of a privacy focused objects clause, and made several suggestions of possible provisions on which it could be modelled:

Such a clause could be modelled on Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which provides that:

- ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’

Article 8 of the European Convention on Human Rights (ECHR) also provides a possible model for such an objects clause. It provides that:

- ‘Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being

---

6 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

7 Western Australia Police, *Submission No. 203*, p. 6.

of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’<sup>8</sup>

- 2.12 The NSW Council for Civil Liberties indicated that a privacy objective would provide an interpretive aid to issuing authorities when considering warrant applications:

A privacy objective should be introduced into the legislation, as the Government proposes. It should be made clear that the privacy objective limits the operations of government agencies as well as those of other persons. This will assist judicial authorities to be tougher in their scrutiny of warrant applications.<sup>9</sup>

- 2.13 The AGD discussion paper refers to strengthening privacy protections in line with contemporary community expectations, but provides no detail on what those expectations are. On that point, Privacy Victoria submitted:

...it is important that we consider what ‘contemporary community expectations’ regarding privacy actually are. For example, in 2007 the Office of the Privacy Commissioner commissioned a survey into community attitudes to privacy. This survey was undertaken at the cusp of the social media boom. In the survey, 86% of respondents felt that it was a serious breach of privacy where a government department monitors an individual’s activities on the internet, recording information on sites visited without the individual’s knowledge. Similarly, 50% were more concerned than two years previous (2005) about providing information over the internet. I consider that these numbers would be greater today, given the mass of information collected by electronic means.<sup>10</sup>

- 2.14 The Information Commissioner suggested that the *Privacy Act 1988* reflects community privacy expectations:

The OAIC considers that the *Privacy Act 1988* (C’t’h) (Privacy Act), as the privacy oversight instrument the public is most familiar with, reflects existing community expectations. Accordingly, incorporating the core principles and values that underpin the Privacy Act into the other privacy accountability frameworks will help ensure that they remain consistent with community values and expectations.<sup>11</sup>

---

8 Law Council of Australia, *Submission No. 96*, pp. 21-2.

9 NSW Council for Civil Liberties, *Submission No. 175*, p. 15.

10 Privacy Victoria, *Submission No. 109*, p. 3.

11 Office of the Australian Information Commissioner, *Submission No. 183*, pp. 1-2.



- 2.15 While supportive of a privacy objective, the Western Australian Corruption and Crime Commission noted the need to balance privacy with investigative needs:

The Commission supports the primary objective of the TIA Act which seeks to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act does this by making it an offence to intercept communications passing over the telecommunications system. However this needs to be balanced against Australia's law enforcement and national security interests.<sup>12</sup>

- 2.16 Similarly, Privacy Victoria assisted the Committee by noting the need to balance other considerations:

Privacy is not an absolute right. A balance must be struck between privacy and other rights, including the public interest in protecting the safety and security of Australians. This balancing act is a central tenet to privacy legislation around the world, and at times privacy must give way to other public and private interests.<sup>13</sup>

- 2.17 The Committee recognises the dual objectives of the TIA Act: to protect the privacy of communications by prohibiting unlawful interception, while enabling limited interception access for the investigation of serious crime and threats to national security. Express recognition of these objectives within the legislation would provide clarity of the purposes of the legislation and some interpretive guidance.

---

12 Western Australian Corruption and Crime Commission, *Submission No. 156*, p. 4.

13 Privacy Victoria, *Submission No. 109*, p. 1.

## 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*.

## The proportionality tests for issuing warrants

2.18 The AGD submission outlined the factors which must be considered by an issuing authority prior to issuing telecommunications interception warrants:

The independent authority may issue the warrant if satisfied from the facts outlined in the affidavit that:

- there are reasonable grounds for suspecting that the person is using or is likely to use the service;
- that information obtained under interception would be likely to assist the investigation of a serious offence in which the person is involved;
- and having regard to:
  - ⇒ the privacy of any persons likely to be interfered with by interception;
  - ⇒ the gravity of the conduct being investigated; and
  - ⇒ the extent to which other methods of investigating the offence have been exhausted or would prejudice the investigation.<sup>14</sup>

2.19 Submitters expressed support for the existence of the proportionality tests within the TIA Act, but expressed frustration about the absence of detailed proposals on which to comment. For example, Mr Bernard Keane stated:

---

14 Attorney-General's Department, *Submission No. 218*, Attachment A p. 1.

The paper is unclear about exactly what ‘strengthening’ is intended beyond a review and consideration of ‘a privacy focused objects clause’. Strengthening privacy laws and reviewing checks and balances is of course unobjectionable; but AGD has failed to even clearly describe its thinking on this important issue.<sup>15</sup>

- 2.20 The Law Council of Australia noted that one way to strengthen the privacy protections within the TIA Act is to ensure consistent consideration of the impact of privacy before any power under the TIA Act is exercised:

...the requirement to consider the extent to which the exercise of a power will interfere with personal privacy currently applies to the issuing of certain TIA Act warrants, but not all.

For this reason, the Law Council supports the inclusion of a single, consistent privacy test in all warrant applications and in all authorisations to intercept, access or disclose telecommunications or telecommunications data.<sup>16</sup>

- 2.21 The Australian Federal Police (AFP) expressed support for strengthening the proportionality test for telecommunications interception warrants, noting that the current formulation has ‘becoming increasingly out of balance to the changes in the way people communicate, the technology available to communicate and the use of that technology to commit crime’.<sup>17</sup> As a result, the AFP:

...sees benefit in strengthening the existing proportionality test to include consideration of the overall community good served by the investigation for which the interception is sought.<sup>18</sup>

- 2.22 The Western Australia Police submitted that ‘the current provisions of the TIA Act provide sufficient scope for the proportionality test to be properly applied’<sup>19</sup> and did not seek change to the proportionality test.

- 2.23 The Committee notes the useful discussion of proportionality tests provided by the Human Rights Law Centre in its submission:<sup>20</sup>

---

15 Mr Bernard Keane, *Submission No. 117*, p. 3. See also Mr Robert Batten, *Submission No. 50*, p. 3; Mr Ian Quick, *Submission No. 95*, p. 4.

16 Law Council of Australia, *Submission No. 96*, p. 23.

17 Australian Federal Police, *Submission No. 163*, p. 8.

18 Australian Federal Police, *Submission No. 163*, p. 8.

19 Western Australia Police, *Submission No. 203*, p. 6. See also: Western Australian Corruption and Crime Commission, *Submission No. 156*, pp. 4-5.

20 Human Rights Law Centre, *Submission No. 140*, pp. 2-3.

Put broadly, general provisions setting out a proportionality analysis require that any limitation of rights be reasonable and demonstrably justified in a free and democratic society.

- 2.24 The Committee considers the TIA Act must continue to require the consideration of proportionality in authorising the use of telecommunications interception as an intrusive investigative technique. Given the evidence cited above the Committee believes it is appropriate that a review of the TIA Act's proportionality tests be carried out. Any review of the proportionality tests must consider a range of matters to be included in the test, including the gravity of the conduct being investigated, the privacy intrusion of proposed investigative activity, the public interest served by the proposed investigative activity, and whether other less privacy intrusive investigative techniques would be effective.
- 2.25 The Committee further considers there would be merit when reviewing the proportionality tests to examine the application of those tests across the range of powers in the TIA Act (interception, access to stored communications, and access to telecommunications data).

## 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.**

## Mandatory record-keeping standards

- 2.26 The AGD discussion paper outlines the current TIA Act record-keeping requirements:

Record keeping and accountability obligations require law enforcement agencies to keep records relating to documents associated with the

warrants issued and particulars relating to warrant applications (such as whether an application was granted or refused) and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed. Agency heads must also report to the Attorney-General on the use and communication of intercepted information within three months of a warrant ceasing to be in effect. The Attorney-General's Department must prepare an annual statistical report about the use of powers under the TIA Act, which the Attorney-General tables in Parliament.<sup>21</sup>

- 2.27 The AGD discussion paper goes on to argue 'the current regime is focused on administrative content rather than recording the information needed to ensure that a particular agency's use of intrusive powers is proportional to the outcomes sought'.<sup>22</sup> The AGD therefore recommends:

Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes.<sup>23</sup>

- 2.28 Two submissions suggested that a streamlined reporting regime could lead to significant weakening of oversight. For example, Mr Bernard Keane stated:

An alternative view is that 'inflexible' and 'one size fits all' provisions ensure that agencies cannot try to avoid reporting obligations and report in a manner that will enable meaningful comparisons over time and with other agencies. For relatively minor regulatory requirements, a 'co-regulatory approach' such as that proposed by AGD might be appropriate, but given the serious nature of the issues on which law enforcement and intelligence agencies are being asked to report, it is wholly inappropriate to leave it up to agencies themselves to determine exactly how and what they report within a general remit. This would represent a significant weakening of accountability in an area where there is already too little scrutiny.<sup>24</sup>

- 2.29 The Committee received evidence from law enforcement agencies regarding the application of the existing record-keeping requirements. For example, the AFP stated:

---

21 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

22 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

23 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

24 Mr Bernard Keane, *Submission No. 117*, p. 3. See also Electronic Frontiers Australia, *Submission No. 121*, pp. 12-13

The AFP believes the current legislated scheme needs review. It may have reached the point where it is too focussed on administrative requirements, rather than providing the basis for Parliament and the Ombudsman to ensure agencies are using the powers in the Act in a way that is consistent with the principles underlying the Act. There would be value in redrafting the legislation to include simplified, comprehensible and meaningful accountabilities and annual reporting obligations to enhance community understanding of the regime and its safeguards.<sup>25</sup>

2.30 In support of this observation, the AFP cited the example of the requirement to provide a certified copy of each warrant despite the obvious efficiencies provided by email or facsimile communications.<sup>26</sup>

2.31 Similarly, the Western Australia Corruption and Crime Commission submitted:

The Commission fully supports a robust regime of mandatory record-keeping standards for agencies exercising powers under the TIA Act. The Commission acknowledges that effective oversight of agencies' use of these powers requires appropriate record-keeping standards sufficient to show compliance with the legislation. However it is the view of the Commission that many of the requirements of the current Act create unnecessary duplication of records and the creation of further records which no longer serve the original purpose of ensuring compliance with the Act and the creation of a robust compliance regime.<sup>27</sup>

2.32 The Law Council of Australia expressed support for streamlining the record-keeping requirements of the TIA Act to ensure they provided effective accountability:

The Law Council strongly supports efforts to ensure that the reporting requirements and oversight mechanisms contained in the TIA Act are '...attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes', as suggested by the Discussion Paper. This may involve review and reform of the different procedural and administrative requirements currently contained in the TIA Act relating to reporting, and to the role of the Commonwealth Ombudsman and his or her State and Territory counterparts. It may also involve consideration of additional or alternative mechanisms to enhance accountability under the TIA Act.<sup>28</sup>

---

25 Australian Federal Police, *Submission No. 163*, p. 9.

26 Australian Federal Police, *Submission No. 163*, p. 9.

27 Western Australia Corruption and Crime Commission, *Submission No. 156*, p. 5. See also Western Australia Police, *Submission No. 203*, pp. 6-7.

28 Law Council of Australia, *Submission No. 96*, p. 48.

- 2.33 The Law Council of Australia cautioned against ‘removing requirements for agencies to collect and record certain information about the exercise of their powers under the Act’ citing the example of the register of warrants maintained by the Secretary of the AGD.<sup>29</sup>
- 2.34 The Committee strongly supports the need for record-keeping requirements as a means of ensuring meaningful oversight and accountability. The TIA Act enables law enforcement and security agencies to exercise intrusive powers. It is vital to the ongoing ability of those agencies to use those powers to be able to demonstrate adherence to the accountability requirements of the TIA Act. During the inquiry, the Committee received assurance from the Commonwealth Ombudsman’s office and the Inspector-General of Intelligence and Security of the high level of accountability discharged by the interception agencies.<sup>30</sup>
- 2.35 The Committee acknowledges, however, that record-keeping is not an end in itself, and must be designed to provide substantive rather than administrative accountability. The Committee is satisfied that there is scope for achieving efficiencies by reviewing the existing reporting requirements without undermining accountability. Further, the Committee considers there is scope to enhance accountability by removing otiose reporting requirements.

### 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.**

## Oversight arrangements by the Commonwealth and State Ombudsmen

- 2.36 The AGD discussion paper outlines the present oversight arrangements for law enforcement agencies:

Oversight of law enforcement agencies’ use of powers is split between the Commonwealth Ombudsman and equivalent State bodies in relation to interception activities. The Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications. This split in responsibility contrasts with the

29 Law Council of Australia, *Submission No. 96*, p. 48.

30 See for example, Inspector-General of Intelligence and Security, *Submission No. 185*, p. 8.

*Surveillance Devices Act 2004*, where the Commonwealth Ombudsman inspects all agencies.<sup>31</sup>

- 2.37 The AGD goes on to note that the prescriptive form of the TIA Act oversight provisions 'impede the Ombudsman's ability to report on possible contraventions and compliance issues by prescribing detailed and time limited procedures that need to be checked for administrative compliance, rather than giving the Ombudsman scope to determine better ways of assisting agencies to meet their requirements.'<sup>32</sup>
- 2.38 The Committee received submissions from law enforcement agencies expressing support for the review of the oversight arrangements to clarify the roles played by different oversight bodies. For example, the Western Australia Police stated:

The TIA Act currently creates a system based on dual oversight by both Commonwealth and State Ombudsman. The role of the oversight body, and the scope of inspection, could be better defined within the TIA Act.

For WA Police, stored communications are inspected by the Commonwealth Ombudsman, annually. Inspections of all other TI Warrants, and the corresponding revocations, destruction of, and associated record keeping, is conducted by the State Ombudsman, on a regular basis.

On occasion, the Commonwealth Ombudsman has made comment on the content of an affidavit in support of an application for a stored communications warrant, and has questioned the appropriateness of the application. WA Police is of the opinion that the determination of the application, and the appropriateness or otherwise of the information contained in the affidavit is a matter for the issuing authority, not the oversight body. It is noted that the issuing authority has the power to receive information in both written and oral form.

An examination of the existing oversight arrangements, the clarity of the role, and the practicality of a single oversight body is supported by WA Police.<sup>33</sup>

- 2.39 Similarly, Telstra noted a desire for consistency of oversight arrangements:

Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy

---

31 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

32 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 26.

33 Western Australia Police, *Submission No. 203*, p. 7.



protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.<sup>34</sup>

- 2.40 The Office of the Australian Information Commissioner noted risks inherent in the fragmentation of oversight arrangements:

...the OAIC notes that the fragmentation of existing oversight arrangements can make it difficult for the public to discern which oversight body is responsible for overseeing the access and interception activities of a particular law enforcement agency. The OAIC is mindful that the nature of the activities undertaken by law enforcement agencies may mean that, in certain circumstances, it is not appropriate for these activities to be made public. In these circumstances, it is particularly important that effective oversight arrangements exist to ensure that these agencies are not exceeding their lawful authority and to give the public confidence that their personal information is being handled in accordance with contemporary community expectations. The OAIC suggests that providing the public with clear information about which oversight bodies are responsible for overseeing the access and interception activities of specific law enforcement agencies would provide a more appropriate level of transparency.<sup>35</sup>

- 2.41 The Law Council of Australia noted its support for consideration of a model similar to the *Surveillance Devices Act 2004* (Cth) whereby the Commonwealth Ombudsman would be the sole oversight body for law enforcement agencies under the TIA Act:

The Law Council supports consideration of this model for potential application to the TIA Act warrant regime, which currently imposes inspection and reporting obligations on State bodies in respect of State agencies' interception activities under the TIA Act. However, if a reform of this nature is to be pursued it must be developed in consultation with State and Territory Ministers and should not detract from the other reporting requirements outlined in the TIA Act...<sup>36</sup>

- 2.42 The Committee believes that reviewing the TIA Act oversight regime to ensure the application of consistent standards of accountability and a single perspective on best practice is warranted. On the evidence before it, the Committee was not persuaded that the *Surveillance Devices Act* model is appropriate. The Committee is also aware of significant jurisdictional issues inherent in progressing this matter..

---

34 Telstra, *Submission No. 189*, p. 6.

35 Office of the Australian Information Commissioner, *Submission No. 183*, p. 12.

36 Law Council of Australia, *Submission No. 96*, p. 50.

## 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.**

## Reforming the lawful access regime for agencies

- 2.43 The second aspect of the legislation in need of reform identified by the AGD discussion paper is the current lawful access regime. The AGD identifies several areas for specific examination. First, it seeks to reform the lawful access to communications regime contained in the TIA Act by 'reducing the number of agencies eligible to access communications information'. Second, it seeks to standardise warrant tests and thresholds. Third, it seeks to expand 'the basis of interception activities'.<sup>37</sup>

### Reducing the number of agencies eligible to access communications information

- 2.44 The AGD discussion paper states that a reduction in the number of agencies able to access communications information is contemplated 'on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so'.<sup>38</sup>
- 2.45 A range of submissions cited with approval the proposal to reduce the number of agencies able to access communications information, but noted the difficulty in identifying which agencies should have these powers removed. Ms Stella Gray commented:

---

37 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 8, 9.

38 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 24.

Reducing the number of government agencies which have access to individuals' private communications, reduces the ability to abuse the TIA. However, there is insufficient detail here on which agencies are being considered for reduction in such powers.<sup>39</sup>

2.46 Similarly, Liberty Victoria submitted:

Liberty Victoria agrees that lawful access by agencies to telecommunications data ought to be restricted to protect the privacy rights of individuals. Liberty Victoria agrees that reducing the number of agencies able to access sensitive data is, in principle, important and necessary. Liberty Victoria would, however, like to understand further how the Government proposes to determine which agencies are able to access this data, to ensure that there are real and substantive security benefits proportionate to the greater privacy risks that arise when information is more widely disseminated.

The Discussion Paper's suggestion that agencies must have a 'demonstrated need' to access information, while a good suggestion (indeed, a suggestion that one would have hoped already applied to agencies' access to personal information), is too general to offer a detailed response. For example, it does not indicate how 'need' would be demonstrated as opposed to 'operational convenience'..<sup>40</sup>

2.47 The Attorney-General's Department outlined to the Committee which agencies have access to telecommunications information:

Currently, access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an 'enforcement agency' to authorise a C/CSP to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. There are separate provisions enabling access for national security purposes.

An enforcement agency is broadly defined as all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. In practice, the range of agencies that are enforcement agencies and which authorise the disclosure of telecommunications data is very broad and includes Shire Councils, Government Departments and Agencies such as Centrelink and bodies as the Royal Society for the

---

39 Ms Stella Gray, *Submission No. 152*, p. 7.

40 Liberty Victoria, *Submission No. 143*, p. 6. See also Mr Bernard Keane, *Submission No. 117*, pp. 3-4; Senator Scott Ludlum, *Submission No. 146*, p. 3; Mr Ian Quick, *Submission No. 95*, p. 5.

Prevention of Cruelty to Animals (RSPCA) (which plays a role in investigating assaults and other criminal acts against animals).<sup>41</sup>

2.48 The Committee noted that in 2010-11 there were 251,631 requests for access to telecommunications data from a variety of agencies including police forces, anti-corruption bodies, Commonwealth and State and territory departments, local shire councils, animal protection authorities, roads authorities, revenue offices, and child support agencies.<sup>42</sup>

2.49 Ms Irene Graham submitted that the range of agencies able to access stored communications and communications data should be reduced:

The range of agencies should certainly be reduced, and probably most especially by deleting all, or most, of the civil and pecuniary penalty agencies that acquired power to obtain access to stored communications when the 'stored communications' warrants were introduced in 2006 (although such agencies were not and still are not authorised to obtain interception warrants).

...

There absolutely does need to be a competent review conducted into which of such agencies have a clearly demonstrated need to access stored communications and/or telecommunications 'data' in specific circumstances, together with consideration of the type of offences and the penalties that apply to any offences in relation to which such agencies claim 'a need'.<sup>43</sup>

2.50 Telstra submitted the TIA Act could be amended to differentiate between types of telecommunications data, with limited agencies being permitted to access sets of data considered to be more sensitive:

Telstra believes there is some merit in adopting a two-tiered communications data access regime to address potential risks of allowing access to customer data for the investigation of lesser offences. Under this type of regime, data readily available through C/CSP customer information systems could be provided under the current threshold test and would potentially remain accessible to a larger number of enforcement agencies and LENSAs [Law Enforcement and National Security Agencies].

Under this construct, access to more intrusive communications data, e.g. URLs, IP addresses or 'created' tailored data sets proposed under the data

---

41 Attorney-General's Department, *Submission No. 218*, p. 9.

42 Telecommunications (Interception and Access) Act 1979 Annual Report 2010-11, pp. 62-5.

43 Ms Irene Graham, *Submission No. 135*, p. 5.

retention regime, would only be provided to a limited number of LENSAs and would require higher approval thresholds to be satisfied.<sup>44</sup>

- 2.51 An alternative approach was submitted by the Australian Mobile Telecommunications Association and Communications Alliance in their joint submission:

The Associations believe that rather than looking to define the number of agencies that are eligible to access communications information (that being content and transactional data), a preferred approach should be to reserve access to communications information solely for purposes of addressing instances of serious crime or threats to national security. The nature of the crime/threat in each instance would then determine the type of information required, and the agency/agencies who are eligible to obtain access. If this approach is taken it will be important to be clear about what constitutes 'serious crime'.<sup>45</sup>

- 2.52 The Committee was not able within the confines of this inquiry to examine the justification for each enforcement agency to be able to continue to access telecommunications data. It was clear from the evidence however that the present definition of enforcement agency, being broad and inexhaustive, leaves the potential for many agencies to request access to telecommunications data without independent scrutiny other than from the telecommunications providers who receive those requests. This is not an acceptable burden to place on telecommunications providers, nor is the Committee convinced that this is an effective accountability mechanism.
- 2.53 The Committee considers the appropriate mechanism to justify access to telecommunications data is the threshold at which access is granted. The threshold acts to establish the level of gravity of the conduct which must be under investigation before the privacy intrusion of accessing telecommunications data can be justified.
- 2.54 The Committee is satisfied that access to telecommunications data for serious crime and threats to security is justified. Access for agencies not enforcing the criminal law or investigating security threats should be subject to further review.

---

44 Telstra, *Submission No. 189*, p. 6.

45 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 7.

## 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.**

### Standardise warrant tests and thresholds

- 2.55 In its submission to the Committee, the AGD addressed possible changes to the tests for telecommunications interception warrants, specifically the threshold at which interception warrants are available:

Warrants relating to accessing real-time content are traditionally limited to investigating an offence that carries a penalty of at least seven years imprisonment: a 'serious offence' as defined in section 5D of the TIA Act. Section 5D is an exhaustive list which includes offences by reference to other Commonwealth legislation (such as an offence against Part 10.7 of the Criminal Code Act 1995) or of a certain type (such as murder) or involving certain conduct (such as trafficking in prescribed substances) all of which generally require at least seven years imprisonment.

...

The Department considers that these requirements should not change: access to real-time content should continue to be subject to an independently issued warrant for the investigation of a serious offence.

...

The Department is concerned that the growing complexity of section 5D of the TIA Act is inefficient in terms of police resources needed to clarify the application of the provision in specific circumstances and, more importantly, potentially privacy invasive in its lack of clarity about how and ...

The Department considers that the interception regime would offer greater privacy protection if the distinction between stored and live warrants was removed and if a standard threshold for both content and stored communications warrants was introduced.<sup>46</sup>

- 2.56 The issue of a standard threshold for TIA Act warrants attracted significant evidence for the Committee's consideration. Many submitters acknowledged the potential administrative efficiencies to be gained from standardisation, but

<sup>46</sup> Attorney-General's Department, *Submission No. 218*, p. 5.

objected to the potential for warrant thresholds to be lowered. For example, Liberty Victoria submitted:

Standardisation of interception warrant tests must not compromise human rights – Liberty Victoria recognises that there may be operational benefits in standardising various warrant tests. However, we are concerned to ensure that any standardisation process does not compromise human rights in the name of operational efficiencies. In particular, we oppose any reduction of the general threshold for interception so that it applies to offences with maximum penalties of less than 7 years' imprisonment.<sup>47</sup>

2.57 The Committee also received extensive evidence from law enforcement agencies regarding the complexity of the present threshold for telecommunications interception warrants. For example, Victoria Police submitted:

The definition of serious offence pursuant to section 5D of the TIA Act is long, complex and outdated and it excludes offences which should be so classified. There are offences Victoria Police routinely investigates that are serious in nature, but are not specified in the definition or only become serious offences if they meet certain additional conditions such as being part of a series of offences, involve substantial planning and organisation and sophisticated methods and techniques.

Offences that are serious in nature but are not captured in this section include blackmail and perverting the course of justice, where an investigative method such as telecommunications interception would assist in the investigation of offenders charged with serious crimes attempting to arrange false alibis or have witnesses change their statement and/or provide false evidence.<sup>48</sup>

2.58 Similarly the Western Australia Police submitted:

At present, under the TIA Act, it is not possible to obtain an interception warrant with respect to offences which carry a penalty of less than 7 years imprisonment but which may be preparatory to more serious offending. For example, precursor or preparatory crimes could include selling unregistered firearms, pervert the course of justice or stealing a motor vehicle. The ability to intercept communications in relation to precursor offences may assist in the prevention of more serious offending.

WA Police would welcome an examination of the current definition of serious offence and serious contravention contained in the TIA Act

---

47 Liberty Victoria, *Submission No. 143*, p. 2. See also Mr Bernard Keane, *Submission No. 117*, p. 4; Electronic Frontiers Australia, *Submission No. 121*, p. 13; Pirate Party Australia, *Submission No. 134*, p. 12; and Ms Stella Gray, *Submission No. 152*, p. 8.

48 Victoria Police, *Submission No. 200*, p. 7.

(section 5D and section 5E). The current definition is complex and unwieldy, and requires simplification.<sup>49</sup>

- 2.59 The appropriate threshold for access to the content of communications is a complex issue. As noted by the Australian Competition and Consumer Commission, stored communications warrants are available for pecuniary penalty offences in addition to the threshold set by a period of imprisonment:

In the main, telephone interception is limited to investigation of serious offences under criminal law where the conduct is punishable by seven years' imprisonment or more. In contrast, stored communications warrants can be issued by a judge for serious contraventions of civil or criminal law involving a fine or pecuniary penalty equivalent to at least \$19,800 (individuals) or \$99,000 (businesses), as well as for serious criminal offences capable of interception.<sup>50</sup>

- 2.60 Rather than lowering the existing threshold, the Law Council of Australia advocated lifting the relevant thresholds:

The Law Council is of the view that it is appropriate for the offence threshold for stored communication warrants to be reviewed and raised to apply only to criminal offences. Consideration should also be given to raising this threshold to 'serious offences', as defined in section 5D of the TIA Act, in recognition of the private nature of stored communication information and to better align the stored communication warrant process with that required for telecommunication interception warrants.<sup>51</sup>

- 2.61 As stated by the Inspector-General of Intelligence and Security, 'proposals to standardise security warrant tests and thresholds must take into account the nature of each of these warrants and the level of intrusiveness.'<sup>52</sup>

- 2.62 The Committee notes that there are differing penalty thresholds within the TIA Act, and between the TIA Act and other electronic surveillance powers (such as the *Surveillance Devices Act 2004*). The appropriate threshold for access to telecommunications and access to stored communications (whether they be combined under a single test) requires a careful consideration of the:

- 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;

---

49 Western Australia Police, *Submission No. 203*, p. 8.

50 Australian Competition and Consumer Commission, *Submission No. 192*, p. 5.

51 Law Council of Australia, *Submission No. 96*, p. 30.

52 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 9.



- impact on law enforcement agencies investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences; and
- privacy impact.

2.63 The Committee is not able, upon the evidence before it, to reach a final position about the appropriate threshold for access to telecommunications and stored communication. Rather, the Committee is attracted to the proposal from the AFP for a further review to consider this issue:

The appropriateness of these separate warrant tests and offence thresholds should be reviewed taking into consideration the contemporary use of communications in society generally and by persons of interest in the commission of crime, and the nature of the technology underpinning telecommunications and internet communication services. A key example of this is the increasing use of stored communication as a means of covert communication.

From a law enforcement perspective such a review needs to take into account the basis of the gravity of the conduct; the increasingly ubiquitous nature of telecommunications content and stored communications as evidence of the commission of an increasing number of offences that cause significant harm to the community, and the transitory nature of that content. It may be that the differentiation currently imposed between the two forms of content is no longer appropriate and that a reviewed and unified threshold would be more appropriate to meet both community expectations and law enforcements needs.<sup>53</sup>

2.64 The Committee notes that telecommunications interception warrants may be issued for the investigation of offences with a maximum penalty of at least seven years imprisonment but stored communications warrants may be issued for the investigation of offences with a significantly lower threshold of at least three years imprisonment as a maximum penalty. There is arguably very little difference in the privacy impact carried out if communications are accessed live via interception or after the communication takes place when accessed with a stored communications warrant. The Committee is of the view that covert access to communications should not distinguish between access methods, and that therefore the penalty threshold should be standardised.

---

53 Australian Federal Police, *Submission No. 163*, pp. 9-10.

## 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.

## Expanding the basis of interception activities

2.65 The AGD discussion paper describes the challenge to the ongoing effectiveness of telecommunications interception as follows:

Telecommunications interception and access to communications data are unique and fundamental tools that cannot be replaced by other investigative techniques. They are cost effective, timely, low risk and extremely successful tools in obtaining intelligence and evidence. Substantial and rapid changes in communications technology and the business environment are rapidly eroding agencies' ability to intercept. Adapting the regime governing the lawful access to communications is a fundamental first step in arresting the serious decline in agencies' capabilities.<sup>54</sup>

2.66 The Committee notes the effectiveness of telecommunications interception as an investigative technique. The *Telecommunications (Interception and Access) Act 1979 Annual Report for 2010-11* notes that intercepted information contributed to 2441 arrests, 3168 prosecutions, and 2034 convictions for the 2010-11 financial year.<sup>55</sup>

2.67 The Committee took evidence on the decline in agencies' interception capability, referred to as 'going dark':

54 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 23.

55 Telecommunications (Interception and Access) Act 1979 Annual Report 2010-11, pp. 42, 44-5.

In terms of this concept of going dark, it is certainly something that is being increasingly discussed amongst the law enforcement fraternity and it is a recognition primarily of these new technologies that we are unable to intercept for a range of reasons. That is one of the areas that I would respectfully suggest that the committee needs to consider in terms of the ongoing viability of telecommunications interception generally.<sup>56</sup>

2.68 The AFP submitted that the telecommunications environment has shifted considerably since 1979 resulting in significant challenges to interception:

That industry environment no longer exists. Several service or application providers may be involved in any one communication event. Individuals often use multiple devices and applications to communicate and free accounts can be established quickly and with no clear connection to a real life identity. Further, the current approach presupposes that the communications are between people using devices, not machine based communications as may be used through botnets or other internet based crimes where communications content is an important source of evidence. Into the future, given the move from circuit based to IP based telecommunication services, identifying communications between persons will become increasing challenging.

In light of this it is no longer viable to continue to base interception solely on the traditional network identifiers prescribed in the TIA Act. For this reason the AFP considers additional bases for interception such as the concept of communications of interest that relate to the offence under investigation would be of benefit. This concept could include the source of a communication, the destination of a communication, and the type of communication.<sup>57</sup>

2.69 The Committee heard evidence that a proposal for 'attribute based interception' would assist in countering the decline of capability caused by technological and counter-security measures. The Western Australia Corruption and Crime Commission explained the proposal:

Being able to identify particular communications within the service, for example, may allow agencies to exclude or include particular communications through relevant identifiers. For example, if an internet based interception were to be conducted on a user's account the agency may only be interested in particular communications such as those linked to an email address or internet chat protocol. By expanding the basis for interception activity, agencies may be able to exclude other

---

56 Detective Inspector Gavan Seagrave, *Transcript*, 5 September 2012, pp. 29-30.

57 Australian Federal Police, *Submission No. 163*, pp. 12-13.

communications thereby better targeting the communications of interest and providing greater privacy protection by excluding other content.<sup>58</sup>

- 2.70 A range of submissions noted the potential privacy protection which could be achieved by introducing a warrant which better targeted communications on the basis of specific attributes. Those submissions noted however the need to ensure appropriate oversight and accountability of the proposed warrant type:

The Law Council recognises the challenges existing and emerging telecommunications technologies pose for agencies attempting to accurately identify the communications they intend to intercept or access. For this reason, the Law Council generally supports 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 that any proposed 'simplification of the warrant process' 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.<sup>59</sup>

- 2.71 Liberty Victoria similarly expressed in principle support subject to appropriate oversight and accountability arrangements:

Liberty Victoria is not at this stage opposed to further consideration being given to expanding interception obligations from the network/service layer to the application layer. Interception at the network/service layer often involves casting the net of information to be intercepted too broadly, with a greater risk of capturing irrelevant and innocent communications. However, any expansion must be accompanied by the adoption of appropriate safeguards and accountability mechanisms.<sup>60</sup>

- 2.72 Other submissions expressed concern at the potential impact on privacy which may result from expanding the basis of interception:

When viewed in the context of a proportional response to the current threat landscape I do not feel that the expansion of interception activities as outlined in the ToR and discussion paper are proportional to the massive invasion of privacy entailed. The cost to our privacy is too high in relation to a threat that if anything is subsiding and to which it appears

---

58 WA Corruption and Crime Commission, *Submission No. 156*, p. 10.

59 Law Council of Australia, *Submission No. 96*, p. 31

60 Liberty Victoria, *Submission No. 143*, p. 3.

the security agencies of our nation have enough tools to combat effectively anyway.<sup>61</sup>

2.73 The AGD submission described the present considerations an issuing authority must address prior to issuing a telecommunications interception warrant:

The independent authority may issue the warrant if satisfied from the facts outlined in the affidavit that:

- there are reasonable grounds for suspecting that the person is using or is likely to use the service
- that information obtained under interception would be likely to assist the investigation of a serious offence in which the person is involved
- and having regard to:
  - ⇒ the privacy of any persons likely to be interfered with by interception
  - ⇒ the gravity of the conduct being investigated, and
  - ⇒ the extent to which other methods of investigating the offence have been exhausted or would prejudice the investigation.<sup>62</sup>

2.74 The Committee received evidence from the Commonwealth Ombudsman and Inspector-General of Intelligence and Security. No issue of substantive non-compliance by the interception agencies was raised before the Committee. The Inspector-General of Intelligence and Security did raise, however, a range of issues for consideration should this proposal be adopted:

A key issue to be considered in this proposal is whether the warrants would be limited to interception based on the 'characteristics' described in the initial warrant (similar to a service warrant) or whether ASIO would itself be able to vary the warrant to add or remove 'characteristics' (similar to a named person warrant). If the proposal is for the latter then there needs to be certainty as to the parameters within which 'characteristics' can be added.

...

A further issue is the technological capacity to actually undertake this type of 'characteristic'-based interception – including whether the carriers should be responsible for collecting, processing and delivering the communications of interest or whether the agencies should be permitted to collect and retain large amounts of information in order to find the communications of interest. It is outside my area of focus to comment on the technology, cost or burden sharing aspects of the proposal. However I would expect to see any regime include appropriate measures to ensure

---

61 Mr Daniel Judge, *Submission No. 157*, p. 9. See also J Trevaskis, *Submission No. 62*, p. 8; Mr Mark Newton, *Submission No. 87*, p. 9, and James (no further details), *Submission No. 7*.

62 Attorney-General's Department, *Submission No. 218*, Attachment A p. 1

that the content of communications which were not the specific target of the warrant were not retained longer than necessary for 'sorting' and to ensure that such information is kept secure.

One of the important accountability and oversight requirements of the current regime is the requirement that ASIO provide a report to the Attorney-General after the expiration or revocation of each warrant. The report must include details of the telecommunications service to or from each intercepted communication was made as well as the extent to which the warrant has assisted ASIO in carrying out its functions. This measure would be particularly important in maintaining oversight and accountability of any discretion to add new characteristics for interception.<sup>63</sup>

- 2.75 The Committee agrees with the need to ensure that telecommunications interception powers remain subject to appropriate accountability and oversight, including a robust system for obtaining telecommunications interception warrants from independent issuing authorities who have considered the privacy, proportionality and investigative necessity of proposed interception activities.
- 2.76 The Committee notes the potential for attribute based interception to assist in 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.
- 2.77 Possible attributes which may be used in these warrants include:
- Time of a communication;
  - Location of a communication; and
  - an identifier or address that uniquely identifies a service or account.

---

63 Inspector-General of Intelligence and Security, *Submission No. 185*, pp. 11-12.

## **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.**

## **Streamlining and reducing complexity**

2.78 The AGD discussion paper also identified the need to reduce complexity in the lawful access regime as a driver of potential reform. As such, it sought an examination of:

- **Ways to simplify the provisions that allow the various agencies to share information and cooperate;**
- **The removal of legislative duplication; and**

- The creation of a single warrant with multiple telecommunications interception powers.<sup>64</sup>

## Simplifying the information sharing provisions that allow agencies to cooperate

- 2.79 The TIA Act is drafted in prescriptive terms, based on the premise that interception is prohibited unless authorised by one of the limited exceptions. The prescriptive nature of the regime continues in the provisions which regulate the use and communication of intercepted information. The AGD Discussion paper explains:

Information obtained under the *Telecommunications (Interception and Access) Act 1979* is subject to more rigorous legislative protections than other forms of information in an agency's possession. The provisions are detailed and complex in relation to record keeping, retention and destruction and can present a barrier to effective information sharing both within an agency and between agencies. This was not an issue when the Act was enacted and applied only to ASIO and the AFP, but with more agencies now defined as interception agencies and the national and transnational nature of many contemporary security and law enforcement investigations, effective co-operation within and between agencies is critical.

Simplifying the current information sharing provisions would support co-operative arrangements between agencies and consideration could be given to the ways in which information sharing amongst agencies could be facilitated.<sup>65</sup>

- 2.80 The NSW Police argued that the prescriptive approach inhibits interagency cooperation and impedes agencies' abilities to cooperate effectively:

Further, the access to and the subsequent use of information is framed throughout the *Telecommunications (Interception and Access) Act 1979* as one agency undertaking one investigation which will lead to a prosecution. I think that the act needs to be reformed to reflect new operational realities, including the different functions of agencies within the act and the fact that effective information sharing is a key component of successful investigations. The current information-sharing and dissemination scheme contained in the act is complex, confusing and cumbersome. The current provisions were not designed with joint agency operations in

---

64 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 8-9.

65 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 25.



mind and are considered to be overly restrictive, with the default position being to prohibit communication of information that has been obtained lawfully.

Whilst acknowledging privacy concerns – and we do acknowledge privacy concerns and the intrusive nature of telephone interception – a simplified, more permissive information-sharing communication model really does need to be adopted. If agencies are going to be encouraged and properly equipped to perform their functions and to cooperate effectively, then we need to be allowed to disseminate, communicate or share information where there is a legitimate reason to do so. Naturally, appropriate oversight and safeguards need to be and must be incorporated in such a scheme. But, overall, it is the agencies that readily use this legislation that I think are best placed to assist in its reform and the New South Wales Police Force is in an excellent position to provide further input from an operational perspective.<sup>66</sup>

2.81 The NSW Police supported the argument for reform with the following examples of current operational impediments:

As an example, if we were tapping a telephone and, as a result of some information which came across that phone, we had concerns that someone was carrying a firearm on the street but we were not in a position to take any action, we cannot post that intelligence on a warning system for our officers. We would like to be able to put out a warning saying, 'If you pull this vehicle over with that person driving, be careful – intelligence suggests that they are armed.'

Another example might be where we have an interception operation running and, as a result of that, we come across some information about a child abuse situation. In that setting, we are not at liberty even to advise a child protection authority that there is a telephone interception running. That is because we are not able to use that lawfully intercepted information. That is difficult. We encounter that every day.<sup>67</sup>

2.82 Victoria Police submitted the current TIA Act regime is too restrictive, and inhibits community protection:

While it is important that there are strict controls over the sharing of information, Victoria Police investigators have on occasion found the legislation to be too restrictive. There have been instances where lawfully intercepted information would be of high importance to other organisations providing a function in the service of the community, but

---

66 Commissioner Andrew Scipione, *Transcript*, 26 September 2012, pp. 17-18. See also Western Australia Police, *Submission No. 156*, p. 6.

67 Commissioner Andrew Scipione, *Transcript*, 26 September 2012, p. 25.

Victoria Police is legislatively prevented from providing it. For example, if an interception identifies that a child is at risk of harm from its parents, this information cannot be communicated to child protection agencies. Similarly, where investigators identify the inappropriate dealings of a prison officer, this information cannot be passed on to prison authorities.<sup>68</sup>

- 2.83 A number of submissions noted in-principle support for streamlined information sharing provisions, citing the need for effective collaboration between law enforcement and national security agencies. That support, however, was subject to concerns that simplified information sharing provisions should not intrude upon privacy to any extent greater than is necessary for the purpose of the investigation. The Liberty Victoria submission is illustrative in this regard:

Liberty Victoria acknowledges that there is an increasing need for agencies defined as 'interception agencies' – including those responsible for national and transnational security and law enforcement investigations – to share information with one another. The nature of transnational security concerns means that agencies other than ASIO and the Australian Federal Police (AFP) are involved in investigations which impact the security of Australia, as well as Australian citizens within Australia and abroad.

However, as noted above in relation to standardisation of the tests and thresholds relating to warrants, detailed information-sharing provisions may reflect a desire to appropriately balance the right to privacy against security considerations. Careful consideration will therefore need to be given about whether the complexity of information-sharing provisions is justified. In Liberty Victoria's view, any broadening of scope to allow additional information-sharing between agencies should be taken seriously and with the upmost concern for privacy. Again, while Liberty Victoria recognises the need to facilitate information-sharing between agencies in some cases, there is insufficient detail in the Discussion Paper for stakeholders to comment in detail.<sup>69</sup>

- 2.84 Similarly, Ms Stella Gray expressed concern that streamlined information sharing did not become unregulated information centralisation:

It is fair and reasonable to assume that if an agency obtains evidence of a crime that is outside their jurisdiction to pursue, they should be able share that evidence with the relevant agency. However, they should only share the evidence relevant to the crime in question. If agencies were allowed to share the entirety of communications intercepted under the original warrant, this would be a clear case of overreach, and has severe

---

68 Victoria Police, *Submission No. 200*, p. 11. See also Western Australia Police, *Submission No. 203*, p. 9.

69 Liberty Victoria, *Submission No. 143*, pp. 8-9.

implications for citizens' privacy. It is crucial that all information gathered from warrants remains stored separately as a privacy safeguard. If this aspect of information sharing is not treated with precision, there will be a temptation to create a central database accessible by all agencies, which is a security and privacy risk in itself.<sup>70</sup>

- 2.85 Mr Bernard Keane submitted that the case for simplified information sharing had not been made:

The argument that information should be more easily shared between agencies is a glib one, and the only justification advanced in the paper is that 'effective co-operation within and between agencies is critical.' This of course is assertion rather than argument; no effort is made by AGD to explain what failings are currently occurring because of the legislative restraints on his intercepted data can be shared.

...

AGD has offered no justification for violating the long-standing philosophy that intercepted information should only be used for the purposes for which it was collected, rather than becoming a common treasure trove to be dipped into by all law enforcement and intelligence agencies at will.<sup>71</sup>

- 2.86 The Pirate Party Australia expressed support for enhanced reporting, but did not support a reduction in accountability:

We support security agencies providing more relevant information about the proportionality of any use of their invasive powers, while opposing any streamlining that reduces the ability of investigative bodies to uncover corruption or abuse of power.<sup>72</sup>

- 2.87 The AFP submission included several case studies to illustrate that the current prescriptive information sharing provisions impede operational collaboration. The AFP stated:

The complex and evolving nature of transnational crime means that no one agency can effectively conduct complex investigations. Collaboration is an essential element in achieving operational goals. The TIA Act as it currently stands impedes the effective exchange of lawfully obtained communications information and reduces the efficiency of operational partnerships. Simplified, principle based use and disclosure rules would be more consistent with the modern approach to cooperation between

---

70 Ms Stella Gray, *Submission No. 152*, p. 7.

71 Mr Bernard Keane, *Submission No. 117*, p. 4.

72 Pirate Party Australia, *Submission No. 134*, p. 13.

agencies and assist in assuring information obtained under lawful interception is maximised appropriately to serve the public good.<sup>73</sup>

- 2.88 The Office of the Australian Information Commissioner acknowledged the necessity of information sharing to effective investigative collaboration, but noted the need to ensure clarity of obligations and standards regarding the protection of the privacy of personal information due to fragmented information handling obligations:

[t]he OAIC considers that this fragmentation makes it particularly important that each of the applicable regulatory frameworks setting out information sharing arrangements between law enforcement and intelligence agencies clearly and consistently specifies the nature, scope and limits of the information sharing activities. This includes specifying what protections are afforded to any personal information collected, used or disclosed under the information sharing arrangement.<sup>74</sup>

- 2.89 Mr Newton noted general support for information sharing simplification, but not if it resulted in a net reduction in privacy protections:

In particular, I would not support a sharing regime which enabled an agency which had obtained evidence for a certain purpose to divulge it to a second agency for a different purpose, if that second agency would otherwise be required to obtain their own warrant.<sup>75</sup>

- 2.90 The Law Council of Australia submitted it is appropriate that information obtained under the TIA Act is subject to more rigorous legislative protections than other forms of information in a law enforcement agency's possession:

Sharing this type of information must necessarily be more restricted than sharing other information in order to recognise its particularly sensitive nature and the intrusive impact on a person's rights and privacy. It could include, for example, details of a person's most private conversations or the precise location of a person, and may include information in relation to non-suspects or other innocent third parties. Provisions relating to the sharing of this type of information must also reflect limits on the types of officers who are able to have primary access to this information.<sup>76</sup>

- 2.91 Rather than simplification to enable greater interagency information sharing, the Law Council suggested reforms should look at 'strengthening and clarifying the existing provisions, recognising that different restrictions on communication, use and disclosure may be appropriate in light of the nature of the information

---

73 Australian Federal Police, *Submission No. 163*, p. 10. See also: Australian Customs and Border Protection Service, *Submission No. 168*, p. 3.

74 Office of the Australian Information Commissioner, *Submission No. 183*, pp. 10-11.

75 Mr Mark Newton, *Submission No. 87*, p. 7.

76 Law Council of Australia, *Submission No. 96*, p. 46.

obtained, and depending on what types of agencies are able to have primary access to such information.’<sup>77</sup>

- 2.92 The Committee supports the need to ensure that any amendments to the information sharing provisions provide appropriate privacy protections. The Committee understands, however, one of the potential benefits of proposed information sharing reforms is to enable investigative agencies to provide intercepted information to an agency that is responsible for investigating particular criminal activity.
- 2.93 The Committee supports the view that information sharing provisions should continue to impose appropriate restrictions upon the use and disclosure of telecommunications interception information, having regard to its privacy intrusive nature. The Committee also supports the need for law enforcement and security agencies to be able to share information to ensure that serious crimes and threats to national security can be investigated in a timely and thorough manner.
- 2.94 The Committee is concerned about the proliferation of institutions that gather and share information, and the absence of consistent guidelines and sufficient oversight.

## 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.**

## Removing legislative duplication

- 2.95 The discussion paper notes that legislative complexity has been created by frequent amendments to the TIA Act:

The pace of change in the last decade has meant the Act has required frequent amendment resulting in duplication and complexity that makes

---

<sup>77</sup> Law Council of Australia, *Submission No. 96*, p. 47.

the Act difficult to navigate and which creates the risk that the law will not be applied as Parliament intended.<sup>78</sup>

- 2.96 The Attorney-General's Department was asked on notice to provide examples of legislative duplication. The Department noted that it considers that the multiple types of warrants are no longer appropriate for the modern communications landscape:

Key areas of duplication relate to the different types of warrants, including the distinction made between intercepted and stored communications.<sup>79</sup>

- 2.97 The Department observed that the duplicated nature of warrants leads to other forms of unnecessary legislative duplication:

The oversight, record keeping and reporting provisions which flow from these warrant provisions are also duplicative. For example, in relation to oversight responsibilities, there is dual oversight of State and Territory agencies by both the Commonwealth Ombudsman and the relevant State or Territory oversight agency.

In relation to record keeping and reporting, there are three separate annual report requirements for telecommunications interception warrants, stored communication warrants and access to telecommunications data. In the case of interception warrants there are separate annual report requirements for Commonwealth agencies and State prescribed authorities, there are also two separate reporting requirements for State agencies. The three requirements differ making it difficult to undertake a meaningful analysis and comparison of the different mechanisms.<sup>80</sup>

- 2.98 The Department presented the overall view that:

...streamlining and modernising lawful access to telecommunications provisions through the creation of a one warrant regime that regulates access to the content of a communication, together with the flow on effects to the oversight, record keeping and reporting requirements, will remove significant duplication and complexity from the TIA Act and create consistency in the accountability framework.<sup>81</sup>

- 2.99 The Committee is of the view that removing legislative duplication would help to make the interception regime easier for the general public, legal practitioners, law enforcement and the justice system to understand and apply.
- 

78 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 17

79 Attorney-General's Department, *Submission No. 236*, p. 18.

80 Attorney-General's Department, *Submission No. 236*, p. 18.

81 Attorney-General's Department, *Submission No. 236*, p. 18.

## Recommendation 9

**The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.**

### A single warrant with multiple telecommunications interception powers

2.100 The AGD submission states:

The Department considers that the interception regime would offer greater privacy protection if the distinction between stored and live warrants was removed and if a standard threshold for both content and stored communications warrants was introduced. Reliance on the higher seven year penalty threshold has not proved successful in limiting the application of interception powers. On the other hand the three year stored communications threshold underestimates the value of non-voice communications in the contemporary communications environment. A threshold in between these two would recognise the growing importance of non-voice communications and enable interception to be used as a tool in investigating a number of serious crimes that currently fall outside the TIA Act.

A single warrant, and clarification of the concept of serious offence, would greatly enhance the capacity of the interception regime to ensure that interception is only available in defined circumstances.<sup>82</sup>

2.101 Victoria Police supported the proposal for a single warrant, noting in its submission:

It is no longer practicable for warrants to be obtained solely on traditional network identifiers such as telephone numbers or International Mobile Equipment Identifier (IMEI) numbers. A single warrant in which particular identifier(s) could be stipulated (such as a username, webmail address, internet account) would enable the targeting of communications of a suspect without the need for multiple warrants over time on the same target.<sup>83</sup>

2.102 Similarly, the Western Australia Police expressed support for the efficiency and flexibility a single warrant regime would represent:

---

<sup>82</sup> Attorney-General's Department, *Submission No. 218*, p. 5.

<sup>83</sup> Victoria Police, *Submission No. 200*, p. 13.

The creation of a single warrant with multiple TI powers would provide the flexibility to cater for future technological change by having a focus on communications made by an individual rather than the specific technology or equipment used.

WA Police is of the view that the use of a single broad based warrant would simplify an otherwise overly complicated regime. At present, the TIA Act provides for 6 different warrants (service warrant, b-party interception warrant, named person warrant, device based interception warrant, section 48 entry onto premises warrant, stored communications warrant), each of which have specific applicability. The application of the current warrant regime has the potential to cause confusion as police officers are often unsure about which warrant best suits the needs of a particular investigation.<sup>84</sup>

- 2.103 The Australian Mobile Telecommunications Association – Communications Alliance joint submission noted reservation with the proposal for a single warrant due to the potential for it to shift obligations and due diligence checks onto telecommunications providers:

A telecommunications service provider must be able to clearly determine from the warrant which services should be intercepted in order to properly implement a warrant. For these same reasons the responsibility to identify relevant services should rest with the intercepting agency and not the service provider. Industry also expects that there will be a continuing need for independent oversight of warrant applications prior to them being served on a carrier or carriage service provider. It would not be possible for the oversight process to fully assess the impact of each warrant if the carrier or service provider is subsequently required to make the decisions about what particular services are to be intercepted.<sup>85</sup>

- 2.104 Similarly, iiNet noted the need for warrants to avoid shifting questions of judgement to telecommunications providers:

The Discussion Paper does not specify what the particular 'TI powers' will be (i.e. whether a consolidation of existing powers is intended or the addition of new powers). iiNet believes that it is important that it be recognised that C/CSPs are not State agents, and a clear demarcation should be maintained between CSPs providing access and C/CSPs doing more than providing access. Furthermore, C/CSPs should not be required to make any judgement calls as regards what particular information is

---

84 Western Australia Police, *Submission No. 203*, p. 11.

85 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 10.



required for a C/CSP to comply with a warrant. Therefore, warrants should contain clear and specific terms.<sup>86</sup>

- 2.105 Interception agencies explained to the Committee, however, that the proposal for a single telecommunications interception warrant would significantly increase administrative efficiency without diminishing accountability:

The current TIA Act requires various types of warrants to access communications lawfully. Additional types of warrants have been created over the years in response to changes in methodologies and technologies. The resultant system is complex requiring detail to be interpreted by agencies, issuing authorities, oversight bodies, and courts. The Commission supports the concept of a single simplified warrant. The relevant thresholds and privacy intrusions are essentially the same where communications are accessed via service device be they stored communications or intercepted in transit.<sup>87</sup>

- 2.106 A number of submissions expressed cautious support for the proposed single warrant, noting the potential for efficiencies within the warrant process, but noted concern at the potential for the proposal to diminish thresholds. The Pirate Party submission is an example of this position:

If this single warrant retains a threshold test for serious crimes (with a penalty of 7 years or greater imprisonment) then there should be no obstacle in implementing it. If, however, the threshold is lower than that then there would be grave concerns in allowing it.<sup>88</sup>

- 2.107 The Tasmanian Association of Community Legal Centres expressed concern the proposal would lead interception agencies to using available powers, rather than the most appropriate power:

In our view the current legislative requirement that law enforcement agencies apply for either a 'telecommunications service' warrant (authorising the interception of only one service, such as a single telephone number) or a 'named person' warrant (authorising the interception of any telecommunication services or devices that are likely to be used by the person named in the warrant) reduces the risk that law enforcement agencies will use all the powers available to them rather than being used for a specific purpose as currently provided in the powers of the two warrants.<sup>89</sup>

- 2.108 The issue of the thresholds and how to deliver the appropriate accountability was usefully addressed by the Inspector-General of Intelligence and Security:
- 

86 iiNet, *Submission No. 108*, p. 10.

87 Western Australia Corruption and Crime Commission, *Submission 156*, p. 8.

88 Pirate Party, *Submission No. 134*, p. 15.

89 Tasmanian Association of Community Legal Centres, *Submission No. 184*, pp. 2-3.

Having multiple sets of warrant applications for a single investigation is administratively inconvenient for ASIO and does not necessarily provide the Attorney-General with a clear view of the totality of proposed activities. Any proposal to streamline this and give the Attorney-General a better picture of the situation is worthy of consideration but issues of proportionality and levels of authorisation will need careful consideration.

...

One interpretation of the proposal in the discussion paper could be that the Attorney-General is to be asked only to agree broadly to 'interception' against a particular individual, group or premises for a specified period and to then allow the Director-General of Security or a delegated ASIO officer to decide what form that interception should take during the warrant period (including whether B-Party interception is appropriate). I note that a 'named person warrant' currently allows the Director-General of Security to add or remove services from interception coverage during the life of the warrant to enable interception of communications made by or to the specified individual. Any proposal to effectively further transfer the level of decision making from Ministerial level to within an agency needs to ensure that appropriate reviews take place within the agency, make allowance for independent scrutiny and consider external reporting requirements.<sup>90</sup>

- 2.109 Similarly, the Gilbert + Tobin Centre for Public Law noted the need to ensure that a regime for a single telecommunications interception warrant should continue to ensure proportionality is considered by the issuing authority:

The most recent report of the Attorney-General's Department into the operation of the TIA Act states that a named person warrant has a 'high impact on privacy'. It should only be used 'when necessary and other alternative methods are not available'. Therefore, in the majority of cases, law enforcement agencies obtain a telecommunications service warrant rather than a named person warrant. This is the correct approach. Any intrusions into the right to privacy should be the minimum required to achieve the public purpose. We are concerned that merging of named person warrants and telecommunications service warrants into a single category of warrant would result in law enforcement agencies using all the powers that are available to them (regardless of whether these powers are strictly necessary to investigate the criminal activity).<sup>91</sup>

---

90 Inspector-General of Intelligence and Security, *Submission No. 185*, pp. 9, 10.

91 Gilbert + Tobin Centre for Public Law, *Submission No. 36*, p. 9.

2.110 The Law Council of Australia also noted reservations about the proposal's potential to diminish accountability, particularly in the absence of detail within the Attorney-General's Department Discussion Paper. The Law Council helpfully indicated some of the considerations which could be addressed if the reform were to be supported:

However, if a proposal of this nature were pursued, the Law Council would suggest that the issuing authority must be satisfied of the following minimum requirements:

- that any person whose telecommunications are to be intercepted is specifically identified as a legitimate target of suspicion from a security or law enforcement perspective;
- that each and every telecommunications service or telecommunications device to be intercepted is, in fact, used or likely to be used by the relevant person of interest; and
- each and every telecommunications service or telecommunications device to be intercepted can be uniquely identified such that relevant telecommunications made using that service or device can be isolated and intercepted with precision.

In addition, the issuing officer should also have regard to:

- the likely benefit to the investigation which would result from the intercepted information substantially outweighing the extent to which the interception is likely to interfere with the privacy of any person or persons;
- the gravity of the conduct constituting the offence or offences being investigated;
- how much the information referred to would be likely to assist in connection with the investigation by the agency of the offence or offences; and
- to what extent methods of investigating the offence or offences that do not involve intercepting communications have been used by, or are available to, the agency<sup>92</sup>.

2.111 The Committee acknowledges the need to ensure that intrusive investigative techniques are exercised only in necessary and justified circumstances, and that the intrusion is proportionate to the conduct being investigated. A balance must be struck between appropriate checks and balances, and the operational flexibility required to deliver effective law enforcement and protection against national security threats.

2.112 The Committee is of the view that revising the present multiple telecommunications interception warrants into a single warrant regime can deliver administrative efficiencies to interception agencies without removing

---

<sup>92</sup> Law Council of Australia, *Submission No. 96*, p. 53.

appropriate accountability and safeguards.

## **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.

## **Modernising the cost sharing framework**

- 2.113 The final area for potential legislative reform identified by the AGD discussion paper relates to modernising the cost-sharing framework. The discussion paper provided by the AGD proposes that cost sharing frameworks be modernised by aligning 'industry interception assistance with industry regulatory policy' and by

clarifying the role of the Australian Communications and Media Authority's role in regulation and enforcement.<sup>93</sup>

## Align industry interception assistance with industry regulatory policy

2.114 The terms of reference to this inquiry state the Government wishes to progress the modernisation of the cost-sharing framework to align industry interception assistance with industry regulatory policy. The industry assistance obligations are contained in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and in the *Telecommunication Act 1997*. The discussion paper explains:

In reforming cost sharing, consideration must also be given to the current make-up of the telecommunications industry. The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers.

A tiered model would also recognise that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant and less capacity to store and retain information about communications and customers.<sup>94</sup>

2.115 The Department explained that the current cost responsibility principles for the maintenance of effective were established following the 1994 review into the *Long term Cost-effectiveness of Telecommunications Interception* by Mr Pat Barrett.<sup>95</sup> The Department also gave an example of a more flexible approach to applying obligations to the contemporary telecommunications environment:

The requirement for all industry participants to have the same interception capability can also be an expensive and unnecessary burden that can act as a barrier to entry to the telecommunications market for new industry players. Therefore, requiring all service providers to have the same interception capability regardless of size (as in the current system) could have the effect of restricting competition rather than promoting it and stifling innovation (noting that the promotion of the

---

93 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 13.

94 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 28.

95 Attorney-General's Department, *Submission No. 236*, p. 19.

supply of diverse and innovative carriage services and content services is one of the objects of the Telecommunications Act).<sup>96</sup>

2.116 The Department concluded:

The current industry and legislative cost allocation framework is working well, but efficiencies may be able to be made in regards to standardisation of technical and administrative requirements in meeting these obligations. Opportunities for reducing red tape and achieving regulatory offsets may also be identified.<sup>97</sup>

2.117 The Committee appreciates that the telecommunications environment has evolved rapidly and is significantly different in size, composition and international presence to the industry that existed when the TIA Act was first passed.

2.118 Therefore, the Committee agrees that there is merit in reconsidering application of the cost-sharing provisions of the telecommunications interception regime to provide a more flexible approach.

## 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*.**

## Clarify ACMA's regulatory and enforcement role

2.119 The Australian Communications and Media Authority (the ACMA) has the following functions and responsibilities:

The Australian Communications and Media Authority (ACMA) is a government agency responsible for the regulation of broadcasting, the internet, radiocommunications and telecommunications.

The ACMA's responsibilities include:

- promoting self-regulation and competition in the communications industry, while protecting consumers and other users
- fostering an environment in which electronic media respect community standards and respond to audience and user needs
- managing access to the radiofrequency spectrum

<sup>96</sup> Attorney-General's Department, *Submission No. 236*, p. 19.

<sup>97</sup> Attorney-General's Department, *Submission No. 236*, p. 19.

- representing Australia 's communications interests internationally.<sup>98</sup>

2.120 The AGD discussion paper suggested that the enforcement mechanisms available to the ACMA in relation to telecommunications interception regulation should be expanded:

Consideration should also be given to clarifying the role of the Australian Communications and Media Authority (ACMA) in regulating industry obligations under the interception regime. The ACMA has rarely used its powers to enforce compliance with the TIA Act because the only effective power available to it under the Act is court action. Court action is usually inappropriate or excessive in the circumstances and unhelpful from an agency perspective because it may publicly disclose that a particular C/CSP is not complying with its TIA Act obligations. The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply.<sup>99</sup>

2.121 Telstra expressed support for clarifying the ACMA's enforcement role, also noting the need to ensure appropriate consideration is given to education and dispute resolution roles:

Telstra believes there needs to be clarification as to what role ACMA will have in future in monitoring compliance by C/CSPs with the Telco Act and TIA Act in respect to national security and law enforcement.

The Discussion Paper does not suggest what types of additional powers may be contemplated. Telstra would recommend that whatever agency is given this enforcement role its primary focus should be on undertaking an active role in education and dispute resolution, with any penalty enforcement role being secondary.<sup>100</sup>

2.122 Mr Ian Quick expressed opposition to the proposal due to the potential loss of transparency:

A significant advantage of the current ACMA's power – going to court– is that it is public and open to scrutiny. If, as the discussion paper suggests –

'The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply.'

it would be possible – though the paper does not say what the 'options' are – that the ACMA could quietly push a C/CSP into doing something it

---

98 Australian Communications and Media Authority website, <[www.acma.gov.au](http://www.acma.gov.au)>, viewed 7 June 2013.

99 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 28.

100 Telstra, *Submission No. 189*, p. 7

did not want to do. While this may be alleviated by clear standards, any option it has should be open to public scrutiny.<sup>101</sup>

- 2.123 The Committee did not receive a submission from the ACMA but notes the suggestion from Mr Bernard Keane to review the 2005 report *Reform of the broadcasting regulator's enforcement powers* prepared for ACMA by Professor Ian Ramsay. As Mr Keane noted:

*Reform of the broadcasting regulator's enforcement powers* is a valuable analysis of regulatory theory that should provide the basis for an effective regulator's suite of tools for achieving effective industry regulation. ... In particular, it addressed the issue of a lack of 'mid-tier' powers, which is a similar issue to that raised by AGD in the paper in relation to powers to enforce compliance with the TIA Act. On this issue, a power to accept enforceable undertakings, and a power to issue infringement notices, would appear to be two mid-tier powers worth considering to enable ACMA to enforce compliance without resorting to litigation.<sup>102</sup>

- 2.124 The Committee notes that an effective enforcement and compliance regime requires a range of sanctions and tools which are tailored to a range of potential conduct.

## 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.**

## Requirements for industry interception obligations

- 2.125 The AGD discussion paper outlines the current situation regarding the expression of industry interception obligations:

The TIA Act places an obligation on each C/CSP to have the capability to intercept communications and requires carriers and nominated carriage service providers to submit an annual interception capability plan outlining their strategy for complying with their obligation to intercept and to deliver communications to interception agencies. The obligation extends to maintaining the capability to intercept communications that

101 Mr Ian Quick, *Submission No. 95*, p. 7.

102 Mr Bernard Keane, *Submission No. 117*, p. 5.



are carried by a service that they provide and to deliver those communications to the requesting agency consistent with a warrant.

However, as networks have become more complicated and the types of services available have expanded, often beyond the C/CSPs' own networks, challenges have evolved in applying a general obligation. Consideration should be given towards introducing measures that implement more specific technical requirements to cater for a diverse and sophisticated telecommunications environment. This includes developing requirements around administrative needs such as the timeliness of cost sharing to agencies and the security measures to be applied to the handling of sensitive information relating to interception operations.<sup>103</sup>

2.126 The Australian Mobile Telecommunications Association – Communications Alliance supported a 'high level set of requirements for industry interception obligations to be clear, straightforward and reasonable.'<sup>104</sup>

2.127 iiNet submitted that it was unclear what was proposed, but that some clarification is necessary:

This proposed reform appears to iiNet to be capable of being very broad. It is not expressly discussed in any detail in the Discussion Paper. Without detail of what this reform would involve, it is difficult for iiNet to provide any meaningful comment, except to say that there should be thorough consultation with industry on these detailed requirements. iiNet believes that consideration of any such reform should include giving consideration to clarifying the scope of section 313 of the Telco Act. The scope of the obligation to 'give such help as is reasonably necessary' is vague and uncertain.<sup>105</sup>

2.128 The Western Australia Corruption and Crime Commission expressed support for the potential benefits to be derived from clearly articulated obligations:

The current regulatory regime for industry interception obligations is administratively burdensome for both industry participants and the regulatory agency. The current requirement of industry to prepare and submit interception capability plans which are then assessed annually should be reviewed.

The implementation of detailed requirements for industry interception obligations may assist in clarifying requirements and account for technical

---

103 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 27.

104 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 10.

105 iiNet, *Submission No. 108*, pp. 10-11.

complexities. The Commission endorses the inclusion of administrative requirements as part of industry interception requirements. In many cases, difficulties or delays in interception are due to administrative, as opposed to, technical limitations.<sup>106</sup>

- 2.129 The Committee notes that while, in general, a cooperative relationship exists between telecommunication companies and law enforcement and national security agencies, a uniform level of cooperation does not exist across all sectors of the industry. The Committee sees benefit in providing detailed guidance on the obligations imposed on the telecommunications industry to ensure telecommunications providers and interception agencies alike understand the extent of those obligations.

### 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.**

### Clarify that the interception regime includes ancillary service providers

- 2.130 Although expressed as 'extending' the interception regime to ancillary service providers such as Facebook, Google and Twitter, the purpose of this term of reference is in fact to clarify that – as the Committee understands to be the case – the existing obligations do apply to ancillary service providers. It is not an extension of existing obligations.
- 2.131 Although he does not refer to ancillary service providers by name, Commissioner Scipione of the NSW Police Service described the challenges to national security services and the law enforcement community posed by technological change:

A further significant challenge for law enforcement agencies investigating national security and serious criminal matters is the increasing use of sophisticated technologies by criminals. Frankly, organised criminals are now able to operate outside the reach of ordinary telecommunications interception and law enforcement agencies that are dealing with criminals who have access to unprecedented advancements in technology. Legislation that not

106 Western Australia Corruption and Crime Commission, *Submission No. 156*, p. 8.

only fails to adequately recognise this but significantly fails to future proof itself against rapidly emerging technologies is what we are dealing with here.<sup>107</sup>

- 2.132 The rationale for clarifying the regulatory obligations of ancillary service providers under the TIA Act was stated by the Western Australia Police:

When communication systems were conducted over telephone networks only, as was the case when the TIA Act was written, there was no question as to who was responsible for supplying the interception points. It is no longer simply the case of going to just one telecommunications provider to intercept a persons' communications. It is now quite feasible for someone to be subscribed to one provider for their telephone traffic and another provider for their Internet. Further, other providers might provide a Voice Over IP (VOIP) telephone service which then utilises a network, or multiple networks of multiple providers to get from point a to point b.

Intercepting an individual's communications is no longer a simple exercise of only going to the major identified service providers. Regardless of the provider, it should be possible to intercept related Internet traffic for the purposes of investigating serious criminal activities.<sup>108</sup>

- 2.133 Victoria Police also submitted that the fact that the existing regime applied to ancillary service providers should be made clear beyond doubt:

Monitoring of intercepted communications by Victoria Police routinely demonstrates that services such as these are being used by suspects in furtherance of their criminal activities. Without a mandatory regulatory obligation placed on the providers of these services used in Australia, criminals can continue to communicate without the risk of being exposed to interception. There needs to be legislative parity with the obligations applicable to Australian service providers.<sup>109</sup>

- 2.134 The Committee notes that the TIA Act facilitates interception and access to telecommunications data by law enforcement and national security agencies. The TIA Act facilitates this by relying upon the cooperation and assistance provided by telecommunications providers. The TIA Act does not distinguish between telecommunications providers, but provides a universal telecommunications interception obligation on all providers of telecommunications services.

---

107 Commissioner Scipione, *Transcript*, 26 September 2012, p. 18.

108 Western Australia Police, *Submission No. 203*, pp. 11-12.

109 Victoria Police, *Submission No. 200*, p. 14

- 2.135 Although the terms of reference requests the Committee to consider whether the existing TIA Act should 'extend' to ancillary service providers the Committee believes that the TIA Act does, under its existing provisions, include ancillary service providers. The use of the term 'extend' is inapt. The Committee received no evidence on behalf of ancillary service providers which disputed that the TIA Act applied to them. It is not an extension of existing obligations.

#### 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.**

### Industry participation model

- 2.136 The AGD discussion paper suggests the Committee should consider the merits of a tiered regime for industry assistance to intercept communications and facilitate access to telecommunications data:

In reforming cost sharing, consideration must also be given to the current make-up of the telecommunications industry. The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers.

A tiered model would also recognise that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant and less capacity to store and retain information about communications and customers. Requirements on industry to retain current information and to assist agencies to decrypt information would greatly enhance agencies' abilities to detect and disrupt criminal and other behaviours that threaten national wellbeing

but should be implemented in a way that does not compromise business viability.<sup>110</sup>

2.137 Ms Stella Gray queried the efficacy of a tiered regime for industry assistance:

A tiered interception-compliance model may simply encourage people to flock to smaller CSPs to evade surveillance, thereby negating the structure of this model.<sup>111</sup>

2.138 iiNet expressed in-principle support for a tiered industry assistance model, noting that it reflected industry practice:

iiNet agrees with the comments in the Discussion Paper that a tiered model would more accurately reflect industry practice. However, iiNet believes that it is appropriate to distinguish between:

- the legal obligation to provide interception capability; and
- the manner in which that obligation is complied with by a particular C/CSP.

iiNet believes that the obligation to provide interception capability should apply uniformly to all C/CSPs. However, iiNet believes that there should be flexibility as regards the manner in which a particular C/CSP complies with the obligation to provide interception capability, and the size and resources of the C/CSP should be a relevant consideration in the assessment of that C/CSP's interception capability plan.<sup>112</sup>

2.139 The Australian Mobile Telecommunications Association – Communications Alliance also expressed in-principle support for a tiered industry assistance model:

Industry favours a tiered participation model, where investment in interception capabilities is based on Agency need and risk, as opposed to the current blanket obligation which requires the deployment of interception capabilities that in some cases are unlikely to be used.<sup>113</sup>

...

The current blanket approach of the TIA Act potentially gives rise to replication of interception capabilities at the carrier, wholesale service provider, retail Broadband service provider and application service layer. A more efficient regulatory framework should be sought, where replication of interception capabilities is not required.<sup>114</sup>

---

110 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 28.

111 Ms Stella Gray, *Submission No. 152*, p. 6.

112 iiNet, *Submission No. 108*, p. 11

113 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 11.

114 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*,

- 2.140 In contrast, Telstra expressed significant reservations about the proposal for a tiered industry assistance model:

Telstra believes these proposals run the risk of creating an uneven playing field, where the compliance burden would rest disproportionately with larger C/CSPs and the effectiveness of the overall regime is undermined by allowing criminals or terrorists to avoid interception arrangements by acquiring services from smaller C/CSPs.

In relation to the interception cost sharing framework, the Discussion Paper indicates that a new tiered model may be introduced where larger C/CSPs are expected to have a comprehensive interception capability (presumably at a greater cost) while smaller C/CSPs may only be required to have a minimum level capability (presumably at a lower cost). While the Discussion Paper states that one of its aims is to maintain 'competitive neutrality' in the industry, it is hard to see how tiered compliance obligations are consistent with this aim. As such, Telstra does not support this proposal.<sup>115</sup>

- 2.141 In testimony before the Committee, Telstra expanded upon these concerns:

Essentially what we are saying is that it should be a uniform application of obligations. Given the nature of their targets, law enforcement and national security schemes are only as strong as their weakest link. On an uneven playing field criminals and terrorists will inevitably locate their operations where security obligations are the lowest, leaving larger telecommunication operators to incur the costs of greater obligations for no offset in law enforcement or national security gain.<sup>116</sup>

- 2.142 Mr Mark Newton also opposed the proposal, submitting that a tiered model already applied by informal means:

This proposal is unnecessary, on the grounds that we have it by fiat already. Current industry interception obligations are consultative, and the Attorney-General's Department doesn't bother to consult with providers that this proposal would envisage as 'tier 3.' I believe considering this proposal is a waste of time, and I don't support it.<sup>117</sup>

- 2.143 The Committee understands the proposal to be that all telecommunications providers would remain subject to an obligation to provide assistance to law enforcement and security agencies, but the manner in which telecommunications interception obligations would be discharged would vary according to the risk profile of the telecommunications provider. As such, the Committee is assured

---

p. 12.

115 Telstra, *Submission No. 189*, p. 9.

116 Mr James Shaw, *Transcript*, 27 September 2012, p. 2.

117 Mr Mark Newton, *Submission No. 87*, p. 9.

that lower tier telecommunications providers will still maintain interception capability.

- 2.144 The committee does not favour a tiered approach. However it acknowledges that there may be situations related to practicability and affordability where exceptions for particular industry players are justifiable. However it is for those who seek exemption from the uniform obligation to demonstrate why they should be excused.

### 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.**

## An offence for failure to assist in the decryption of communications

- 2.145 The AGD submission explains the rationale and scope of the decryption assistance proposal:

Encryption is becoming widespread in information and communications technology. Criminals and terrorists are increasingly using encryption to avoid detection, investigation and prosecution causing difficulties for agencies to access clear, intelligible communications in their operations.

Encryption can be difficult to manage. It may not always be the case that a person who uses or creates encryption is able to provide assistance with decryption. Often an applications provider, organisation or individual provides encryption services, rather than a carrier. Criminal organisations and terrorists can obtain these services or even create and use their own encryption solutions.

Section 3LA of the *Crimes Act 1914* (the Crimes Act) sets out provisions concerning decryption regarding information obtained under search warrants; however this does not extend to communications intercepted pursuant to a warrant under the TIA Act.

In summary, section 3LA of the Crimes Act allows a police officer to apply to a magistrate for a warrant to require a person to provide in accessible form (i.e. in decrypted form) data held on a computer or data storage device, where the computer or data storage device had been seized under a warrant. A warrant may be applied to the person under

investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator. There is a penalty of up to two years imprisonment for failing to comply with an order.

A consistent approach to that contained in the Crimes Act would ensure that information lawfully accessed for national security or law enforcement purposes under the TIA Act was intelligible.<sup>118</sup>

- 2.146 The Committee received many submissions about the absence of clarity as to whom the proposed offences would apply to, and what type of decryption assistance is envisaged.

End users, wholesale service providers, broadband retail service providers and content providers could all potentially play a role in the encryption of communications. Where the provider is based offshore then the matter of jurisdiction also needs to be considered.

Any decryption requirement should also specify that the obligation is to make available, if it is available, the means for decryption, as opposed to the actual content/communications that is to be decrypted.

There must not be a presumption that a person or organisation is capable of decrypting communications. The imposition of sanctions or penalties must be based on proof that the person or organisation is capable of assisting with the decryption of communications and there is evidence they have refused to do so.<sup>119</sup>

- 2.147 The AFP confirmed in testimony to the Committee that the decryption assistance sought by law enforcement agencies is limited to encryption applied by telecommunications providers:

From our perspective, encryption is a terrific advancement for the Australian community. Because it helps protect people from those who would do them harm in scams and those sorts of things it is a very good thing. What we would be seeking as far as the uptake to the act goes is that, where we have a warrant to intercept particular information going to a particular service, that the service provider provide those encryption keys to us to allow us to undertake that interception under warrant – as I have said – rather than anything else. This is not about people's home encryption. This is about talking to service providers about their

---

118 Attorney-General's Department, *Submission No. 218*, pp. 6-7.

119 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 12. See also Mr James Sinnamon, *Submission No. 100*, p. 1; Privacy Victoria, *Submission No. 109*, p. 6; Mr Arved von Brasch, *Submission No. 126*, p. 3.



providing those encryption keys under warrant for us to then intercept a particular device which has been duly authorised.<sup>120</sup>

2.148 The AFP provided a case study in support of the proposal:

During an investigation into an online paedophile network, it was noted that targets deployed a multiplicity of encryption techniques. They sent messages using an encryption overlay; images were encrypted and ‘hidden’ within other images which were then sent via closed peer to peer networks which also used encryption. Advanced Encryption Standards applications were used on virtual machines (computers within computers). The combined effect meant persons of interest were able to browse the internet without leaving detectable forensic footprints for investigators.

Additional members of this network identified and pursued in a related operation took the anti-forensic techniques further and used full disk encryption along with hidden volumes that were disguised using a technique that allowed for plausible deniability of the content, effectively circumventing both interception and search warrant legislation. Persons of interest identified in the investigation included a computer antivirus developer, and a computer networking trainer; their technical expertise was such that they were able to develop and customise their own encryption protocols rather than relying on off the shelf products.<sup>121</sup>

2.149 The Queensland Crime and Misconduct Commission expressed support for the proposal noting the current investigative challenge which encryption presents:

The increased use of sophisticated encryption presents challenges to the CMC. Internet service providers (ISPs) as well as application service providers (ASPs) are increasingly providing end to end encryption. The fact that ASPs can be located anywhere in the world can make it extremely difficult to seek assistance in the decryption of content that may be vital in an investigation. TIA Act reform that envisages law enforcement agencies being able to request decryption assistance where possible from ISP’s, Carriers and ASPs, would potentially allow for greater access to critical evidence.<sup>122</sup>

2.150 A range of submissions raised the prospect that an offence for failing to provide decryption assistance would undermine confidentiality requirements. The Electronic Frontiers Australia submission was indicative:

---

120 Commissioner Tony Negus, *Transcript*, 26 September 2012, p. 28.

121 Australian Federal Police, *Submission No. 163*, pp. 14-15.

122 Queensland Crime and Misconduct Commission, *Submission No. 147*, p. 7. See also Western Australia Corruption and Crime Commission, *Submission No. 156*, p. 10; Victoria Police, *Submission No. 200*, p. 15, Western Australia Police, *Submission No. 203*, p. 13.

EFA is concerned about the possible creation of an offence for failing to assist in the decryption of communications for the following reasons:

- it undermines the right of individuals to not cooperate with an investigation
- it poses a threat to the independence of journalists and their sources, particularly in circumstances involving whistle-blowing activity related to cases of official corruption
- it could undermine the principles of doctor-patient and lawyer-client confidentiality and other trusted relationships
- there are foreseeable and entirely legitimate circumstances in which decryption of data is not possible, such as where a password has been forgotten and is unrecoverable.<sup>123</sup>

2.151 The Human Rights Law Centre submitted that decryption assistance could impose an obligation on suspects to provide a 'level of assistance to investigators [that] runs counter to the right to remain silent.'<sup>124</sup>

2.152 Mr Ian Quick objected to the proposal on a number of practical and theoretical grounds:

On the practical front, what would an agency do if someone said

- 'I can't remember the password'
- 'I've deleted whatever the password was that was used for that period, so cannot assist.'
- 'I didn't know it was encrypted, so have no idea what you are talking about.'
- 'It's not encrypted, it's just random junk (for whatever reason..)'
- 'The password I gave you doesn't work? The file/message must be corrupted,
- I can't help you.'

In addition, many communication protocols regularly used on the internet have session keys used for encryption, which are not recoverable by the end user.

What would the agency do? All the responses above might be legitimate, I have certainly experienced every one of them! How would you distinguish between someone who was truthfully saying it and someone who was lying? Surely it would be against the presumption of innocence to fine/jail people who failed to assist unless it could be proven that they could assist – and how could this be done? How would it be legislated?<sup>125</sup>

123 Electronic Frontiers Australia, *Submission No. 121*, p. 15

124 Human Rights Law Centre, *Submission No. 140*, p. 11. See also, Mr Breheny, *Transcript*, 5 September 2012, p. 45; Mr Bernard Keane, *Submission No. 117*, p. 12.

125 Mr Ian Quick, *Submission No. 95*, p. 13.

- 2.153 The Law Council of Australia gave in principle support for assisting agencies access communications once authorised, but queried whether an offence was the appropriate mechanism:

However, the Law Council also appreciates the need to ensure that officers who have been authorised to access communications can do so in an effective, meaningful way.

To this end, the Law Council does not oppose mechanisms to assist agencies to reconstruct or decrypt the content of communications to which access has been authorised.

It notes for example, that the Telecommunications Act already obliges carriers and carrier service providers to provide such help to agencies as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting public revenue and safeguarding national security.

However, it is not clear on the basis of the information provided in the Discussion Paper that the introduction of a criminal offence, presumably aimed at participants in the telecommunications industry such as carriers and carriage service providers, would be an effective or appropriate response, particularly when other non-punitive efforts may to be available to enhance cooperation between the agencies and the telecommunication industry.

Before introducing criminal liability for failing to assist in the decryption of communications, the Law Council suggests that the PJCIS requests that information be provided by the Attorney-General's Department that explains whether the proposed offence adheres to the principles contained in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.<sup>126</sup>

- 2.154 The Committee notes that, like the proposal for data retention, much of the discussion of the proposal for decryption assistance was confused by the lack of clarity on what is being proposed.
- 2.155 The Committee understands the proposal is for an offence to apply where a telecommunications provider does not provide assistance to decrypt communications where those communications have been encrypted by that telecommunications provider. This will of course only arise in circumstances where the relevant national security agency has established grounds where it is necessary to intercept and decrypt the communication. That being the understanding, many of the concerns raised by submitters about individuals being subject to the offence, or being forced to provide passwords, do not apply.

---

126 Law Council of Australia, *Submission No. 96*, p. 36.

- 2.156 The Committee notes encryption can impede access to telecommunications interception where access to the content of communications has been lawfully authorised.
- 2.157 The Committee acknowledges, however, that there remains a lack of specificity regarding the scope of the offence and the circumstances in which it may apply. In this context, the Committee appreciates the guidance provided by the Law Council of Australia in referring to the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.

### 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.**

### Institute industry response timelines

- 2.158 The Western Australia Police expressed support for the imposition of industry timelines for assistance sought from telecommunications providers:

It is important that telecommunication carriers are capable of dealing with urgent requests for communications data. This is particularly relevant when dealing with stored communications data. It is the practice of some carriers to purge such data after a short period of time. To ensure that evidence is not lost, carriers must have the capability of immediately responding to requests from law enforcement agencies to preserve the data, or alternatively they must have a reasonable ability to store data to until the completion of a police investigation.<sup>127</sup>

- 2.159 Optus expressed concern if the timeliness proposal was raised as more than a minimum standard:

Optus does not support mandated response times for warrants, unless it is calibrated as a backstop for extremely poor responsiveness. If the objective is to achieve an overall improvement in timeliness, then the

<sup>127</sup> Western Australia Police, *Submission No. 203*, p. 13. See also: Western Australia Corruption and Crime Commission, *Submission No. 156*, pp. 10-11.

focus should be on end-to-end process opportunities, taking into account both the agency activities and the carrier activities. The adoption of more effective and complete B2B electronic transaction processes for warrants by both agencies and carriers could drive substantial improvements in timeliness.<sup>128</sup>

- 2.160 In relation to requirements for timeliness however, the Australian Mobile Telecommunications Association and Communications Alliance considered the current regime enables the law enforcement and national security agencies to negotiate service levels for the supply of reasonably necessary assistance.<sup>129</sup>
- 2.161 Similarly, iiNet did not support the proposal, noting an absence of justification: iiNet submits that imposing specific industry timeframes is unnecessary. iiNet notes that there is no suggestion in the Discussion Paper that industry tardiness is in any way a cause of any of problems for law enforcement agencies.<sup>130</sup>
- 2.162 Telstra indicated a significant resource implication from the proposal: Telstra submits that for Government to mandate 'response timelines' would also require Government to spend significant funds to support the introduction of a fully automated request management system (as discussed in 8a) for use by LENSAs and C/CSPs otherwise the LENSAs would not obtain the benefits intended from this proposal.<sup>131</sup>
- 2.163 The Committee notes the need to ensure that telecommunications providers are able to provide timely assistance to law enforcement and national security investigations. The evidence presented to the Committee, however, was sparse on the question of whether or not such assistance is presently provided in a timely manner.
- 2.164 The Committee acknowledges, however, that clearly expressed obligations would enable telecommunications providers to better assist the investigative agencies.

---

128 Optus, *Submission No. 206*, p. 2.

129 Australian Mobile Telecommunications Association – Communications Alliance, *Submission No. 114*, p. 13.

130 iiNet, *Submission No. 108*, p. 12.

131 Telstra, *Submission No. 189*, p. 10.

## 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.**

## Revision of the interception regime

- 2.165 Submissions and testimony provided to the Committee, particularly from interception agencies, indicate a desire for a comprehensive revision of the TIA Act. For example, the Western Australia Police submission states:

WA Police supports the suggested reform of the TIA Act in its entirety, for ease of understanding and in order to remove duplication. Further, there is a need to update the content of the TIA Act to ensure that the provisions are practical and responsive.<sup>132</sup>

- 2.166 In its submission, the AGD supports the proposal for comprehensive reform, stating:

The magnitude of current and anticipated change to the telecommunications landscape means it is now timely to consider whether the privacy needs of Australians and the investigative needs of law enforcement and national security agencies are best served through continuous ad-hoc change or whether the time is right to put in place a new interception framework that squarely focuses on the contemporary communications environment. The Department considers that holistic reform would establish a new foundation for the interception regime that enables users and participants, as well as the broader Australian community to understand their powers, rights and obligations.<sup>133</sup>

---

<sup>132</sup> Western Australia Police, *Submission No. 203*, p. 9.

<sup>133</sup> Attorney-General's Department, *Submission No. 218*, pp. 2-3

- 2.167 The Committee received extensive evidence from interception agencies, privacy advocates and legal practitioners about the complexity of the TIA Act. Indeed, the Committee's consideration of the statutory framework supports the conclusion that it is so complex as to be opaque in a number of areas. That this is the case in legislation which strives to protect the privacy of communications and enabling legitimate investigative activities is of concern.
- 2.168 The Committee acknowledges, however, the risks associated with comprehensive revision of legislation and that a cautious approach is necessary. Privacy Victoria noted in-principle support for revision to achieve technological neutrality, but cautioned:
- However, when revising these laws, the goal should not be to lower protections contained within, but rather to standardise and enhance existing protections irrespective of the method of communication (that is, to make the laws technologically neutral).<sup>134</sup>
- 2.169 The Committee did not have the advantage of receiving draft legislation to review. That being the case, there is an inherent difficulty in recommending comprehensive revision of the TIA Act in the absence of draft proposals.
- 2.170 The Committee acknowledges, however, that the TIA Act is complex. It could be improved significantly by providing clear direction on the protections afforded to telecommunications users, and the scope of the powers provided to agencies able to undertake telecommunications interception and access to stored communications and telecommunications data.
- 2.171 Implementing the recommendations of this report necessitates a significant revision of the interception regime. The Committee therefore supports comprehensive revision of the TIA Act.

---

134 Privacy Victoria, *Submission No. 109*, p. 2

## 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.



## Telecommunications security

3.1 The Terms of Reference to this inquiry state that the Government expressly seeks the views of the Committee on amending the *Telecommunications Act 1997* to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

- instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference;
- instituting obligations to provide Government with information on significant business and procurement decisions and network designs;
- creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers; and
- creating appropriate enforcement powers and pecuniary penalties.

3.2 The Attorney-General's Department (AGD) discussion paper notes that, with the pace of technological change, serious challenges to the security of telecommunications data have emerged:

Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental misconfiguration, external hacking and even trusted insiders.<sup>1</sup>

3.3 The implications of this risk are significant, especially given that Australian businesses, individuals and public sector actors rely on telecommunication carriers and carriage service providers' (C/CSPs) ability to store and transmit their data safely and securely, and to protect it from potential national security threats. The discussion paper notes that:

---

<sup>1</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29.

Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.<sup>2</sup>

3.4 The discussion paper further explains the significance of the telecommunications industry to national security:

While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy, degrade or alter the functioning of our critical telecommunications infrastructure and the information held on it. A clear understanding of the current telecommunications environment is essential to identifying network vulnerabilities and managing them effectively. This includes the composition and operation of the telecommunications industry, national security risks, and the current regulatory environment.<sup>3</sup>

3.5 The discussion paper cites the Director-General of ASIO's speech at the Security in Government Conference on 7 July 2011 outlining how poor security of telecommunications information poses a threat to national security:

States, as well as disaffected individuals or groups, are able to use computer networks to view or siphon sensitive, private, or classified information for the purpose of, political, diplomatic or commercial advantage.

Individual records or files stored or transmitted on telecommunications networks may not be classified or particularly sensitive in and of themselves but, in aggregate, they can give foreign states and other malicious actors a range of intelligence insights not otherwise readily available. This threat extends to information vital to the effective day-to-day operation of critical national industries and infrastructure, including intellectual property and commercial intelligence.<sup>4</sup>

3.6 Furthermore, these threats come from a variety of sources:

...other nation states, acting in their own national interest; criminal syndicates, especially – but not exclusively – well-resourced organised

---

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29. An externality refers to a cost or benefit that accrues to actors which are not directly involved in a transaction.

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 30.

4 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 32.

crime networks, which in some cases operate transnationally, compounding the difficulty of detecting and disrupting their activities; business corporations seeking commercial advantage over competitors; political or other issue-specific motivated groups; cyber-vandals; and a catch-all of other malicious and non-malicious 'hacktivists'.<sup>5</sup>

3.7 These threats originate in many different countries. According to a recent study by McAfee:

36 percent of all attacks originated from the United States, 33 percent from China and 12 percent from Russia. Of the remainder, Germany, the UK and France accounted for no more than six percent.<sup>6</sup>

3.8 The McAfee study also discussed the types of threats, finding that of the telecommunications infrastructure companies surveyed:

89 percent ... had experienced infection by a virus or malware; 60 percent had experienced 'theft of service' attacks; 54 percent experienced 'stealthy infiltration' that targeted theft of data or the takeover of critical Supervisory Control and Data Acquisition control systems; approximately 20 percent experienced extortion through the targeting and infiltration of control systems; and 29 percent had experienced large scale distributed denial of service attacks, often several times a month, of which two thirds had impacted on operations.<sup>7</sup>

3.9 To counter those threats, the discussion paper proposes the development and implementation of a 'risk based regulatory framework to better manage' these national security challenges to telecommunications security.<sup>8</sup>

3.10 The discussion paper proposes a package of reforms to the *Telecommunications Act 1997* and associated legislation to establish this regulatory framework:

- An industry-wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;
- A requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and

---

5 Ian Dudgeon, 'Cyber-Security: the importance of partnerships', *Regional Security Outlook 2013*, Council for Security Cooperation in the Asia-Pacific, p. 9.

6 Ian Dudgeon, 'Cyber-Security: the importance of partnerships', *Regional Security Outlook 2013*, Council for Security Cooperation in the Asia-Pacific, p. 10.

7 Ian Dudgeon, 'Cyber-Security: the importance of partnerships', *Regional Security Outlook 2013*, Council for Security Cooperation in the Asia-Pacific, p. 10.

8 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29.

- Powers of direction and a penalty regime to encourage compliance.<sup>9</sup>

3.11 The discussion paper states that the desired outcomes of the proposed framework are that:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,
- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,
- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities,
- the protection of information, including customer information and information about customers, contained on or transmitted across telecommunications networks is better assured, and
- compliance costs for industry are minimised.<sup>10</sup>

## Issues raised in evidence

### Is there a need for an industry wide obligation to protect telecommunications?

3.12 Mr Mark Newton disputed the discussion paper's contention that there is a need for Government intervention in the telecommunications industry for the purpose of national security advising that 'it isn't the role of carriers and carriage service providers (C/CSPs) to make business decisions in the intelligence community's best interests', rather:

It's the intelligence community's job to stay sufficiently informed and organisationally nimble that they can accommodate C/CSPs' business decisions without feeling a need to interfere in them.<sup>11</sup>

3.13 In a similar vein, Mr Daniel Black contended that telecommunications security was the Government's responsibility:

---

9 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 34.

10 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 29-30.

11 Mr Mark Newton, *Submission No. 87*, p. 10.

Private industry values the privacy of its business and procurement decisions as much as the government values its “information about the national security environment”. Instituting obligations in legislation is a crude mechanism and shows the government to industry relationship is broken that these meaningful private dialogues are not taking place to the level required.<sup>12</sup>

- 3.14 Macquarie Telecom disagreed that there is a need for Government intervention on the issue of security because it saw that providing security was already in the interests of service providers:

You could imagine that we would have a significant interest in ensuring that that information is kept secure and that it is retained and dealt with at a high level of security. In that sense we wanted to bring it to the attention of the committee that the market is responding to the need for cyber security. We are not saying that means that the entire Australian network and national security is in perfect hands, but we want to bring it to the attention of the committee that there are market responses going on that ought to be taken into account when thinking about what the broader regulatory arrangements should be that affect all players.<sup>13</sup>

- 3.15 Macquarie Telecom contended that industry-led self-regulation would be a more proportionate alternative regulatory intervention. Self-regulation could involve a voluntary obligation to protect telecommunications infrastructure, networks and systems. Macquarie Telecom further argued that an unenforceable industry code, informed by government guidelines, would be preferable for obtaining voluntary compliance.<sup>14</sup>

- 3.16 In contrast, the Commonwealth Privacy Commissioner (within the Office of the Australian Information Commissioner), Mr Timothy Pilgrim, agreed with the discussion paper’s objective of requiring telecommunications industry participants to protect information:

The Office of the Australian Information Commissioner welcomes the fact that one of the desired outcomes of the framework is that the security of individuals’ personal information contained on or transmitted across telecommunication networks is better assured.

The OAIC supports the policy intention behind the proposal to introduce a regulatory framework that will address security and resilience risks posed to Australia’s telecommunications infrastructure.

---

12 Mr Daniel Black, *Submission No. 97*, p. 7.

13 Mr Matthew John Healy, National Executive, Industry and Policy, Macquarie Telecom, *Transcript*, 5 September 2012, pp. 11 -12.

14 Macquarie Telecom, *Submission No. 115*, pp. 2-3.

...

The OAIC welcomes the fact that one of the desired outcomes of the framework is that the security of individuals' personal information contained on or transmitted across telecommunication networks is better assured.<sup>15</sup>

- 3.17 In contrast to Macquarie Telecom, another telecommunications industry participant, Optus, favoured obligations being equally placed on all industry participants and expressed 'cautious support' for a legislated framework:

For a number of years Optus has engaged informally with national security agencies on matters relating to the security and resilience of its networks and business operations, including offshore operations. Having regard to the positive aspects of this experience, Optus has formed the view that it is desirable to move to a more structured scheme, to ensure that the benefits and responsibilities are proportionately shared across the industry (for competitive and equity reasons). Optus provides "cautious support" for the implementation of a scheme.<sup>16</sup>

- 3.18 Optus' cautious support was contingent on how the Government might design such a framework:

I want to emphasise that our caution arises more from the challenge of correctly calibrating the practical design of such a scheme (and the downside risks of incorrectly calibrated arrangements), than fundamental concern about the principle.<sup>17</sup>

### How should a telecommunications security model be structured?

- 3.19 The AGD discussion paper proposes a compliance framework, based on requiring industry participants to be able to demonstrate 'competent supervision' and 'effective control' over their networks.
- 3.20 Competent supervision refers to the ability of a service provider to maintain technically proficient oversight of the operations of their network, and the location of data; awareness of, and authority over, parties with access to network infrastructure; and a reasonable ability to detect security breaches or compromises.<sup>18</sup>

---

15 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

16 Optus, *Submission No. 206*, p. 3.

17 Optus, *Submission No. 206*, p. 3.

18 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 35.

3.21 Effective control refers to the ability of a C/CSP to maintain direct authority or contractual arrangements which ensure that its infrastructure and the information held on it is protected from unauthorised interference.<sup>19</sup>

3.22 Optus agreed that this proposed framework could be effective:

We support the idea that a scheme should be targeted to achieve and verify outcomes, rather than be prescriptive about particular business practices, network designs or purchasing decisions. This aligns with the proposed approach of a scheme requiring carriers to demonstrate:

- Competent supervision; and
- Effective control.<sup>20</sup>

3.23 The Australian Mobile Telecommunications Association and Communications Alliance, representing the industry as a whole, preferred an outcomes-based approach to regulation:

The Associations agree that the regulatory framework should focus on security outcomes rather than technical requirements and that industry should be able to demonstrate compliance rather than have prescriptive obligations imposed.

Noting the importance of network security and resiliency in the digital age, the Associations on the whole welcomes the Government's pragmatic security outcomes/objectives based approach as opposed to stipulating a requirement for Government approval of network architecture at a technical or engineering level.<sup>21</sup>

3.24 Similarly, the Commonwealth Privacy Commissioner, within the Office of the Australian Information Commissioner, agreed that a framework should be focussed on the end results, rather than a prescriptive government-led process:

The Office of the Australian Information Commissioner considers that such an outcomes-based regulatory framework would ensure that [service providers] have sufficient flexibility to respond to changes in telecommunications technology, whilst also ensuring that the Government remains responsible for ensuring that the overall protection of personal information is achieved.<sup>22</sup>

---

19 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 36.

20 Optus, *Submission No. 206*, p. 3.

21 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 17; see also: Huawei Technologies (Australia) Pty Limited, *Submission No. 149*, p. 11.

22 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

- 3.25 The Australian Mobile Telecommunications Association and Communications Alliance further argued that direct government control of the business decision-making process would be excessive:

A regulatory regime that mandates external controls over procurement and network design practices and requires extensive notification practices would certainly amount to an overly prescriptive level of intervention.

The Associations believe that such a regulatory framework would restrict the ability of network and infrastructure providers to cost-effectively implement platforms that are innovative, progressive and provide supplier differentiation. Controls over procurement would also unnecessarily increase timeframes for network rollouts, which would contradict the Government's advocacy for increased broadband deployment.<sup>23</sup>

## Information sharing and compliance auditing

- 3.26 The AGD discussion paper states that Government would provide guidance to assist industry to understand and meet its obligations, and to inform Carriers/Carriage Service Providers (C/CSPs) how they can maintain competent supervision and effective control over their networks. In order to monitor compliance with the obligations under a framework, C/CSPs would be required to demonstrate compliance to Government. This could be done by compliance assessments and audits, based on a risk assessment to inform the level of engagement required.<sup>24</sup>

- 3.27 In relation to the inherent risk of private sector entities being obliged to provide information to Government Mr Mark Newton observed that:

Businesses also need to be mindful of the fact that any information they provide to the Government can potentially be released (e.g., under Freedom of Information, subpoena, or leak), so it's wise to be reluctant about sharing.<sup>25</sup>

- 3.28 The Committee observes that industry is required to provide similar network and service information to the Attorney-General's Department under the interception capability obligations contained in the *Telecommunications (Interception and Access) Act 1979*. That information is given statutory protection

---

23 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 17.

24 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 36.

25 Mr Mark Newton, *Submission no. 87*, p. 10.



from disclosure to any other person without the written permission of the C/CSP concerned.<sup>26</sup>

- 3.29 Macquarie Telecom, in accepting that protecting the security of Australia's telecommunications network infrastructure is in Australia's national interest, noted that it was incumbent on Government to communicate with industry:

At the same time, C/CSPs and other players in the broader communications sector are highly motivated to ensure the security of their own network infrastructure, systems and data. With a clear alignment between the interests of industry players and the Government on the need for network infrastructure security, Macquarie believes a better outcome could be achieved with increased communication at a trusted level between industry and Government.<sup>27</sup>

- 3.30 The complementary roles that industry and government can play was highlighted by Vodafone Hutchison Australia:

- The Government's security agencies are best placed to outline what are actual and emerging security risks and provide clear guidance to the industry about effective protections and controls to mitigate these risks.
- The telecommunications industry is best placed to determine what are the most appropriate operational and technical controls for their businesses.<sup>28</sup>

- 3.31 The Australian Mobile Telecommunications Association and Communications Alliance argued that industry participants need to know in advance of making their decisions what position and advice Government may have:

The Associations have proposed that requirements regarding networks and infrastructure need to be clearly defined so that industry can invest and deploy infrastructure with confidence and, without concern that government will raise objections once such networks are deployed.<sup>29</sup>

- 3.32 Telstra highlighted uncertainty in how risk assessments might work in practice:

What is not clear is whether these "risk assessments" would be subject to legislated timeframes so as to avoid delaying procurement or network design activities. It is also unclear if C/CSPs will have to implement the

---

26 *Telecommunications (Interception and Access) Act 1979*, section 202.

27 Macquarie Telecom, *Submission No. 115*, p. 2.

28 Vodafone Hutchison Australia, *Submission No. 113*, p.2; see also: Optus, *Submission no. 206*, p. 3, Cisco Systems Australia Pty Limited, *Submission No. 112*, p. 2; and Huawei Technologies (Australia) Pty Limited, *Submission No. 149*, p. 12.

29 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 18; see also: Telstra, *Submission no. 189*, p. 12.

suggested outcomes of the “risk assessments” and if there are any penalties for not doing so.<sup>30</sup>

## Remediation powers and a penalty regime

- 3.33 The AGD discussion paper proposes that the risk management framework for determining that Carriers and Carriage Service Providers (C/CSPs) will practice competent supervision and effective control of their systems will need to be underpinned by penalties and the ability of government to make directions to service providers:

Where potential issues of concern are identified, the preferred approach would be to engage with the relevant C/CSPs to establish whether national security concerns can be co-operatively addressed. Where this is not possible, one way to proportionately address various levels and forms of non-compliance could be to provide a graduated suite of enforcement measures (including the power of direction). The availability of enforcement measures would provide industry with greater incentive to engage co-operatively with Government.

Under such an approach, in cases where engagement with C/CSPs proves to be ineffective, or a blatant disregard of security information jeopardises the Government’s confidence in the security and integrity of Australia’s telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance.<sup>31</sup>

- 3.34 The Australian Mobile Telecommunications Association and Communications Alliance in their joint submission were not convinced that it is yet necessary to create an interventionist or punitive compliance regime:

With regard to the proposal for an amendment to the Act to allow for the creation of appropriate enforcement powers and associated pecuniary penalties, the Associations’ position is that development of a financial penalties framework is premature, and not conducive to the development of an appropriate level of trust, and a common vision on security and resiliency, between Government and service providers.<sup>32</sup>

- 3.35 Telstra argued that government already possesses the means to dissuade service providers from engaging in poor security practices:

---

30 Telstra, *Submission No. 189*, pp. 12-13.

31 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 37.

32 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 19.

Telstra believes the most sensible way to provide these incentives would be through the Government's own procurement practices – i.e. Government to specify in requests for proposal/tender their security, resilience and integrity requirements for IT and communications services supplied to Government by C/CSPs.<sup>33</sup>

- 3.36 The Australian Mobile Telecommunications Association and Communications Alliance also argued that if the framework in the discussion paper was to be established as proposed, the framework should include avenues to appeal government decisions:

The Associations propose that it should include a facility for an appropriate and truly independent means of review or appeal to prevent arbitrary or unjust use of directions or penalties.<sup>34</sup>

## Other considerations

### Regulatory impacts

- 3.37 The Committee received some limited evidence about the potential regulatory impacts that the telecommunications security reform might have on industry. However, these points were not elaborated upon in submissions or in oral evidence to the Committee. The Australian Mobile Telecommunications Association and Communications Alliance in their joint submission stated:

Concerns previously raised by the Associations on the proposal to make legislative and regulatory changes to enhance the security and resilience of telecommunications network infrastructure, are as follows:

- the potential for the proposed regime to bring providers into conflict with existing corporate regulations, particularly those relating to the disclosure of information;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia. Many operators have global or regional supply arrangements which would in effect become invalid under the proposed regime. This would result in costs to operators in the amount of many millions of dollars as a result of having to break regional/global supply contracts;
- impacts on competition in the market-place and risk that proposed requirements may create a barrier to entry for new, lower cost providers and could eliminate some of those already in the market,

---

33 Telstra, *Submission No. 189*, p. 13.

34 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 18.

resulting in decreased market competition on pricing and general consumer detriment;

- the absence, to date, of any protection/indemnity to civil action for providers who have acted in good faith under the requirements of the proposed amendments;
- the fact that the rapidly changing technology landscape, where potential vulnerabilities now exist at the physical, network and application layers, has not been sufficiently taken into account, specifically with regards to the concept of “critical infrastructure”; and
- the need to engage further with industry on possible regulatory alternatives: such as a set of guidelines to provide guidance for providers in the areas of procurement and network design; a process for Government-industry engagement where a high risk event is identified and a framework for periodic reporting to Government agencies on the security measures being taken by providers.<sup>35</sup>

## Data breach notifications

- 3.38 The Privacy Commissioner, within the Office of the Australian Information Commissioner (OAIC), raised the potential introduction of a compulsory data breach notification regime to supplement security arrangements:

While notification of a data breach is currently not required by the Privacy Act, the OAIC suggests that it be considered as part of the proposed framework as an important mitigation strategy against privacy risks. It may also assist in promoting transparency and trust for C/CSPs.

The OAIC suggests that the implementation of an effective mechanism for ensuring that industry has taken reasonable steps to mitigate security risks is essential and will assist in achieving the necessary levels of transparency and accountability. In the event that there is a complaint to the OAIC, access to any compliance assessments and audits of the Government under the proposed regime would assist the OAIC in its investigation of the matter.<sup>36</sup>

- 3.39 Similarly, the Australian Mobile Telecommunications Association and Communications Alliance, in their joint submission, contended that a cyber-attack reporting regime would be preferable to the penalty and remediation regime proposed in the discussion paper:

---

35 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, pp. 18-19.

36 Office of Australian Information Commissioner, *Submission No. 183*, p. 20.

An alternative, and preferable, approach would be to require a reporting regime relating to cyber-attacks on Australian networks with noticeable operational impact by service providers as opposed to a system which enforces penalties on those providers. Where service providers can demonstrate implementation of reasonable minimum network security measures then imposition of a penalty based instrument would seem to be punishing those service providers who have taken steps to ensure, within their control, that a certain level of precaution has been exercised at a network level.<sup>37</sup>

- 3.40 Senetas, a private sector security consultant, was also of the view that the government make data breach notification mandatory for C/CSPs.<sup>38</sup>

### Free trade commitments

- 3.41 Australia's free trade commitments require any barriers to trade to be no more trade-restrictive than necessary to fulfil the legitimate objective of protecting national security. Huawei Australia cautioned that a legislative framework that targets particular vendors or vendors from particular countries could also raise concerns about free trade commitments:

Under the General Agreement on Tariffs and Trade (GATT), World Trade Organisation (WTO) members are essentially required not to discriminate against imported products on the basis of their country of origin. If the Network Security Reforms result in discrimination against vendors on the basis of their country of origin, it is likely that this would place Australia in breach of its WTO obligations under the GATT.<sup>39</sup>

---

37 Australian Mobile Telecommunications Association and Communications Alliance, *Submission No. 114*, p. 19.

38 Senetas, *Submission No. 237*, p. 1.

39 Huawei Technologies (Australia) Pty Limited, *Submission No. 149*, p. 15.

## Committee comment

- 3.42 The Committee understands the rationale of the Telecommunications Sector Security Reform proposal and notes the warm, if cautious support, of most industry submitters.
- 3.43 There are threats to Australia's national security that can be effected through the telecommunications systems. The industry itself is best placed to deal with those threats, however, it cannot protect its systems and infrastructure of which it is ignorant or that it does not understand. As well, there is the problem of participants which ignore, or fail to take them sufficiently seriously. The relevant threat information is held by government. Where appropriate, there is therefore a need for Government to share threat information with industry in order for industry participants to make informed decisions about their procurements and outsourcing arrangements.
- 3.44 Conversely, it would not be possible for government and industry to have effective or guided discussions without industry providing essential background information to government with which it can assess threats. The greatest improvements to telecommunications sector security would come through dialogue – with both industry and Government exchanging useful, and sensitive, information.
- 3.45 The Committee is of the view that it will be necessary to encourage service providers to engage with Government and to accept the advice given to them. Although there are currently indirect incentives for service providers to protect their customers' information (such as public relations damage), commercial interests will not always align with the national interest.
- 3.46 To account for those instances where advice is not acted upon and where national security is threatened, the Committee agrees that Government should create a scheme including the capacity for Government to direct service providers to take certain remediation actions.
- 3.47 The Committee believes there cannot be an effective and equitable security regime without enforcement mechanisms.

## Interaction between data retention and telecommunications security

- 3.48 The Privacy Commissioner drew the Committee's attention to the need to consider telecommunications sector security reform for telecommunications data that is held under any potential data retention regime:

The OAIC notes that ensuring that Australian telecommunications networks are protected by an effective security framework is particularly important given the proposals relating to data retention.<sup>40</sup>

- 3.49 The Committee agrees with the Privacy Commissioner that there is a clear need to secure information or data that is stored, given that there are already large volumes of telecommunications information held by telecommunications providers.
- 3.50 The Committee is, therefore, of the view that an infrastructure and information security regime should be introduced whether or not Government chooses to introduce a data retention regime.

### Regulatory impacts

- 3.51 As highlighted by the Australian Mobile Telecommunications Association and Communications Alliance, a Regulation Impact Statement should consider further issues that were not examined in detail in submissions or in evidence given at hearings to this inquiry. Such issues should include:
- the interaction of the proposed regime with other corporate regulations;
  - the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
  - consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
  - impacts on competition in the market-place, including:
    - ⇒ the potential for proposed requirements may create a barrier to entry for lower cost providers;
    - ⇒ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
    - ⇒ any other relevant effects.

---

40 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

## Recommendation 19

The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide:

- a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference;
- a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and
- powers of direction and a penalty regime to encourage compliance.

The Committee further recommends that the Government, through a Regulation Impact Statement, address:

- the interaction of the proposed regime with existing legal obligations imposed upon corporations;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
- impacts on competition in the market-place, including:
  - ⇒ the potential for proposed requirements to create a barrier to entry for lower cost providers;
  - ⇒ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
  - ⇒ any other relevant effects.



## Australian Intelligence Community Legislation Reform

- 4.1 The Attorney-General's Department (AGD) discussion paper notes that the security environment in which Australia's intelligence agencies operate 'is continually evolving and becoming increasingly diversified'. This evolution and diversification in turn requires these intelligence agencies to adapt, and as such the discussion paper argues that:

...it is imperative that these agencies are appropriately equipped with the necessary statutory powers to uphold Australia's vital national security interests.<sup>1</sup>

- 4.2 The Attorney-General's Department and agencies within the Australian Intelligence Community have identified a number of practical difficulties with the legislation governing the operation of those agencies.

- 4.3 As such, the discussion paper canvasses a number of reforms to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act). According to the discussion paper, these reforms are necessary to:

...maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.<sup>2</sup>

---

<sup>1</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

<sup>2</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

4.4 The proposed reforms fall into three broad categories:

- Matters the Government wishes to progress: changes to ASIO's warrant provisions; changes to ASIO Act employment provisions; and clarifying the authority of DIGO.
- Matters the Government is considering: amending the ASIO Act to create an authorised intelligence operations scheme; further changes to ASIO's warrant provisions; and clarifying the ability of ASIO to cooperate with private sector actors.
- Matters on which the Government seeks the views of the Parliamentary Joint Committee on Intelligence and Security (the Committee): further changes to ASIO's warrant provisions; ministerial authorisations for Australia's foreign intelligence agencies to produce intelligence on Australian citizens; and ASIS cooperation with overseas authorities on self-defence and weapons training.

## **Proposals the Government wishes to progress**

### **ASIO Act – Computer access warrants**

- 4.5 The Terms of Reference for this inquiry incorporate three separate issues relating to computer access warrants. One issue is a matter that the Government wishes to progress, a second is a matter that the Government is considering and the third is a matter that for which the Government expressly seeks the Committee's views. In this report, the three issues will be dealt with together because of their common subject matter.
- 4.6 Section 25A of the ASIO Act currently allows the Director-General of Security to request the Attorney-General to issue a computer access warrant. The Attorney-General may issue the warrant if satisfied that there are reasonable grounds for believing that access to data held in a particular computer will substantially assist the collection of intelligence in respect of a security matter.
- 4.7 Computer access warrants authorise ASIO to do things specified by the Attorney-General in relation to a particular computer, subject to any restrictions also specified by the Attorney-General.
- 4.8 The ASIO Act currently allows the Attorney-General to specify the entering of premises, the use of computers, telecommunications facilities, other electronic devices and data storage devices for the purpose of obtaining data that is held on the target computer and, if necessary, adding, deleting or altering other data in the target computer if it is necessary to obtain the data.
- 4.9 A warrant issued under section 25A empowers ASIO to copy any data that appears to be relevant to the collection of intelligence, as well as do anything that

is reasonably necessary to conceal that any action has been done under the warrant.

4.10 However, ASIO is prohibited from adding, deleting or altering other data in the target computer or doing anything that interferes with, interrupts or obstructs the lawful use of the target computer by other persons.

4.11 The Attorney-General's Department discussion paper nominates three particular changes to section 25A that would enhance its effectiveness.

### References to 'computer' in section 25A

4.12 The Terms of Reference state that the Government wishes to amend the ASIO Act to update the definition of computer in section 25A. The discussion paper elaborates that the ASIO Act could be amended so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.<sup>3</sup>

4.13 Computer access warrants under section 25A of the ASIO Act are limited to obtaining data stored on 'a computer'. A 'computer' is defined to mean 'a computer, a computer system or part of a computer system'. This means that if an individual has more than one computer which is not part of the same computer system, or data is stored on a computer network, it may be necessary for the Attorney-General to issue more than one warrant.

4.14 The discussion paper asserts that 'this is inefficient and does not increase the level of accountability around the issue of warrants'. The discussion paper further suggests that a possible solution to this issue could be to:

...amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.<sup>4</sup>

4.15 Mr Ian Quick identified that there may be some over-reach or ambiguity in how far removed from the target intelligence a computer could be lawfully accessed:

Could a single warrant cover all computers at BHP headquarters? All computers at a university?<sup>5</sup>

4.16 Mr Quick added:

A 'computer network' is even more worrying. How is the network defined? Everything the person could access anywhere on the internet? Everything on their 'local' (on the premises) network? Where exactly

---

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 39.

4 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 39.

5 Mr Ian Quick, *Submission No. 95*, p. 8.

would the warrant boundaries be, given that it could be argued that the bulk of computers on the planet are on the same 'network'?<sup>6</sup>

4.17 The Inspector-General of Intelligence and Security (IGIS) noted that:

Computing technology and usage patterns have changed and continue to change, however the proposed response may introduce further issues. For example, the term 'computers connected to a computer network' is potentially very broad in scope. It is difficult to contemplate when it would be reasonable to access *all* computers connected to a network in the absence of further limitations. Similarly 'computers on a particular premises' could inadvertently include computers that can have no connection whatsoever with the individual of interest.<sup>7</sup>

4.18 Similarly, the Gilbert + Tobin Centre of Public Law argued:

ASIO should not be able to seek a warrant to access the computers on a particular network unless there are reasonable grounds to believe that the person in relation to whom intelligence is being sought had a connection with computers other than his own on the network.<sup>8</sup>

4.19 The Australian Privacy Foundation argued that the ambiguity of the discussion paper meant that such changes 'may be harmless or disastrous depending on exactly what is intended'. The Australian Privacy Foundation further advised that:

The Committee should reject outright the concept of agencies ever being permitted to perform an act that "adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons", on the grounds that such acts pollute evidence, and enable the "framing" of suspects.<sup>9</sup>

### Committee comment

4.20 The Committee notes the concerns that have been raised as to the authority that may be given to ASIO under the proposed changes to the computer access warrants regime. However, the Committee is of the view that giving full effect to the original intention of that warrant regime is necessary.

4.21 In an environment of rapidly evolving technology, the capability of ASIO should not be degraded by the definition of computer in the ASIO Act being obsolete. Therefore, the Committee considers that the existing definition of computer in the ASIO Act, and in particular the term "computer system", may not be sufficient to include a multiplicity of computers operating together as a network.

6 Mr Ian Quick, *Submission No. 95*, p. 8.

7 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 14.

8 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 11.

9 Australian Privacy Foundation, *Submission No. 162*, p. 9.

In the Committee's view, computer networks should be within the definition of "computer".

- 4.22 The Committee understands the desire of ASIO to enable warrants to extend to all computers located on a particular premises, or connected to a particular person; however it does not consider that the issue is appropriately addressed by amending the definition of "computer" but rather by amending the warrant provisions.

## **Recommendation 20**

**The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words "and includes multiple computers operating in a network".**

**The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.**

## **Enabling the disruption of a target computer**

- 4.23 The Terms of Reference state that the Government is considering amending the ASIO Act to modernise and streamline ASIO's warrant provisions to enable the disruption of a target computer for the purposes of a computer access warrant.
- 4.24 The discussion paper elaborates that subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.
- 4.25 The discussion paper explains that the existing formulation of the prohibition leads to difficulties in executing computer access warrants:
- The increasingly complex nature of the global information technology environment and the use by some targets of sophisticated computer protection mechanisms can adversely impact ASIO's ability to execute a

computer access warrant for the purpose of obtaining access to data relevant to security.<sup>10</sup>

4.26 The discussion paper suggests that to address those difficulties section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant.

4.27 The Law Council of Australia countered the discussion paper's assertions by highlighting the original intent of the provision that prevents ASIO from disrupting the target computer when it executes its warrant:

Having regard to this legislative history, the Law Council questions the basis of this proposed reform in relation to sub-section 25A(5). This key provision was considered important to the community and the Parliament when it was introduced and the discussion paper does not justify its removal other than through the general statement about the global information technology environment and sophisticated computer protection mechanisms adversely impacting on ASIO's ability to execute computer access warrants.<sup>11</sup>

4.28 The Inspector-General of Intelligence and Security (IGIS) addressed concerns by clarifying the intent of the proposal:

I understand that the proposal is to enable ASIO to do only what is necessary to covertly retrieve the information sought under the warrant. That is, the primary purpose of any disruption would be to avoid disclosing to the person or group under surveillance that ASIO was monitoring them. This seems to be a reasonable solution to current operational problems.<sup>12</sup>

4.29 The Attorney-General's Department was asked why ASIO should be allowed to disrupt a target computer if the law currently prevents such actions from being authorised. The Department expanded upon the intent of the proposal:

This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be. As this requirement is expressed in absolute terms, it can prevent ASIO from being able to execute a warrant if doing so would have even a minor or inconsequential impact, such as a temporary slowing of the computer. It could also create uncertainty if it is not possible to determine whether doing something under a computer access warrant may interfere with, interrupt or obstruct the lawful use of the computer by other persons.<sup>13</sup>

---

10 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

11 Law Council of Australia, *Submission No. 96*, p. 66.

12 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20.

13 Attorney-General's Department, *Submission No. 236*, p. 2.

- 4.30 In their joint submission, the peak industry bodies the Australian Mobile Telecommunications Association and Communications Alliance expressed concern that disruption of a target computer could inadvertently lead to damage to broader telecommunications networks:

Disruption of a target computer, or network, should be facilitated by agency mechanisms. Industry would strongly oppose any proposal for disruption mechanisms being inserted into information communications networks, communications devices, and any other publicly available applications platforms.<sup>14</sup>

- 4.31 Similarly, Telstra expressed its concern as to the involvement of telecommunications service providers:

If such a change to legislation is contemplated, Telstra would expect that ASIO provide [service providers] with full indemnity in relation to proceedings brought by a third party in relation to this form of interception.<sup>15</sup>

- 4.32 In relation to accessing information stored in cloud computing facilities, Mr Robert Batten, submitting in a private capacity, cautioned:

Any reform that allows interruption to service needs to be worded to be cognisant of the potentially very broad implications of such interruption, and that warrants for physical computers are becoming less relevant in the face of rapid virtualisation.<sup>16</sup>

### Committee comment

- 4.33 The Committee notes the Attorney-General's Department's submission that there is a need to address difficulties that can arise in executing ASIO's computer access warrants. The Committee further notes that the ASIO Act should be amended so that the prohibition on disrupting computers does not apply to activities that would be necessary to execute the warrant.
- 4.34 The Committee also encourages the Government to consider including provisions in the ASIO Act that would prevent damage or cause loss to telecommunications systems operated by third parties.
- 4.35 The Committee agrees with the comments of the IGIS that this proposal should be framed carefully to minimise the impact on parties unrelated to the security matter:

<sup>14</sup> Australian Mobile Telecommunications Association and Communications Alliance, *Submission no. 114*, p. 20.

<sup>15</sup> Telstra, *Submission No. 189*, p. 14; see also: Mr Evan Slatyer, *Submission No. 131*, p. 1.

<sup>16</sup> Mr Robert Batten, *Submission No. 50*, p. 10; see also Internet Society of Australia, *Submission No. 145*, p. 3.

As this proposal could directly affect the activities of persons unrelated to security interests it would be essential to have to clearly justify the case as to why it is appropriate to affect any lawful use of the computer. The reasons would need to balance the potential consequences of this interference to the individual(s) with the threat to security.<sup>17</sup>

- 4.36 The Committee also agrees with the IGIS that there should be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties.

### Recommendation 21

**The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.**

### Access via third party computers and communications

- 4.37 The Terms of Reference state that the Government expressly seeks the views of the Committee on amending the ASIO Act to modernise and streamline ASIO's warrant provisions by using third party computers and communications in transit to access a target computer under a computer access warrant.

- 4.38 As with the proposals considered above, the discussion paper attributes the increasingly difficult situation ASIO faces in executing its computer access warrants to advancements in technology. This is particularly the case where a target is security conscious and ASIO must consider 'innovative methods' to access the target computer:

In the same way that access to a third party premises may be necessary to execute a search warrant, it may be necessary to use a communication that is in transit or use a third party computer for the purpose of executing a computer access warrant.<sup>18</sup>

- 4.39 The discussion paper proposes:

17 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20.

18 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 50.



To overcome this problem, it may be appropriate to amend the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer. Noting that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.<sup>19</sup>

- 4.40 The description of the proposal and the lack of reference to what a legislative framework for third party access might entail drew criticism:

There is no reference to proportionality tests applicable or the need to balance any national security benefit against the cost to individual privacy.<sup>20</sup>

- 4.41 There was also criticism of the very nature of accessing the computers of people who are not directly national security targets:

In my view, this proposal is completely unjustified. To access a third party's computer which has no connection with the target is extraordinarily broad and intrusive. These are powers usually characteristic of a police state. Adversely impacting the privacy of an individual (the third party) should only be permitted in the most extreme circumstances as a "last resort" when all other methods have been exhausted. Furthermore, the power to alter (rather than "access") a third party computer should not be permitted.

Even with such safeguards and accountability mechanisms (which are not detailed in the discussion paper), I cannot support a measure that could severely diminish the privacy of individuals and could cause a chilling effect on the way that individuals communicate and use technology.<sup>21</sup>

- 4.42 The Acting Commissioner of the Victorian Privacy Commission elaborated on his comment for the Committee at a hearing. The Commissioner was asked whether this proposal would be acceptable if there were appropriate safeguards:

It still severely diminishes the privacy of individuals. Certainly, it would need the safeguards and accountability mechanisms and it would need to be strongly argued that it met those tests of legitimacy, necessity and proportionality. But there is not even an attempt, in my view, in the discussion paper to do that.<sup>22</sup>

---

19 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 50.

20 Liberty Victoria, *Submission No. 143*, p. 3; see also: Mr Daniel Judge, *Submission No. 157*, p. 13; Ms Stella Gray, *Submission No. 152*, pp. 11-12; see also: New South Wales Young Lawyers, *Submission No. 133*, p. 8.

21 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 6.

22 Dr Anthony Bendall, Acting Privacy Commissioner, Office of the Victorian Privacy Commissioner, *Transcript*, Melbourne, 5 September 2012.

- 4.43 The Attorney-General's Department was asked why ASIO should be empowered to 'hack' the computers of people who are not threats to security. The Department clarified that the proposal would not allow for surveillance of third party computers:

The proposals would not involve hacking in the sense of authorising ASIO to examine the content of material. AGD notes the concerns raised in submissions to the Committee, for example from the Office of the Victorian Privacy Commissioner, that the proposal would allow surveillance of virtually unlimited services. However, the purpose of a warrant authorising the use of a third party computer would still be to access the computer of security interest, and the warrant would not authorise ASIO to obtain intelligence material from the third party computer or the communication in transit.<sup>23</sup>

- 4.44 The IGIS suggested an appropriate precedent within the *Telecommunications (Interception and Access) Act 1979* (TIA Act) that could be adapted in the ASIO Act to provide appropriate accountability safeguards, should the proposal be adopted:

Any such change must ensure that the impact on the third party, including privacy implications as well as any impact on the security or lawful use of the third party computer are considered carefully in the approval process.

Currently the TIA Act allows ASIO to obtain a warrant from the Attorney-General to intercept communications via a third party only where all other practicable methods have been exhausted or where it would not otherwise be possible to intercept the relevant communications. This appears to be an appropriate safeguard.<sup>24</sup>

- 4.45 The IGIS refers to interception warrants that are labelled 'B-Party' warrants.

- 4.46 The Attorney-General's Department offered further clarification of the safeguards that would limit the intrusiveness of access to third party computers and communications:

There are a range of safeguards that already exist so that third party computers and communications in transit could only be used in limited circumstances. It is envisaged that use of third party computers and communications in transit would need to be expressly authorised by the Attorney-General when issuing a warrant. The Attorney-General's Guidelines contain requirements for ASIO to use as little intrusion into

---

23 Attorney-General's Department, *Submission No. 236*, p. 1.

24 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 21.

privacy as possible and for the measures used to obtain intelligence to be proportionate to the gravity of the threat (section 10.4).<sup>25</sup>

- 4.47 Mr Johann Trevaskis, submitting in a private capacity, noted additional practical questions that the Government should consider when it develops draft legislation for Parliament's consideration:

It also raises the issue of what happens if the third party detects what is going on. The third party is unlikely to be aware of the ASIO operation. The third party may deliberately or unintentionally reveal details of it, or interfere with it. The third party, thinking his system is under attack, may actively take countermeasures. Will the third party be indemnified for any of this? If the third party becomes aware of what is going on is the third party obliged to consent to the intrusion?<sup>26</sup>

### Committee comment

- 4.48 The Committee notes that there are circumstances in which it would be necessary for ASIO to access a third party computer or communication in transit for the ultimate purpose of lawfully accessing a target computer.
- 4.49 The Committee notes that third party access has significant privacy implications and that therefore appropriate safeguards and accountability mechanisms, such as those included in the TIA Act for 'B-Party' interception warrants, would need to be incorporated into such a scheme.
- 4.50 The interception of voice communications via third parties is already lawful under the TIA Act. This proposal would extend this capability under warrant to ASIO via the ASIO Act to allow it to access data through third parties. In essence, this is another case of updating the Acts to keep pace with technological developments.

### Recommendation 22

**The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*.**

25 Attorney-General's Department, *Submission No. 236*, p. 1.

26 Mr Johann Trevaskis, *Submission No.62*, p. 11.

## ASIO Act warrant proposals

- 4.51 The Terms of Reference and discussion paper describe three related proposals that have the potential to affect the operation of all warrant types contained in the ASIO Act. Broadly, these proposals relate to the duration, variation and renewal of ASIO warrants.
- 4.52 Under the ASIO Act, the Director-General of Security applies to the Attorney-General for warrants. If satisfied that all the criteria have been met and that a case has been made that special powers should be used in a particular matter, the Attorney-General may issue a warrant at their discretion.
- 4.53 It is important to note that those powers exercised under warrant are of an inherently intrusive nature. They include search, listening device, tracking device and computer access warrants. In the case of surveillance and computer access warrants, they are executed covertly and the persons affected might never know that they were under surveillance.
- 4.54 Some general observations and criticisms that cover all three related proposals were made:
- Liberty Victoria is concerned that the proposals to extend the duration and allow the renewal of warrants potentially undermine judicial scrutiny of warrants. The lack of evidence to support the need for reforms and the lack of reference to accountability measures is problematic given the highly invasive nature of search warrants.<sup>27</sup>
- 4.55 The IGIS outlined the principles that ought to underpin the ASIO Act warrants regime:
- Proposals to increase the scope of existing powers or their duration need to ensure that safeguards exist such that the extended scope or longer timeframes do not become the norm, and that the warrants are not unduly broad and are executed reasonably and in accordance with the specifics of the legislation as well as the overarching privacy and proportionality objectives.<sup>28</sup>

## Variation of warrants

- 4.56 The first proposal, which the Government states it wishes to progress, would allow the variation of all types of ASIO Act warrants.
- 4.57 The discussion paper explains that:
- Currently, the ASIO Act does not specifically provide for a warrant to be varied if the circumstances justify such a variation. A new warrant is required in every instance where there is a significant change in

---

27 Liberty Victoria, *Submission No. 143*, p. 3.

28 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 3.

circumstances. A variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability.<sup>29</sup>

- 4.58 NSW Young Lawyers argued that the existing requirement that a new warrant should be applied for when there is a change in circumstances should be retained as that is an important accountability mechanism:

In order to maintain accountability and ensure that an existing warrant did not endure inappropriately following a significant change in circumstances, any variation of a warrant as proposed would call for a level of accountability whereby the entire basis of the warrant would be reviewed in light of present, past and altered circumstances. This level of accountability is achieved under the existing provisions.<sup>30</sup>

- 4.59 The Law Council of Australia criticised the short description of the proposal in the discussion paper as lacking detail vital for consideration:

For example, would there be different requirements for seeking a variation of a search warrant under section 25 compared with a variation of warrant to use a listening device under section 26? Would there be different limits on the period in respect of which an existing warrant could be renewed, depending on the nature of the power to be exercised? <sup>31</sup>

- 4.60 The Attorney-General's Department was asked which warrants are intended to be varied and in what ways might those warrants be varied. The Department clarified:

It is envisaged that a general power to vary warrants could apply to all warrants under Division 2 Part III of the ASIO Act (this proposal does not cover questioning and detention warrants). A variation might be sought if there is a relatively minor change in circumstances. For example, if ASIO had a computer access warrant relating to a particular computer and also entry to the premises in which that computer is located. If the person moved house unexpectedly, before entry to the premises to access the computer occurred, the ability to request a variation to amend the address could be appropriate, as the core grounds (to access data on the target computer) would not have changed.<sup>32</sup>

---

29 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 41.

30 New South Wales Young Lawyers, *Submission No. 133*, p. 7; see also: Law Council of Australia, *Submission No. 96*, p. 67.

31 Law Council of Australia, *Submission No. 96*, p. 67; see also: New South Wales Young Lawyers, *Submission No. 133*, p. 6.

32 Attorney-General's Department, *Submission No. 236*, p. 5.

- 4.61 The Office of the Victorian Privacy Commissioner criticised what might be a potential expansion of the activities authorised by the warrant, without recourse to the issuing authority:

In my view, the level of variation required needs to be carefully considered and should be extremely limited. Courts are (rightly) vested with authority to grant warrants; allowing “operational flexibility” to vary a warrant could potentially allow extension of a warrant beyond what was authorised by a court.<sup>33</sup>

- 4.62 The Attorney-General’s Department was also asked which officer might be vested with the authority to vary the terms of a warrant. The Department responded that it would be the Attorney-General, the original issuer of the warrant:

Given that the Attorney-General issues warrants and their terms and conditions, it would seem appropriate that the Attorney-General should have the responsibility for approving the variation of warrants.<sup>34</sup>

### Committee comment

- 4.63 The Committee notes the Attorney-General’s Department contention that allowing the variation of active ASIO Act warrants is appropriate in order to ensure sufficient operational flexibility for ASIO.
- 4.64 The Committee is satisfied that the appropriate accountability would be maintained if any such variation was authorised by the Attorney-General.

---

## Recommendation 23

**The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.**

### Duration of search warrants

- 4.65 The second proposal that the Government wishes to progress relates to the duration of ASIO Act search warrants. The discussion paper elaborated that the maximum duration of search warrants could be increased from 90 days to six

---

33 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 4; see also: Ms Stella Gray, *Submission No. 152*, p. 9.

34 Attorney-General’s Department, *Submission No. 236*, p. 5.

months, making those warrants consistent with the duration of all other warrants issued under that Act.

- 4.66 The discussion paper's rationale for extending the duration of search warrants to six months is that:

... [it] would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors.

Indeed, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control, and a new warrant would be required.<sup>35</sup>

- 4.67 The proposal to increase the duration of ASIO Act warrants was subject to many of the same criticisms that the variation of ASIO warrants proposal received, namely that current arrangements serve to protect the interests of affected parties. The Castan Centre for Human Rights Law observed that:

A modest additional administrative burden is a small price to pay in return for avoiding any implication, for example, that certain persons are, by default, subject to covert intelligence surveillance.<sup>36</sup>

- 4.68 Contrary to the discussion paper's rationale, Mr Daniel Nazer asserted that the efficacy of search warrants may be better served by shorter deadlines for executing searches:

As days, weeks, or even months go by, it becomes increasingly likely that a search warrant is based on stale information. Indeed, with a deadline as long as 180 days, it is possible that an investigation might evolve to the point of exonerating a target. Thus, limited warrant durations promote privacy by ensuring that searches are conducted based on fresh, accurate information.<sup>37</sup>

- 4.69 The Attorney-General's Department was asked why the current 90 day timeframe for the execution of search warrants is inadequate. The Department explained:

ASIO operations require careful planning, and may require a high degree of flexibility as to when warrants are executed, in order to ensure access to the intelligence information and ensure protection of ASIO officers and methodology. Searches may be undertaken covertly, which may significantly limit opportunities to execute the warrant. A warrant enabling a search to take place within a six month period would provide

---

35 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p41, p. 42.

36 Castan Centre for Human Rights Law, *Submission No. 142*, p. 4.

37 Mr Daniel Nazer, *Submission No. 110*, p. 7.

operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors.<sup>38</sup>

- 4.70 The IGIS shed further light on the possible rationale of extending the duration of these warrants:

I am aware of one general category of warrants where there is sometimes difficulty executing the warrant within 90 days. To ensure the legislative response is proportionate it may be preferable to allow this particular category of search warrants to be extended rather than all search warrants.<sup>39</sup>

- 4.71 Though it was not publicly discussed what types of searches may be difficult for ASIO to execute within 90 days, the IGIS offered an alternative solution to a blanket extension of all ASIO search periods:

If that period is extended to six months then this should clearly be set as the maximum possible duration – not the default standard for all warrants. If this provision was enacted I would monitor search warrant requests closely to see whether the duration of each warrant request was considered on an individual basis to ensure it was valid for an appropriate time, which would usually be less than six months.<sup>40</sup>

- 4.72 The IGIS finally observed that there was overlap with another proposal included in the terms of reference, the ‘named person warrant’ for ASIO warrants. That concept is to create an additional form of warrant that would enable all forms of special powers to be available under the ASIO Act against a particular person. That proposal was referred to the Committee as one that the Government is considering and is discussed separately below.

- 4.73 The IGIS observed that:

...it may be that the policy reason behind the change from 90 days to 6 months is directed at administrative ease and consistency for such warrants. However my view is that administrative ease and consistency are, in themselves, not compelling reasons to increase warrant powers or extend their duration.<sup>41</sup>

- 4.74 The Attorney-General's Department responded to the IGIS's concern:

As with all ASIO warrant powers, six months would be a maximum duration. It would be open to ASIO to apply for a period shorter than six months where appropriate, or for the Attorney-General to grant a warrant

---

38 Attorney-General's Department, *Submission No. 236*, p. 3.

39 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

40 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

41 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.



with a shorter duration if an adequate supporting case for the maximum duration is not presented.

While it is possible for ASIO to reapply for a new warrant if it has not been possible to conduct the search within the 90 day period, if the search has not been conducted and the grounds remain unchanged, arguably seeking a fresh warrant does not significantly add accountability. The warrant, whether in force for 90 days or six months, still only authorises one search of the premises. There is also a requirement under section 30 of the ASIO Act for the Director-General to notify the Attorney-General and take steps to ensure that any action under the warrant is discontinued if the Director-General ceases to be satisfied that the grounds for it exist.<sup>42</sup>

### Committee comment

- 4.75 The Committee did not receive sufficient evidence to justify the proposal that the maximum duration of search warrants be increased from 90 days to six months.

### Recommendation 24

**Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.**

### Renewal of warrants

- 4.76 The third proposal that the Government wishes to progress relates to the renewal of ASIO Act warrants. The discussion paper notes that when a warrant expires, which is up to 6 months for most ASIO warrants, and there remains an ongoing need to use special powers, a new warrant must be sought from the Attorney-General by the Director-General of Security. The current provisions in the ASIO Act do not enable a warrant to be extended.
- 4.77 The discussion paper notes that certain threats to security can endure for many years and that the threats creating the need for a significant proportion of warrants continue beyond the initial authorisation periods. This means that:
- In such circumstances, ASIO must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant

---

42 Attorney-General's Department, *Submission No. 236*, p. 3.

change to either, and where the assessment of the intelligence case remains unchanged. A renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources.<sup>43</sup>

- 4.78 Liberty Victoria questioned the desirability of removing the need to obtain a new warrant:

The renewal of a warrant is not a minor matter. It extends the power of ASIO officers to interfere in the personal privacy of suspects through the interception of communications, searches of private premises, installation of listening devices, inspection of postal articles and use of tracking devices. All renewals need to be based on clear evidence of the intelligence case and reference to the legislative threshold. Such basic standards should not be regarded as “excessive” administrative requirements.<sup>44</sup>

- 4.79 Though not expressly endorsing the introduction of a renewal process *in lieu* of requiring fresh warrants when existing investigations carry on past the expiry of original warrants, the IGIS did offer comfort to the Committee that ASIO would not lower the standards expected of it when assessing which matters are investigated with intrusive powers:

My experience is that ASIO actively monitors changes in circumstances and is generally prompt in ensuring that action under a warrant is discontinued when the grounds for a warrant have ceased to exist. My understanding is that there is no intention in ASIO to reduce the scrutiny given to the intelligence case on renewal or re-issue of warrants or the ongoing monitoring of the grounds for the warrant – these essential internal assurance processes may limit the “streamlining” benefits the proposed amendment could deliver.<sup>45</sup>

- 4.80 The Gilbert + Tobin Centre of Public Law reminded the Committee that consideration of the concept of renewing warrants should also be considered in the context of the ‘named person warrant’ proposal:

We would, however, note that the criteria, especially for renewal, should not be significantly less than those for issuing a warrant in the first place. This is particularly important given the proposal to merge warrant powers into a single category of warrant. Otherwise, renewal may become

---

43 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 42.

44 Liberty Victoria, *Submission No. 143*, p. 10; see also: Castan Centre for Human Rights Law, *Submission No. 142*, p. 4; Mr M Newton, *Submission No. 87*, p. 11.

45 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 15.

a means of rolling all of the warrant powers over every six months without meaningful consideration of whether the need still exists.<sup>46</sup>

- 4.81 The Attorney-General's Department was asked what was envisaged for a renewal process for ASIO warrants and how that may differ from applying for fresh warrants. The Department replied:

It is envisaged that a renewal process would differ by enabling ASIO to present a renewal application to the Attorney-General that focuses on why it is necessary to continue the warrant and certifies that the facts and grounds specified in the original application have not changed. A simplified renewal process would provide significant administrative efficiencies for ASIO and the Attorney-General, without reducing oversight and accountability, as the Attorney-General would still need to be satisfied that the application meets the relevant threshold.<sup>47</sup>

- 4.82 Noting community concerns raised in submissions, the Attorney-General's Department also advised:

...that the criteria for renewal should not be significantly less than those for issuing a warrant in the first place. The Attorney-General could still have responsibility for renewing warrants, and the IGIS would also continue to have oversight of all warrant documentation. On that basis, the Attorney-General would only grant a renewal if satisfied that the legislative requirements continue to be met. In doing so, the decision to renew warrants would be focused on any change in circumstances from when the original warrant was issued and the appropriateness of continuing the warrant for a further period.<sup>48</sup>

### Committee comment

- 4.83 The Committee is of the view that there is merit in making the process of obtaining authority to continue the use of intrusive powers more efficient. This could be done with a form of renewal, rather than requiring ASIO to start its application afresh.
- 4.84 However, the standards and thresholds for obtaining a warrant should not be lowered for the renewal of the very same warrant. The Attorney-General ought to remain satisfied, by applying the same standards, that there is a threat that requires intrusive investigation, as they were when the original warrant or warrants were issued.

---

46 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, pp. 13-14.

47 Attorney-General's Department, *Submission No. 236*, p. 4.

48 Attorney-General's Department, *Submission No. 236*, p. 4.

## Recommendation 25

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.**

### ASIO Act employment provisions

- 4.85 The Terms of Reference to this inquiry state that the Government wishes to progress the modernisation of the ASIO Act employment provisions. ASIO officers are employed under the ASIO Act rather than the *Public Service Act 1999*. The discussion paper notes that the provisions relating to the employment of ASIO officers do not align with the Australian Public Service framework as the ASIO Act provisions have not been updated since they were originally enacted 30 years ago.
- 4.86 These proposals are:
- To delete the requirement for an ASIO employee to hold an “office” within ASIO;
  - Replacing various descriptors denoting employment within ASIO, with a single descriptor, ‘employee’, throughout the ASIO Act;
  - Repealing section 87 of the ASIO Act, which relates to employees who were employed immediately before the ASIO Act’s commencement in 1979, of whom there are no longer any employed; and
  - Secondment provisions.
- 4.87 The Committee received no evidence in relation to the first three proposals, however, they appear on their face to be of an innocuous administrative character.

### Proposed secondment arrangements

- 4.88 The Terms of Reference to this inquiry state that the Government wishes to progress amendments to the ASIO Act to ‘provide for additional scope for further secondment arrangements’. The discussion paper elaborates that this proposal is to legislate secondment arrangements for ASIO officers into other agencies and for officers from other agencies into ASIO:

In order to access specialist skills and as part of arrangements whereby ASIO works closely with other agencies, ASIO often places staff of other agencies to work within ASIO, or agrees to its staff members working in other agencies. Legal complexities can arise in making such

arrangements because of the specified scope of the functions and powers of ASIO and the other organisation involved.<sup>49</sup>

- 4.89 The discussion paper suggests that ASIO's ability to engage with other agencies would be enhanced, and administrative difficulties could be overcome if the ASIO Act expressly enabled the secondment of staff to and from ASIO. It is also proposed that, during the secondment, a seconded staff member carries out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation.<sup>50</sup> For instance, this would mean that an ASIO officer seconded to the AFP would act according to the laws and rules that apply to the AFP, rather than ASIO.
- 4.90 The Inspector-General of Intelligence and Security submitting on the secondment proposal noted that there is potential for poorly constructed secondment arrangements to create opportunities for circumventing existing statutory limitations:
- If the secondment proposal is adopted I would be looking to ensure that the changes are applied in such a way that it is clear to individual officers which agency they are undertaking an activity for and that 'secondments' are a true change in working arrangements for a reasonable period. In my view it would not be proper for such a mechanism to be used to circumvent limits placed on employees in other legislation. For example it would not be proper for an ASIS staff member to be 'seconded' to ASIO for a day or two to enable them to perform an activity that they would otherwise not be permitted to undertake. My understanding is that this is not a practice the agencies intend to adopt.<sup>51</sup>
- 4.91 The discussion paper acknowledges that there is no intention for future secondment arrangements to be used to circumvent statutory limitations on the acts that officers from particular agencies may carry out. The current requirements that allow Intelligence Services Act agencies to co-operate with ASIO would operate independently of any new secondment provisions.<sup>52</sup>

### Committee comment

- 4.92 The Committee is satisfied with the creation of new secondment provisions in the ASIO Act, provided that those arrangements cannot be used for the purpose

---

49 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 43.

50 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 43.

51 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 16.

52 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 41.

of officers of agencies circumventing existing safeguards and limitations that apply to their employment and conduct.

## Recommendation 26

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.**

### Intelligence Services Act – Clarifying the authority of the Defence Imagery and Geospatial Organisation

- 4.93 The Government wishes to clarify the authority of the Defence Imagery and Geospatial Organisation (DIGO). The discussion paper explains that minor amendments to subsection 6B(e) of the *Intelligence Services Act 2001* (IS Act) would ensure that DIGO has clear authority to undertake its geospatial and imagery functions.
- 4.94 Under the IS Act, DIGO has a number of geospatial and imagery related intelligence functions, as well as civilian functions that relate to supporting Commonwealth, State and Territory governments as well as other bodies. The discussion paper explains that minor legislative clarifications are required to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions.
- 4.95 DIGO's work under its civil assistance function may involve collecting imagery and other data in relation to locations inside and outside Australia. That work is not done for the purpose of providing information about a particular person or entity. This means that is not an intelligence-gathering function but DIGO may still utilise the same sources or capabilities that it uses for intelligence collection to perform its statutory civil assistance function.
- 4.96 The discussion paper proposes amendments to the Intelligence Services Act to avoid any doubt that DIGO is enabled to provide Commonwealth and State authorities, and other approved bodies, assistance in relation to the production and use of both non intelligence and intelligence imagery and geospatial products.<sup>53</sup>
- 4.97 The discussion paper also proposes that the IS Act be amended to include an express power for DIGO to provide specialised imagery and geospatial technologies assistance to Commonwealth, State and Territory authorities and

---

53 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

certain non-government bodies. This would include the use and application of specialised imagery and geospatial technologies, including geospatial web-based services.<sup>54</sup>

4.98 Because DIGO is an organisation that uses intelligence-gathering capabilities for both intelligence and non-intelligence functions, as well as using those capabilities to image locations within Australia and overseas, some submitters urged caution in amending the legal framework in which DIGO operates.

4.99 For example, Ms Stella Gray highlighted for the Committee that:

This would enable ASIS, DSD and DIGO to collect intelligence on Australian citizens whenever the agencies are cooperating with ASIO in the performance of its functions. This proposal does not include any provision to prevent the abuse of power by these agencies whilst working in concert. This proposal cannot be supported with the current level of accountability it demands of these agencies.<sup>55</sup>

4.100 The discussion paper explains that the safeguards that prevent possible abuses of power will remain in place:

The proposed amendments do not change the original intended operation of section 6B of the IS Act. The existing safeguards in the IS Act would remain unaffected and in place. The suggested changes involve minor clarifications to provide more certainty and practical utility. By making the legislation clearer, it would be easier for the Inspector-General of Intelligence and Security to effectively review whether DIGO is operating within its powers, and ensure accountability is maintained.<sup>56</sup>

4.101 The IGIS further elaborated on the protections that would prevent the risk of abuse of power by DIGO and the agencies and bodies that it may assist:

If such assistance was also for the specific purpose of producing intelligence on an Australian person my expectation is that DIGO would continue to be required to obtain ministerial authorisation. I also expect DIGO to continue to apply the Privacy Rules made under s. 15 of the IS Act to any disclosure of intelligence about an Australian person, regardless of which function the intelligence was collected under.<sup>57</sup>

---

54 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

55 Ms Stella Gray, *Submission No. 152*, p. 10.

56 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

57 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 23.

## Committee comment

- 4.102 The Committee agrees that the IS Act should be amended to clarify DIGO's authority to assist other agencies and bodies, provided that the existing oversight and accountability mechanisms would apply.

## Recommendation 27

**The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.**

## Matters the Government is considering

- 4.103 The second category of reform proposals are matters which the Terms of Reference state the Government is considering. These are proposals to amend the ASIO Act to:
- Create an authorised intelligence operations scheme;
  - Create a named person warrant;
  - Align the ASIO Act surveillance device provisions with the *Surveillance Devices Act 2004*;
  - Allow the Director-General of ASIO to create authorisation lists for the execution of warrants;
  - Clarify ASIO's ability to operate with the private sector; and
  - Refer breaches of the prohibition on identifying ASIO officers to law enforcement for investigation.

## Creation of an authorised intelligence operations scheme

- 4.104 The Terms of Reference state that the Government is considering amending the ASIO Act to create an authorised intelligence operations scheme. Such a scheme would provide ASIO officers and its human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.
- 4.105 The discussion paper proposes the creation of an authorised intelligence operations scheme (or controlled operations scheme) for ASIO officers, based on that currently available to certain law enforcement officers under the Crimes Act



‘with appropriate modifications and safeguards that recognise the scheme would operate in the context of covert intelligence gathering investigations or operations’.<sup>58</sup>

4.106 Existing controlled operations provisions in Commonwealth and State and Territory laws provide for the issue of authorities which provide immunity from prosecution and indemnity from civil liability for law enforcement officers and nominated civilian participants who engage in activities that would otherwise be unlawful.

4.107 The Australian Federal Police (AFP)’s Annual Controlled Operations Report for 2010-11 notes that controlled operations can be used to uncover serious illicit and organised criminal activity such as the smuggling of drugs, firearms and persons and to disband or disrupt organised criminal syndicates.<sup>59</sup>

4.108 In relation to creating an analogous scheme for ASIO, the discussion paper explains that:

An authorised intelligence operations scheme would significantly assist covert intelligence operations that require undercover ASIO officers or human sources to gain and maintain access to highly sensitive information concerning serious threats to Australia and its citizens.<sup>60</sup>

4.109 The discussion paper also provides that:

Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility and appropriate oversight and accountability. Key features that may contribute to such could include:

- the Director-General of Security to issue authorised intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months);
- oversight and inspection by the IGIS, including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General;
- specifying conduct which cannot be authorised (for example, intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person), and

---

58 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 46.

59 AFP, *Controlled Operations annual Report 2010-2011*, viewed 12 November 2012, <[www.afp.gov.au/media-centre/publications/~media/afp/html/controlled-operations-annual-report-2010-2011.ashx](http://www.afp.gov.au/media-centre/publications/~media/afp/html/controlled-operations-annual-report-2010-2011.ashx)>.

60 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 46.

- independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement.<sup>61</sup>

4.110 The potential creation of an authorised intelligence operations scheme raised a number of criticisms in submissions and at hearings.

4.111 Dr Patrick Emerton of the Castan Centre for Human Rights Law at Monash University drew an important distinction between ASIO and traditional law enforcement agencies such as police forces. Dr Emerton contended that ASIO:

...is not a law enforcement agency and is not accountable through the criminal trial process in the way that a law enforcement agency is, and it is therefore not governed by the very strict chapter 3 [of the *Constitution*] jurisprudence that governs the behaviour of law enforcement agencies under our constitutional law. It is in a very different constitutional position, a very different administrative position and a very different policy position, and it is essentially secret.<sup>62</sup>

4.112 The IGIS questioned why ASIO's existing relationships with law enforcement agencies could not be utilised to take advantage of the existing controlled operations regimes:

I am aware that over a period of some years my office has received a small number of complaints from current and former ASIO human sources that demonstrate the complexity of the relationship. The paper does not explain why ASIO could not request the AFP or ACC to use existing powers to perform these functions, including where necessary authorising ASIO officers or sources under the existing schemes.<sup>63</sup>

4.113 The Attorney-General's Department was asked if ASIO would be able to rely on the AFP to conduct controlled operations on its behalf. The Department contended that it would not always be possible:

While there might be some capacity to utilise this scheme in joint counter-terrorism investigations, ASIO security intelligence operations extend across the range of national security matters within the ASIO Act. Some operations may cover matters not normally the subject of criminal investigations, such as foreign interference. Similarly, ASIO may be involved at a stage where there would not be sufficient grounds for law enforcement to investigate the possible commission of an offence.<sup>64</sup>

---

61 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, pp. 46-47.

62 Dr Patrick Emerton, Castan Centre for Human Rights Law, *Transcript*, Melbourne, 5 September 2012, p. 21; see also NSW Council for Civil Liberties, *Submission No. 175*, p. 13; Law Council of Australia, *Submission No. 96*, p. 58.

63 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 18.

64 Attorney-General's Department, *Submission No. 236*, p. 6.

- 4.114 The Gilbert + Tobin Centre of Public Law argued that it would not be necessary to create an indemnity scheme for ASIO as it would be unlikely that ASIO officers would be prosecuted for crimes committed in the course of their duties because the Commonwealth Director of Public Prosecutions has a discretion whether or not to prosecute individuals for terrorism and other offences:

It is highly unlikely that an ASIO officer would be prosecuted for activities done in the course of an undercover operation.<sup>65</sup>

- 4.115 The Attorney-General's Department argued that ASIO would not be able to rely on prosecutorial discretion, even where it was available:

While a general prosecutorial discretion is available, decisions on whether to pursue a prosecution are determined on a case-by-case basis by the relevant Director of Public Prosecutions. It is not normal practice for the Director of Public Prosecutions to give advance indemnities or immunities from future prosecution. In addition, there is no equivalent mechanism to provide indemnity from civil proceedings.<sup>66</sup>

### Committee comment

- 4.116 The Committee received evidence that there are occasions on which ASIO officers and sources are placed in positions where, in order to carry out their duties, they may need to engage in conduct which may, in ordinary circumstances, be a breach of the criminal law. The Committee understands that such occasions would be seldom but may from time to time arise. The Committee also understands that it will not be possible for ASIO to rely on the existing framework under which the AFP operates.
- 4.117 The Committee is therefore of the view that the ASIO Act should be amended to create a controlled intelligence operations scheme.
- 4.118 The discussion paper suggests particular restrictions, reporting and accountability mechanisms. The Committee agrees that an ASIO authorised intelligence operations scheme should be subject to strict accountability and oversight.
- 4.119 The Committee supports the adaptation of the procedures and safeguards in the *Crimes Act 1914* that apply to the AFP's controlled operations. This would mean that ASIO officers and agents would be exempted from criminal and civil liability only for certain authorised conduct.
- 4.120 The Committee expects that unreasonable or reckless conduct would not be indemnified by an authorised intelligence operation, and the ASIO officer or source would be liable for such conduct.

---

<sup>65</sup> Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 16.

<sup>66</sup> Attorney-General's Department, *Submission No. 236*, p. 6.

## Recommendation 28

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.**

### Named person warrants

4.121 The Government is considering amending the ASIO Act to establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target, instead of requesting multiple warrants against a single target.

4.122 The discussion paper explains that:

In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types, which is administratively burdensome.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.<sup>67</sup>

4.123 As noted above, ASIO Act warrants are issued by the Attorney-General at the request of the Director-General of Security.

4.124 The different types of warrants involve different activities and consequently different levels of intrusiveness. In addition, the precise matters in respect of which the Attorney-General must be satisfied vary depending on the power to be exercised under the warrant.

4.125 The warrants are also required to specify the particular activities or things that are authorised in the particular circumstances.

4.126 The notion that the different types of warrants with their different powers could be combined into a single type raised several issues with submitters.

---

<sup>67</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 45.

- 4.127 The Castan Centre for Human Rights Law objected to the asserted benefit of reducing administrative burdens, arguing that:

Administrative burden is a small price to pay in order to preserve a regime which creates a strong presumption against the permissibility of covert intelligence intrusion into people's affairs.<sup>68</sup>

- 4.128 The Attorney-General's Department was asked if there are any benefits, beyond administrative convenience, in creating a named person warrant that would enable all ASIO powers to be used against a single target. The Department explained that efficiency could be introduced without weakening accountability:

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all powers proposed to be used against the target where the relevant legislative thresholds are satisfied. The proposal is intended to cover various warrant powers in Division 2 of Part III other than foreign intelligence collection warrants, and it would not include questioning or questioning and detention warrants.<sup>69</sup>

- 4.129 The Law Council of Australia noted that the current warrant processes require the Attorney-General to consider the use of each power separately, which allows the Attorney-General to consider the particular nature of the power to be exercised, the benefit this is likely to have to the collection of intelligence relevant to security and that:

This type of assessment would be made significantly more difficult if a single warrant covering multiple powers were introduced.<sup>70</sup>

- 4.130 The Attorney-General's Department countered that:

Arguably, a named person warrant could enhance the Attorney-General's assessment of the appropriateness of the use of particular powers against a single person when issuing a warrant, and whether the use of a particular power or number of powers will assist ASIO in obtaining intelligence relevant to security.<sup>71</sup>

- 4.131 The Inspector-General of Intelligence and Security (IGIS) questioned how the Government intends to reconcile the different tests and thresholds for the different warrants into a combined warrant. The IGIS further asked if there was an intention to shift the decision-making process for which powers would be exercised from the Attorney-General, to the Director-General of ASIO:

---

68 Castan Centre for Human Rights Law, *Submission No. 142*, p. 4.

69 Attorney-General's Department, *Submission No. 236*, p. 11.

70 Law Council of Australia, *Submission No. 96*, p. 70.

71 Attorney-General's Department, *Submission No. 236*, p. 11.

While such a scheme might be administratively simpler, there is the risk that the warrant would authorise activities that were not proportionate to the threat to security and may shift the balance between what is currently authorised by the Attorney-General and what is authorised by the Director-General.<sup>72</sup>

- 4.132 The Attorney-General's Department, being aware of the IGIS' concern, explained:

It is important to note that it is not proposed that a named person warrant would provide a blanket authority for ASIO to use any special power. The warrant would need to specify which powers are covered and the use of each power would need to be justified and meet the relevant legislative threshold. It is not intended that this proposal will weaken any of the thresholds.<sup>73</sup>

### Committee comment

- 4.133 The Committee received evidence that there would be a benefit to ASIO and to the Attorney-General in being able to issue a single warrant to authorise the use of multiple powers, over one person, for the same investigatory purpose.
- 4.134 The Committee notes that this proposal does not intend to weaken any of the thresholds for the use of the various special powers.
- 4.135 The Committee has been advised that it is not proposed that a named person warrant would provide a blanket authority for ASIO to use any special power and that the Attorney-General will have to decide which particular powers will be covered by each warrant.
- 4.136 In classified evidence a case was made supporting the establishment of a named person warrant. While it is the preference of the Committee wherever possible not to rely on classified evidence, in this instance it has been unavoidable. While the classified evidence was sufficient to give in principle support to the proposal, the Committee believes that further examination is necessary.

---

72 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 19.

73 Attorney-General's Department, *Submission No. 236*, p. 11.

## Recommendation 29

**The Committee recommends that should the Government proceed with amending the *Australian Security Intelligence Organisation Act 1979* to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.**

### Surveillance devices – use of optical devices

- 4.137 The Government is considering amending the ASIO Act to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004* (SD Act).
- 4.138 The discussion paper notes that the ASIO Act provisions governing ASIO's capabilities with respect to electronic surveillance have not been updated to align with legislation governing the use of electronic surveillance by law enforcement. The discussion paper proposes aligning the surveillance device provisions in the ASIO Act with the more modern SD Act, which provides for warrants for the use of surveillance devices by the Australian Federal Police, the Australian Crime Commission and the Australian Commission for Law Enforcement Integrity.
- 4.139 The Attorney-General's Department was asked on notice for further information on the purpose of aligning the two pieces of legislation. The Department explained how the ASIO Act provisions had fallen behind the equivalent provisions for law enforcement agencies:

For example, ASIO's ability to use optical surveillance devices is tied to its ability to use listening devices. This is a relic of the time in which the ASIO Act was first drafted. Additionally, the administrative and procedural provisions governing the use of listening and tracking devices in the ASIO Act are not aligned with provisions governing the use of surveillance devices by law enforcement. Some of the differences where alignment is proposed would be:

- addressing the lack of a separate optical surveillance device warrant
- the provision of a single surveillance device warrant
- the ability to adapt new future technologies by allowing surveillance devices to be prescribed in regulation, and
- clarifying that certain surveillance devices may be used in limited circumstances without a warrant (for example, the use of an optical

device that does not involve entry onto premises without permission or interference without permission of any vehicle or thing).<sup>74</sup>

4.140 The Inspector-General of Intelligence and Security commented that:

If the proposal is only to modernise the language of the ASIO Act – which for example rather confusingly includes a device for recording images within the definition of a ‘listening device’ – then this is a more focussed proposal that does not raise propriety concerns<sup>75</sup>.

### Committee comment

4.141 The Committee did not receive any evidence contradicting the IGIS and AGD evidence. Consequently, there is no apparent reason to doubt the desirability of aligning those two pieces of legislation.

### Recommendation 30

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the warrant provisions to align the surveillance device provisions with the *Surveillance Devices Act 2004*, in particular by optical devices.**

### Person searches

4.142 The Terms of Reference state that the Government is considering amending the ASIO Act to enable person searches to be undertaken independently of a premises search.

4.143 The ASIO Act currently contains the power to search a premises. That power also contains a further power to search a person who is at or near the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to the security matter.

4.144 The discussion paper explains that:

Where ASIO assess that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched. However, it is not always feasible to execute a search warrant on a person of interest while they are ‘at or near’ the premises specified in the warrant.<sup>76</sup>

74 Attorney-General’s Department, *Submission No. 236*, p. 9.

75 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20.

76 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.



4.145 The existing limitation leads to a practical problem that:

For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible.<sup>77</sup>

4.146 When answering a question about the purpose of enabling person searches to be undertaken independently of a premises search, the Attorney-General's Department gave a more detailed example of where a person search could be executed away from a specified premises:

As noted in the discussion paper, the sort of scenario where power to search a person might be relevant is where a foreign agent is passing security relevant material to someone in a public space, such as a park.<sup>78</sup>

4.147 The discussion paper proposes that that problem could be addressed by enabling ASIO to request a warrant to search a specified person rather than premises so that there would be 'sufficient operational flexibility' while maintaining appropriate accountability via the warrant process.

4.148 The discussion paper also suggests that the existing safeguard that ASIO Act search warrants do not authorise a strip search or a search of a person's body cavities will remain in place.<sup>79</sup>

4.149 The IGIS noted that this proposal is better described, not as an extension of the existing power to search premises, but is rather a proposal to introduce a new class of warrant. The IGIS argued, therefore, that it is important to carefully consider of the restrictions and conditions that should apply to the new warrant:

I am aware of one category of activities where ASIO currently relies on premises search warrants to achieve what is in effect a person search. While I do not have concerns about the legality of the current approach, from an oversight and transparency perspective it would be preferable for the legislation to provide a specific mechanism for person searches with appropriate limits rather than using a premises search warrant for this purpose.

Care needs to be taken that those undertaking a person search have appropriate training and qualifications. To this end it may be preferable to require that, where possible, such searches are undertaken by law enforcement officers who have specific training in this regard.<sup>80</sup>

---

77 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

78 Attorney-General's Department, *Submission No. 236*, p. 10.

79 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

80 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 20

- 4.150 The search power proposal was criticised in a number of submissions, including the acting Victorian Privacy Commissioner:

I consider an alteration of the warrant procedure in such a fashion to be extraordinarily broad and intrusive. It would have a serious adverse impact on an individual's privacy, may unduly infringe a number of human rights and freedoms (such as the freedom from arbitrary search and seizure), and interfere with the privacy of one's home and family. In particular, despite the safeguards in place, there is a possibility of using a person search to repeatedly harass a target at multiple locations (eg work, home, in a public space etc).<sup>81</sup>

- 4.151 In response, the Attorney-General's Department explained that the person search proposal would not lead to a series of searches or the possibility of ASIO harassing suspects:

ASIO would only be able to conduct one search per warrant and could not use the warrant to harass the target at multiple locations. This proposal is not recommending ASIO be given stop and search powers, such as those available to police in some circumstances.<sup>82</sup>

- 4.152 Liberty Victoria submitted that allowing the search of people away from pre-determined premises could be disruptive to the lives of searched people if they were to be searched in public spaces and offered that:

While we recognise that the current 'at or near' requirement poses operational challenges, we believe that the appropriate solution lies with operational tactics, not with legislative amendment.<sup>83</sup>

- 4.153 The Castan Centre for Human Rights Law submitted that ASIO's existing search warrant power remains controversial and that search powers should only be granted to police:

If individuals are suspected of committing criminal offences there is already ample provision under state and Commonwealth law for police officers to exercise powers of arrest and/or search. Steps should not be taken which would give ASIO even the hint of the character of a secret police force.<sup>84</sup>

- 4.154 The Gilbert + Tobin Centre for Public Law agreed that search powers are better delegated to police forces than to an intelligence agency but suggested means to mitigate their existence:

---

81 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 5.

82 Attorney-General's Department, *Submission No. 236*, p. 10.

83 Liberty Victoria, *Submission No. 143*, p. 12.

84 Castan Centre for Human Rights Law, *Submission No. 142*, pp.4-5; see also: Law Council of Australia, *Submission No. 96*, p. 58.

However, in the event that a separate category of person search warrant is established, ASIO searches must be accompanied by similar safeguards as apply to searches by law enforcement officers. If not, there is a risk that ASIO searches will be used as a means of circumventing the safeguards attaching to law enforcement searches.<sup>85</sup>

- 4.155 The Attorney-General's Department elaborated on the safeguards that might apply if ASIO was allowed to conduct these searches independent of particular premises:

The existing safeguards that apply to searching a person when on a premises would also continue to apply, including:

- Not authorising a strip search or a search of a person's body cavities.
- Where practicable, the search must be carried out by a person of the same sex as the person being searched.
- Key requirements in the ASIO Guidelines that are relevant would be the requirement of proportionality, to use the least intrusive powers where possible, and the need to have regard to the cultural sensitivities, values and mores of certain persons.
- ASIO has internal policies, procedures and training requirements that relate to the proper conduct of searches.
- The exercise of this power, as with all ASIO's powers, would be subject to oversight by the IGIS.<sup>86</sup>

### Committee comment

- 4.156 The Committee is very mindful of the importance of maintaining the clear distinction between intelligence and law enforcement. ASIO is not a law enforcement agency; it is an intelligence agency. Its statutory charter makes this clear. The Committee has serious misgivings about whether this power would take ASIO into the realm of law enforcement and policing. As well, we note that ASIO did not, upon inquiry, press for this power.

### Recommendation 31

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.**

<sup>85</sup> Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 13. See also: Tasmanian Association of Community Legal Centres, *Submission No. 184*, p. 4.

<sup>86</sup> Attorney-General's Department, *Submission No. 236*, p. 10.

## Authorisation lists for warrants

- 4.157 The Government is considering amending the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to establish classes of persons able to execute warrants.
- 4.158 Section 24 of the ASIO Act provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of this section) may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act.
- 4.159 The discussion paper explains that the requirement to maintain a list of the individual names of employees who may be involved in executing a warrant can create operational inefficiencies for ASIO. For example, sometimes the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to quickly expand the list of authorised persons.<sup>87</sup>
- 4.160 The discussion paper proposes that:
- The problem could be overcome in large part if the Director-General could approve classes of people to execute a warrant. For example, the Director-General could authorise officers of a certain level within a particular Division of ASIO. Such persons at any one time would be readily ascertainable ensuring the level of accountability is not diminished, while improving operational efficiency.<sup>88</sup>
- 4.161 The proposal to alter authorisations from specific named individuals to classes of people received limited public comment. Mr Mark Newton, submitting in a private capacity, stated:
- I have no objection to authorisation lists for warrants, provided the persons on the authorisation lists would otherwise qualify as officers and employees able to execute warrants under the current version of Division 2 of Part III of the ASIO Act.<sup>89</sup>
- 4.162 Arguing in the contrary, the Law Council of Australia was of the view that specifically naming particular officers within ASIO offered an accountability benefit:
- For the Law Council, moving beyond the existing level of flexibility to allow the Director-General to authorise a list of persons based on a certain level within a particular Division of ASIO would tip the balance too far in favour of operational efficiency, and away from the need to strictly regulate the use of these intrusive and extraordinary powers. As noted
- 

87 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 49.

88 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 49.

89 Mr Mark Newton, *Submission No. 87*, p. 12.

elsewhere in this submission, improving operational efficiency, while a worthy goal, is not of itself enough to justify an expansion of powers or in this case, a dilution of important safeguards.<sup>90</sup>

- 4.163 The Inspector-General of Intelligence and Security, who would be empowered to carry out that oversight function was of the view that:

While this could be operationally effective, it would be essential for ASIO to ensure that all officers in a particular class were fully trained and understood the limits of their authorisation. As noted above in relation to [person search warrants] there may be cases where the best qualified officers to conduct a particular search are law enforcement officers.<sup>91</sup>

- 4.164 Telstra advised that telecommunications industry participants that carry out interception activities on behalf of ASIO would need to be kept advised of which individual officers fall within the proposed classes in order to ensure that the industry participants can remain fully aware of which officers are in fact so authorised:

Telstra agrees that the classes of persons who are eligible to execute a warrant will need to be clearly defined as to what types of warrants they can authorise and under what law. Careful consideration will also need to be given to the appropriate levels of oversight and record keeping. A list of persons will then need to be conveyed to C/CSPs to reduce any risk of harm, unauthorised interception or breaches of customer privacy by persons who are not eligible to execute a warrant.<sup>92</sup>

### Committee comment

- 4.165 It is not clear what benefit there is in maintaining the current requirement to specifically name ASIO officers who are authorised to execute warrants. Allowing the Director-General of ASIO to delegate those functions to a class of people appears sensible.
- 4.166 The Committee accepts the rationale for moving to authorising ASIO officers by position rather than specific name.

---

<sup>90</sup> Law Council of Australia, *Submission No. 96*, p. 73; see also: New South Wales Young Lawyers, *Submission No. 133*, p. 9.

<sup>91</sup> Inspector-General of Intelligence and Security, *Submission No. 185*, p. 21.

<sup>92</sup> Telstra, *Submission No. 189*, p. 14.

## Recommendation 32

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.**

### Clarifying ASIO's ability to co-operate with private sector

4.167 The Terms of Reference to this inquiry state that the Government is considering amending the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to clarify ASIO's ability to co-operate with the private sector.

4.168 The ASIO Act enables ASIO to cooperate with authorities of the Commonwealth and States and Territories where it is necessary or conducive to the functions of ASIO. However, it is unclear whether the Act implies that ASIO should not cooperate with organisations outside of government.

4.169 The discussion paper explains that it is conducive to ASIO's functions to cooperate with the private sector as the private sector plays a role in Australia's national security, including by owning and operating a significant proportion of Australia's critical infrastructure. ASIO's Business Liaison Unit provides an interface between Australian business and the Australian Intelligence Community by providing security reporting that can be used for private sector risk management.<sup>93</sup>

4.170 Consequently, the discussion paper suggests it may be desirable to amend the ASIO Act to avoid any doubt about ASIO's ability to cooperate with the private sector.

4.171 Despite ASIO already interacting with some elements of the private sector on critical infrastructure matters, the Australian Privacy Foundation disagreed that ASIO should be able to co-operate with the private sector:

The Committee should express serious concern about the continued trend to enlist corporations as part of the national security apparatus. All responsibilities of corporations and individuals must be explicit and clear at law and not subject to discretionary interpretation by law enforcement and national security agencies of rubbery clauses that permit or require "cooperation".<sup>94</sup>

4.172 Conversely, Mr Ian Quick, submitting in a private capacity, agreed as to the need for ASIO to co-operate with private sector entities:

<sup>93</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 49.

<sup>94</sup> Australian Privacy Foundation, *Submission No. 162*, p. 10.

There is no doubt that ASIO should be able to cooperate with the private sector, the big issue is on what basis, with what oversight, what permissions it requires (or should require) on a case by case basis, etc etc.<sup>95</sup>

- 4.173 Oversight of ASIO's co-operation with private sector entities by the IGIS would be one of the oversight mechanisms that would give the Committee comfort. Indeed, the IGIS offered as much in her submission:

My office regularly inspects the files of ASIO's interactions with, for example, State law enforcement agencies. We also have the ability to review ASIO's cooperation with private sector entities if appropriate.<sup>96</sup>

### Committee comment

- 4.174 ASIO's co-operation with private sector organisations is clearly necessary given that so much of Australia's critical infrastructure is controlled and secured by the private sector. There is a clear public interest in the Government, through its security intelligence agency, to advise on security threats to all parties that are involved in providing critical infrastructure.
- 4.175 The Committee offers support to amending legislation to give ASIO a clear mandate to co-operate with the private sector.
- 4.176 The Committee appreciates that there are issues of confidentiality likely to arise in dealing with the private sector. The Committee has an open mind as to whether those confidentiality issues should be addressed by legislation or administrative arrangements. The Committee recommends that the Government clarify the types of information that would be shared and what handling and dissemination limitations would apply in legislation. For example, creating similar limitations for co-operating with the private sector as currently exist for ASIO's co-operation with various government bodies.

### Recommendation 33

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.**

<sup>95</sup> Mr Ian Quick, *Submission No. 95*, p. 12.

<sup>96</sup> Inspector-General of Intelligence and Security, *Submission No. 185*, p. 21

## Identifying ASIO officers

- 4.177 The Terms of Reference to the Inquiry state that Government is expressly seeking the views of the Committee on Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.
- 4.178 The discussion paper explains that section 92 makes it an offence for a person to publish the identity of an ASIO officer. The offence is punishable by 12 months imprisonment.
- 4.179 However, section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their association with ASIO. In particular, information may only be passed to law enforcement agencies in relation to a 'serious crime' (defined as an offence punishable by imprisonment exceeding 12 months).
- 4.180 Because the ability to pass information to law enforcement only applies if the maximum penalty for an offence *exceeds* 12 months and the maximum penalty for the section 92 offence is precisely 12 months, ASIO is therefore precluded from passing information about the possible commission of this offence to law enforcement agencies.
- 4.181 The Committee received limited comment on this particular proposal. Ms Stella Gray, submitting in a private capacity, objected to the existence of section 92 in its current formulation:

Under The ASIO Act 1979 it is a serious offence to publicly identify ASIO officers or agents, which means detainees are unable to take ASIO or one of its officers to court for torture prolonged interrogation and other abuses.<sup>97</sup>

- 4.182 Similarly, Mr Mark Newton contended that the ASIO Act should be amended to allow for identifying ASIO officers in limited circumstances:

I object to section 92 in its current form. There have been times in recent history when it would be in the public interest to identify ASIO officers, specifically those who are likely to be involved in criminal acts. I would not support any strengthening of section 92 unless and until it is amended to include a workable public interest exception.<sup>98</sup>

## Committee comment

- 4.183 The Committee agrees that there is a need to allow ASIO to refer breaches of section 92 to law enforcement for investigation.

---

97 Ms Stella Gray, *Submission No. 152*, p. 8.

98 Mr Mark Newton, *Submission No. 87*, p. 12.



- 4.184 Regarding the idea of a public interest defence for identifying ASIO officers, the Committee foresees a significant risk in allowing for the identification of ASIO officers. Because of the inherent secrecy of ASIO's work, it is necessary to keep each officer's association with ASIO secret. If that secrecy is breached and an ASIO officer's identity is disclosed then their career is effectively finished. In some cases there may be risks to the safety of an officer due to unauthorised disclosure of their identity.
- 4.185 Allowing a public interest defence for disclosure of an ASIO officer's identity leads to the dilemma that an ASIO's officers identity would be disclosed with the negative consequences effective immediately. However, the public interest of exposing an ASIO officer's identity, if any, would not be determined until a much later date.
- 4.186 For these reasons the Committee does not support a mechanism that would allow for the disclosure of an ASIO officer's identity.

### Recommendation 34

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.**

## Matters on which the Government expressly seeks the Committee's views – ASIO Act amendments

- 4.187 The third category of proposals is those that the Government expressly seeks the views of the Committee. The proposals are to amend the ASIO Act to:
- Allow for the incidental entry onto premises while executing warrants;
  - Clarify when force can be used in the execution of warrants; and
  - The creation of an evidentiary certificates regime for some ASIO warrants.

### Incidental entry onto premises

- 4.188 The Government expressly seeks the views of the Committee on amending the ASIO Act to clarifying that the 'incidental power in the search warrant provision authorises access to third party premises to execute a warrant'.
- 4.189 The discussion paper elaborates that:
- Sections 25 and 25A of the ASIO Act currently enable an officer, in the execution of a search or computer warrant, to do any thing that is reasonably incidental to the exercise of powers under that warrant. It is

not clear whether this incidental power includes entry to a third party's premises for the purposes of executing the search or computer warrant. Additionally, it may be necessary to enter a third party premises for the purposes of installing a surveillance device. Clarification of the scope of the incidental power would assist ASIO in executing search and computer warrants.<sup>99</sup>

- 4.190 Repsonses to the proposal were not welcoming. Mr Mark Newton argued against allowing for incidental entry onto premises:

I absolutely do not support the Incidental Entry proposal. If ASIO wants to gain access to a premises, it should get a warrant. If it then becomes apparent that they need access to a different premises, they should get a different warrant. If they can't justify the second warrant, they shouldn't enter the premises. It's that simple.<sup>100</sup>

- 4.191 Similarly, NSW Young Lawyers highlighted important issues that the discussion paper did not address in the description of the proposal:

The proposal does not specify which third parties could be covered by such a power, whether there would be limits of proximity or otherwise in this respect. The proposal does not specify whether a warrant or any other kind of formal procedure would be necessary to enable ASIO to exercise the proposed powers.<sup>101</sup>

- 4.192 The Office of the Victorian Privacy Commissioner highlighted the human rights risks that an incidental entry proposal might raise if not properly confined and authorised by law:

Any encroachment into the privacy of a person's domicile should be treated seriously and should only occur when absolutely necessary. This is an essential principle of human rights law, mentioned in the *International Covenant on Civil and Political Rights* (Article 17), which states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.<sup>102</sup>

- 4.193 The Attorney-General's Department was asked why ASIO would need an additional power to be able to enter premises that are not related to the premises of the target person. The Department explained that the intent of the proposal was to clarify the current operation of ASIO's ability to do anything that is reasonably incidental to the exercise of powers under that warrant:

99 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

100 Mr Mark Newton, *Submission No.87*, p. 13. See also: Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 6.

101 New South Wales Young Lawyers, *Submission No. 133*, p. 8.

102 Office of the Victorian Privacy Commissioner, *Submission No. 109*, p. 6.

When executing search warrants, it may occasionally be necessary for ASIO officers to enter third party premises to access or exit the target premises. This may be because there is no other way to gain access – such as where the target premises are in an apartment block and entry is through common areas or adjoining premises – or due to ‘emergency’ and unforeseen circumstances – such as when the target person unexpectedly returns to the premises during the search.

The incidental power in the warrant provisions is currently relied on where it is necessary to access third party premises. However, it would be preferable to specifically deal with the circumstances that ASIO may be permitted to access third party premises, to provide greater clarity about the detail of the authorisation.<sup>103</sup>

- 4.194 The Department further explained that entry onto third party premises would authorise entry where consent could not be obtained:

It is ASIO’s practice to approach the owner of the third party premises to seek their consent to access the premises for the purposes of executing the warrant where possible. The proposed amendment is designed to ensure clear legal authority to enter a third party premises in those circumstances where doing so is necessary but where it is not possible to obtain consent to do so, including in an ‘emergency’ situation where access to third party premises may be necessary to avoid detection.<sup>104</sup>

### Committee comment

- 4.195 The Committee shares community concerns that the existing incidental entry power might lead to arbitrary interference with an innocent person’s home or property. It is not desirable that any agency should be given an unfettered discretion to intrude into places that are not the subject of lawful investigation purely because of a geographical coincidence in being located close to a premises of interest.
- 4.196 However, on balance, the Committee appreciates that there may be a need for incidental entry onto premises to give effect to ASIO warrants in some limited circumstances, particularly unforeseen or emergency situations.
- 4.197 The Committee accepts that the proposal as clarified by the Attorney-General’s Department would not lead to the arbitrary interference with an innocent person’s home or property as the scheme is intended to operate with requirements of proportionality and using as little intrusion into privacy as possible.

---

103 Attorney-General’s Department, *Submission No. 236*, p. 8.

104 Attorney-General’s Department, *Submission No. 236*, p. 8.

## Recommendation 35

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.**

### Use of force

- 4.198 The Government expressly seeks the views of the Committee on amending the ASIO Act to allow reasonable force to be used at any time during the execution of a warrant, not just on entry.
- 4.199 The discussion paper notes that the ASIO Act allows the use of force in the execution of search, computer access and tracking device warrants but that the legislative drafting of headings to those provisions suggest that force may only be used to facilitate entry to target premises. The paper notes that, contrarily, the substantive bodies of the warrant provisions are not so limited. It is suggested that technical legislative amendments may be necessary to correct those drafting anomalies.<sup>105</sup>
- 4.200 The Attorney-General's Department explained that confusion over the limits of ASIO's use of force came about as unintended consequences of amendments to other legislation:

A number of the ASIO warrant provisions provide that ASIO may be authorised to 'use any force that is necessary and reasonable to do the things specified in the warrant' (subsections 25(7), 25A(5A), 26B(4) and 26C(4)). These provisions are found under headings relating to 'authorisation of entry measures'. In light of changes made in 2011 to section 13 of the *Acts Interpretation Act 1901*, the headings form part of the ASIO Act. However, the terms of the use of force provision are not stated so as to limit the use of force to enter the premises. At the time these subsections were inserted into the ASIO Act, in 1999 and 2005, there does not appear to have been an intention to limit the use of force to entry, as headings were specifically excluded from the Act at that time.<sup>106</sup>

<sup>105</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 48.

<sup>106</sup> Attorney-General's Department, *Submission No. 236*, p. 12.

4.201 The Human Rights Law Centre in its submission argued:

The Government's proposal to allow ASIO to use reasonable force at any time during the execution of a warrant, not just on entry, may raise concerns in relation to the right of liberty and security of person, which is enshrined in article 9 of the ICCPR.<sup>107</sup>

4.202 The Human Rights Law Centre further argued that to address human rights concerns about the use of force, the law should be carefully framed:

A human rights-based approach to the use of force can be characterised as requiring the state to act in the three stages involved in the use of force:

- before the use of force – putting in place systems to protect human rights and avoid or minimise resort to force, such as proper policies and training;
- during the use of force – requiring that force be used in a proportionate way; and
- after the use of force – ensuring that there are accountability mechanisms in place to hold agents of the state to account for their use of force.<sup>108</sup>

4.203 To understand the impact of this proposal the Attorney-General's Department was asked on notice about the circumstances it envisaged that reasonable force may be used during the execution of a warrant. The Department explained:

In addition to the possible need to use force to enter a premises, it may be necessary to use force to obtain access to a locked room or locked cabinet, or to use force to install or remove a surveillance device. The proposal is intended to ensure the power to use any force that is necessary and reasonable to do the things specified in a warrant is not read down by reference to the heading and limited to entry.

The existing provision requires that the use of force must be reasonable and necessary to do what is required to execute the warrant. The ASIO Guidelines requirement of proportionality and using as little intrusion into privacy as necessary are also relevant safeguards in this context.<sup>109</sup>

## Committee comment

4.204 The Committee is of the view that ASIO's power to use reasonable force during the execution of a search warrant should extend to all of the acts undertaken for the purpose of the execution of the warrant, not just on entry to the premises. If there is any doubt about the existence of that power, that doubt should be removed. The Committee emphasises that the purpose of this proposal is not to

---

<sup>107</sup> Human Rights Law Centre, *Submission No. 140*, p. 8.

<sup>108</sup> Human Rights Law Centre, *Submission No. 140*, p. 8.

<sup>109</sup> Attorney-General's Department, *Submission No. 236*, p. 12.

authorise the use of force against a person, but against property in order to facilitate the conduct of the search.

### Recommendation 36

**The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.**

### Evidentiary certificates

- 4.205 The Government has requested the Committee's advice on whether an evidentiary certificate regime should be introduced to protect the identities of officers and sensitive capabilities of ASIO involved in the execution of warrants under the ASIO Act.
- 4.206 The discussion paper proposes that the evidentiary certificate regime would be similar to those which exist under the TIA Act and *Surveillance Devices Act 2004*. This would avoid the need for ASIO to rely upon public interest immunity claims or orders obtained under the *National Security Information (Criminal and Civil Proceedings) Act 2004*.
- 4.207 The purpose of evidentiary certificates is to protect sensitive information, sensitive capabilities and the identities of individuals from public disclosure.
- 4.208 The Gilbert + Tobin Centre for Public Law was of the view that evidentiary certificates would be appropriate for ASIO warrants that authorise powers that are technological in nature:

We accept that it would be appropriate to adopt a similar evidentiary certificate regime in respect of *some* of the warrant powers in the *ASIO Act*. That is, those warrant powers which are technological in nature.<sup>110</sup>

- 4.209 Noting that evidentiary certificates are already issued under the *Telecommunications (Interception and Access) Act 1979* for the same purposes of protecting sensitive capabilities and the identities of people involved in interception activities, NSW Young Lawyers highlighted the acceptable limits that evidentiary certificates should be allowed:

The evidentiary certificate provision(s) sought to be introduced should not be drafted in a way that prevents a defendant from challenging the

<sup>110</sup> Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 15. See also: New South Wales Young Lawyers, *Submission No. 133*, p. 13 and NSW Council for Civil Liberties, *Submission No. 175*, p. 17.

accuracy of anything said or relied on in the intercepted communication. Furthermore the certificate should not operate to preclude a defendant from being able to provide evidence inconsistent with the Crown's case in respect of the interception, or indeed any evidence that would undermine a fact in a certificate. Importantly the evidentiary certificate should not operate to preclude the operation of s 137 of the Evidence Act, which would apply where the probative value of a certificate is outweighed by the unfair prejudice it would cause to a defendant. It may be that an evidentiary certificate goes to the exercise of the court's discretion in this regard, but there will be other factors influencing the exercise of the court's discretion. Although national security will be carefully considered by the court, a certificate in this context should not be able to dictate an outcome in the face of inconsistent or doubtful evidence.<sup>111</sup>

### Committee comment

- 4.210 The Committee agrees that there is a legitimate need to protect the technological capabilities of ASIO when information under warrant is eventually led in evidence as part of a prosecution. Evidentiary certificates issued under the TIA Act have been proven to effectively protect capabilities without prejudicing the rights of defendants to a fair trial.
- 4.211 With that being said, there ought to be a limit to the extent to which those evidentiary certificates can be utilised. The Committee does not think it appropriate that ASIO evidentiary certificates be used to prove, without challenge, the material facts in question.
- 4.212 This would mean that evidentiary certificates could be used to prove the validity of how information was obtained, but not whether the information itself is true. It would grossly unfair to a defendant if an element of an offence would be determined by the prosecution simply issuing a certificate to that effect.
- 4.213 The Committee is of the view that any future amendments for an ASIO evidentiary certificate scheme should be drafted in a way such that ultimate facts are not to be the subject of an evidentiary certificate, and that the content of such a certificate would be limited to certain technical facts removed from a fact in issue before a court.

---

<sup>111</sup> New South Wales Young Lawyers, *Submission No. 133*, p. 13; See also: Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 15 and NSW Council for Civil Liberties, *Submission No. 175*, p. 17.

### Recommendation 37

The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code.

The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.

## Matters on which the Government expressly seeks the Committee's views – Intelligence Services Act amendments

4.214 In addition to the above proposed amendments to the ASIO Act, the Government also expressly seeks the Committee's views on amending the *Intelligence Services Act 2001* (the IS Act) to:

- Add a new ministerial authorisation ground to allow the investigation of a person who is, or is likely to be, involved in intelligence or counter-intelligence activities;
- Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person where the Agency is cooperating with ASIO; and
- Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

4.215 Australia's foreign intelligence agencies, the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO), collect intelligence in accordance with requirements set by Government and operate under the *Intelligence Services Act 2001* (the IS Act). These agencies have identified problems arising out of the operation of the IS Act, as described in the sections which follow.



## Section 9 – Ministerial authorisations

- 4.216 The Government expressly seeks the Committee's views on amending the Intelligence Services Act to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.
- 4.217 The IS Act imposes strict controls on the ability of ASIS, DSD and DIGO to produce intelligence on an Australian person.
- 4.218 The Minister responsible for each Australian foreign intelligence agency is required to direct that the agency obtain authorisation from the Minister before undertaking activities for the purposes of producing intelligence on an Australian person.
- 4.219 The grounds on which a foreign intelligence agency may seek a ministerial authorisation are laid out in section 9 of the IS Act and, *inter alia*, include acting for, or on behalf of, a foreign power and activities that are, or are likely to be, a threat to 'security' (as defined in the *Australian Security Intelligence Organisation Act 1979*).
- 4.220 The discussion paper notes that those grounds 'do not specifically cover the situation where a person is or is likely to be involved in intelligence or counter-intelligence activities.'

A new item could be added to the list in section 9(1A)(a) of the IS Act which would allow the Minister to give an authorisation if he or she is satisfied that the person is, or is likely to be, involved in intelligence or counter-intelligence activities.<sup>112</sup>

- 4.221 The Gilbert + Tobin Centre for Public Law argued that the necessity of the proposed new ministerial authorisation ground was unclear. It was further contended that such counter-intelligence activities would fall within the existing ministerial authorisation ground of 'activities that are, or are likely to be, a threat to security'.<sup>113</sup>
- 4.222 ASIS's submission elaborated on the discussion paper and stated that the purpose of investigating a person for intelligence or counter-intelligence activities relates to operational security:

Operational security is about the protection of the integrity of ASIS operations from the risk of being undermined by foreign and non-State adversaries such as terrorist organisations, or reliance on inaccurate or false information. It is important to the protection of individuals, maintaining the effectiveness of ASIS and other Australian intelligence

---

<sup>112</sup> Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 52.

<sup>113</sup> Gilbert + Tobin Centre of Public Law, *Submission No. 36*, pp. 19–20.

and security agencies, as well as protecting Australia's international reputation.<sup>114</sup>

- 4.223 ASIS further submitted that such necessary counter-intelligence collection would not fall within any current ground for the issuing of ministerial authorisations.<sup>115</sup>

### Committee comment

- 4.224 Provided that ministerial authorisations would be subject to existing approval mechanisms, the Committee recommends that a new ministerial authorisation ground be created to enable the authorisation of activities for the purpose of producing intelligence on an Australian person who is, or is likely to be involved, in activities that will, or are likely to, undermine operational integrity.

---

### Recommendation 38

**The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.**

## Section 13A – Co-operation with intelligence agencies

- 4.225 The Terms of Reference state that the Government expressly seeks the Committee's views on amending the IS Act to enable the Minister of an agency to authorise specified activities which may involve producing intelligence on an Australian person or persons where an IS Act agency is cooperating with ASIO in the performance of an ASIO function.
- 4.226 Section 13A of the IS Act allows the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO) to obtain ministerial authorisations to allow co-operation with other bodies in the performance of those other bodies' functions.
- 4.227 The discussion paper explains that the purpose of amending section 13A would be to 'better meet the intention of enabling Australia's intelligence agencies to

---

114 Australian Secret Intelligence Service, *Submission No. 219*, p. 3.

115 Australian Secret Intelligence Service, *Submission No. 219*, p. 3.

cooperate and assist each other in the performance of each other's functions to protect Australia and Australians'.<sup>116</sup>

- 4.228 The discussion paper further notes that there are differences in the legislative regimes which apply to ASIS, DSD and DIGO under the IS Act and to ASIO under the ASIO Act when they produce intelligence on Australians.
- 4.229 For example, ASIO can collect intelligence about an Australian of security interest, whether that person is in Australia or overseas, based on internal approvals, whereas ASIS would in all cases require the approval of the Minister for Foreign Affairs and the agreement of the Attorney-General to do the same thing.
- 4.230 The Gilbert + Tobin Centre of Public Law at the University of New South Wales criticised this proposal holding that it would 'radically alter' the requirement for IS Act agencies to obtain a ministerial authorisation before collecting intelligence on Australians:

It would amend 13A to allow the Minister to authorise ASIS, DSD or DIGO to produce intelligence on an Australian where the agency is cooperating with ASIO in the performance of an ASIO function. In essence, it would create a parallel, and significantly broader, ministerial authorisation regime for ASIS, DSD and DIGO to produce intelligence on Australians.<sup>117</sup>

- 4.231 However, the Inspector-General of Intelligence and Security (IGIS) noted in her submission that in some instances the level of privacy protection given to an Australian would depend, not on the matter being investigated or the tools used in the investigation, but on which agency was conducting the investigation. The IGIS concluded that:

Through my experience in the oversight of the agencies I am aware of the operational difficulties and anomalies of the current regime and can see the need for change.<sup>118</sup>

- 4.232 Rather than support the discussion paper's suggestion for dealing with the inconsistent privacy protections for Australians who are of interest to both ASIO and a foreign intelligence agency, the IGIS proposed an alternative solution.
- 4.233 The IGIS proposed that an equivalent common standard across the IS Act and the ASIO Act be introduced to particularly intrusive activities involving the purpose of collecting intelligence on an Australian person.

---

116 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 51.

117 Gilbert + Tobin Centre of Public Law, *Submission No. 36*, pp. 20-21.

118 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 24.

- 4.234 The solution proposed by the IGIS was also endorsed by ASIS which considered the IGIS's proposal to be 'an elegant solution'.<sup>119</sup>

### Committee comment

- 4.235 The Committee in turn agrees with the IGIS alternative solution to this particular proposal. This alternative solution would ensure that the inconsistent privacy protection would be eliminated and a consistent standard across all intelligence agencies would apply.
- 4.236 The Committee also notes that where ASIS proposes to collect intelligence on an Australian person to assist ASIO with its functions, this would still need to be at the request of ASIO.

### Recommendation 39

**The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the *Australian Security Intelligence Organisation Act 1979* should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.**

### ASIS co-operation on self-defence and weapons training

- 4.237 The Government expressly seeks the Committee's views on amending the IS Act to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.
- 4.238 The IS Act was amended in 2004 to to enable ASIS staff members and agents to receive training in the use of weapons and self-defence techniques in certain limited circumstances.
- 4.239 ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. The IS Act does not currently enable ASIS staff members to participate in joint training in the use of weapons with persons who are lawfully cooperating with ASIS. This applies even though ASIS staff members are authorised to use weapons to protect such persons.
- 4.240 To remedy this inconsistency the discussion paper proposes that ASIS would be allowed to engage in weapons training with Commonwealth, State and Territory bodies that have their own rights to carry weapons in the course of their duties.

---

119 Australian Secret Intelligence Service, *Submission No. 219*, p. 1.

ASIS would also be enabled to cooperate with a limited number of approved overseas authorities in the delivery of training in self-defence and weapons.<sup>120</sup>

- 4.241 The Pirate Party of Australia submitted that allowing the Foreign Minister to approve foreign bodies to receive such training ‘is deeply concerning’:

This could be used to train insurgent armies, assassination squads and even terrorists. Such activities are not justified under any circumstances and is contrary to Australia’s national interest. Any tool created to fight foreign enemies can be turned upon the Australian people or at minimum be justification for our enemies to adopt the same strategies against us.<sup>121</sup>

- 4.242 Similarly, the Human Rights Law Centre expressed concern that weapons and self-defence training:

...may pose risks to right to life contained in article 6 of the ICCPR. These proposals should have regard to human rights standards on the use of force.<sup>122</sup>

- 4.243 Contrarily, ASIS’s submission asserted that the current carriage of weapons by ASIS is strictly for defensive purposes in accordance with the limitations imposed by Schedule 2 of the IS Act.<sup>123</sup>

- 4.244 Similarly, the Inspector-General of Intelligence and Security noted in her submission that:

Generally I am satisfied that the powers afforded to ASIS under Schedule 2 of the ISA are reasonable given the high threat environments in which it conducts some of its more sensitive activities, that the numbers of individuals who are authorised to use weapons is quite small and these authorisations are not being misused. I have been briefed on the need for joint training activities and have no propriety concerns with what has been proposed. If the proposed amendments are made I will monitor their implementation.<sup>124</sup>

## Committee comment

- 4.245 The Committee is of the view that as ASIS officers are permitted at law to co-operate with certain agencies and use weapons and self-defence techniques to protect themselves and their partner agencies, it is reasonable for ASIS to be able to train with those same partners in the self-defence techniques and with the weapons that are intended to save their lives.

---

120 Attorney-General’s Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 54.

121 Pirate Party Australia, *Submission No. 134*, p. 31.

122 Human Rights Law Centre, *Submission No. 140*, p. 8.

123 Australian Secret Intelligence Service, *Submission No. 219*, p. 3.

124 Inspector-General of Intelligence and Security, *Submission No. 185*, p. 25.

- 4.246 Indeed, the lack of such joint training poses an unacceptable danger to ASIS officers and agents.

#### **Recommendation 40**

**The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.**

### **Concluding comment**

- 4.247 The Committee has carefully considered each of the reform proposals. Where the Committee has recommended draft amendments be made to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, these amendments should first be released as an exposure draft for consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.
- 4.248 Consistent with the approach recommended for reform of the TIA Act in chapter two, the Committee recommends that the reforms to the AIC legislation be subject to public consultation and Parliamentary scrutiny.

#### **Recommendation 41**

**The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.**

**In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.**

## Data Retention

### Introduction

- 5.1 The Attorney-General's Department (AGD) Discussion Paper notes that the Australian Government is seeking the Committee's views on a mandatory data retention regime.<sup>1</sup>
- 5.2 Specifically, the Discussion Paper states that the Committee should consider:
- Applying tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts.<sup>2</sup>
- 5.3 The Discussion Paper discusses the importance of accessing communications data in investigating crime and threats to national security:
- Lawful interception and access to telecommunications data are cost-effective investigative tools that support and complement information derived from other sources.<sup>3</sup>

---

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

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

3 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 14.

5.4 Furthermore:

Telecommunications data is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest.<sup>4</sup>

5.5 The Discussion Paper also explains why reforms in this area are necessary:

Currently, authorised access to telecommunications data, such as subscriber details, generated by carriers for their own business purposes is an important source of information for agencies. As carrier's business models move to customer billing based on data volumes rather than communication events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations.<sup>5</sup>

5.6 In subsequent correspondence to the Committee, the Attorney-General clarified the data set, noting that it is similar to that set out under the European Union data retention directive.

5.7 In this letter, Attorney-General the Hon Nicola Roxon MP stated that:

'Telecommunications data' is information about the process of a communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the telecommunications carrier or internet service provider to establish the account, and information such as the time and date of the communication, its duration, location and type of communication.<sup>6</sup>

5.8 Furthermore, Attorney-General Roxon noted that the Government does not 'propose that a data retention scheme would apply to the content of communications', including 'the text or substance of emails, SMS messages, phone calls or photos and documents sent over the internet'. Access to these would continue to be authorised only under warrants issues in accordance with the *Telecommunications (Interception and Access) Act 1979* (TIA Act).<sup>7</sup>

---

4 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 21.

5 Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats*, July 2012, p. 21.

6 Letter from Attorney-General Nicola Roxon to the Hon Anthony Byrne MP, 17 September 2012, Appendix F.

7 Letter from Attorney-General Nicola Roxon to the Hon Anthony Byrne MP, 17 September 2012, Appendix F.



- 5.9 Many submitters to this inquiry expressed their concerns about content being retained under any mandatory data retention regime. However, the Attorney-General and AGD categorically ruled out retaining content in evidence to the Committee.<sup>8</sup> This would preclude access to content such as the substance of text messages and emails, about which many submitters expressed concern. Nevertheless, the vital definitional issue of what constitutes 'data' and 'content' is examined.

## The current regime

- 5.10 According to the report on the TIA Act that is published by AGD annually, enforcement agencies are able to access certain communications data under part 4-1 of TIA Act, however access to the actual content of this communication is prohibited except under a warrant.<sup>9</sup>
- 5.11 The communications data that can be accessed includes:
- subscriber information;
  - telephone numbers of the parties involved in the communication;
  - the date and time of a communication;
  - the duration of a communication;
  - Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication; and
  - location-based information.<sup>10</sup>
- 5.12 A table listing the telecommunications data currently provided to agencies by Telstra under the provisions of the TIA Act is available at Appendix H.
- 5.13 Under the current regime, law enforcement agencies may access historical communications data in circumstances where it is considered reasonably necessary for:
- the enforcement of criminal law;
  - the enforcement of a law imposing a pecuniary penalty; or
  - the protection of public revenue.<sup>11</sup>

---

8 A letter from the Secretary of AGD, Mr Roger Wilkins AO, clarifying the data set can be found at Appendix G.

9 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 10.

10 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 10.

11 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 11.

- 5.14 Access to prospective communications data, however,  
...may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years.<sup>12</sup>
- 5.15 For ASIO, these authorisations may only be made where the person making the authorisation is 'satisfied that the disclosure would be in connection with the performance by the Organisation of its functions'.<sup>13</sup>
- 5.16 The TIA Act also sets out who is able to make these authorisations:
- Head of an agency;
  - the deputy head of an agency; or
  - an officer or employee of the agency covered by an approval, in writing, of the head of the agency.<sup>14</sup>
- 5.17 The regime governing access to prospective data is very similar to that for historical data. The key difference is that the authorisation for access to prospective data either ends at a specified time, or ends after 90 days.<sup>15</sup>
- 5.18 It is important to note that the AGD Discussion Paper proposes no changes to the regime for accessing communications data, and simply raises the possibility of making retention of the relevant data mandatory for carriers/carriage service providers (C/CSPs).

## The international experience

- 5.19 During this inquiry, the experience of the European Union in implementing a data retention regime in its member countries was raised by several submitters and witnesses.<sup>16</sup> As a result, the Committee explored this experience to see what lessons it can offer in terms of potential data retention regimes in Australia.
- 5.20 The two relevant international examples of data retention regimes that the Committee explored were implementations of the European Union's data retention directive; particularly the controversy surrounding its implementation in Germany, and the United Kingdom's voluntary data retention scheme.

---

12 Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2011*, Commonwealth of Australia, 2011, p. 11.

13 *TIA Act*, Part 4-1.

14 *TIA Act*, Part 4-1.

15 *TIA Act*, Part 4-1.

16 See Blueprint for Free Speech, *Submission No. 165*; Law Council, *Submission No. 96*; Pirate Party of Australia, *Submission No. 134*; Human Rights Law Centre, *Submission No. 140*.

## EU data retention directive

- 5.21 On 15 March 2006 the European Parliament and the Council of the EU passed a directive requiring all member states to transpose laws mandating the retention of telecommunications data for periods between six months and two years, according with their legal and constitutional processes.<sup>17</sup>
- 5.22 According to the Law Council, the EU Data Retention Directive:
- ...requires providers of publicly available electronic communications services and public communication networks to retain communications data for the investigation, detection and prosecution of serious crime as defined by each Member State.<sup>18</sup>
- 5.23 This directive ‘does not permit the retention of data revealing the content of the communication’, and instead focuses on a ‘wide range of other telecommunications data’ that allows enforcement and security agencies to:
- Trace and identify the source of a communication, such as the calling telephone number, the name and address of the subscriber or registered user... or the name and address of the internet subscriber or registered user to whom an Internet Protocol (IP) address, user identification or telephone number was allocated at the time of the communication;
  - Identify the destination of a communication, such as numbers dialled or the name and address of the internet subscriber or registered user and user ID of the intended recipient of the communication;
  - Identify the data, time and duration of a communication, such as the data and time of the start and end of a telecommunication, the data and time of the log-in and log-off of the internet access service, the date and time of the log-in and log-off of the internet email service;
  - Identify the type of communication; such as the telephone service used or the internet service used;
  - Identify users’ communication equipment, such as the International Mobile Subscriber Identity of the calling party or the digital subscriber line or other end point of the originator of the internet communication; and
  - Identify the location of mobile equipment, such as the location label at the start of the telecommunication.<sup>19</sup>
- 5.24 The EU Data Retention Directive required member states to ‘implement measures to ensure this data is retained for periods between six months and two years from the date of the communication’, the Law Council told the Committee,

---

17 European Union Data Retention Directive 2006/24/EC.

18 Law Council, *Submission No. 224*, p. 6.

19 Law Council, *Submission No. 224*, p. 6.

and also makes provisions for access to the data and the security of the retained data.<sup>20</sup>

5.25 While the Directive has been implemented in several countries, and notably in the UK via a voluntary code of practice, it has been subject to successful constitutional challenges in three EU member states: Germany, Romania and the Czech Republic.

5.26 According to the Law Council:

The Romanian Court accepted that interference with fundamental rights may be permitted where it respects certain rules and where adequate and sufficient safeguards are provided to protect against potential arbitrary state action. However, the Court found the transposing law to be ambiguous in its scope and purpose with insufficient safeguards. The Court held that a 'continuous legal obligation' to retain all traffic data for six months was incompatible with the rights to privacy and freedom of expression...<sup>21</sup>

5.27 In the case of Germany, the Law Council stated:

The German Constitutional Court said that data retention generated a perception of surveillance which could impair the free exercise of fundamental rights. It explicitly acknowledged that data retention for strictly limited uses along with sufficiently high security of data would not necessarily violate the German Basic Law. However, the Court stressed that the retention of such data constituted a serious restriction of the right to privacy and therefore should only be admissible under particularly limited circumstances, and that a retention period of six months was at the upper limit of what could be considered proportionate. The Court further held that data should only be requested where there was already a suspicion of a serious criminal offence or evidence of a danger to public security, and that data retrieval should be prohibited for certain privileged communications which rely on confidentiality.<sup>22</sup>

5.28 Finally, in the case of the Czech Republic, the Law Council told the Committee:

The Czech Constitutional Court annulled the transposing legislation on the basis that it was insufficiently precise and clear in its formulation. The Court held that the definition of authorities competent to access and use retained data and the procedures for such access and use were not sufficiently clear in the transposing legislation to ensure the integrity and

---

20 Law Council, *Submission No. 224*, p. 7.

21 Law Council, *Submission No. 224*, p. 9.

22 Law Council, *Submission No. 224*, pp. 9-10.

the confidentiality of the data. Because of this, the individual citizen had insufficient guarantees and safeguards against possible abuses of power by public authorities. In obiter dictum the Court also expressed doubt as to the necessity, efficiency and appropriateness of the retention of traffic data given the emergence of new methods of criminality such as through the use of anonymous SIM cards.<sup>23</sup>

- 5.29 In addition to these successful challenges, there are currently cases in Bulgaria, Cyprus, Hungary and Ireland being mounted to challenge the implementation of the EU Data Retention Directive, the latter has 'been referred to the European Court of Justice'.<sup>24</sup> It must be noted, however, that these challenges took place in countries with human rights frameworks that are significantly different to those in Australia.

### UK voluntary data retention

- 5.30 The Law Council told the Committee that the UK has implemented the EU data retention directive via a voluntary code of practice relating to data retention:

The United Kingdom (UK) has a system of voluntary data retention which derives from Part 11 of the Anti-Terrorism, Crime and Security Act 2001. Telephone operators and Internet Service Providers retain some data under a voluntary arrangement with the UK Home Office.<sup>25</sup>

- 5.31 The NSW Young Lawyers elaborated on how this code works:

In the UK, this convention has been the basis upon which the Home Office has issued a voluntary code of conduct under which telephone and internet service providers retain some data. The legislation enabling the Convention in the UK also provides that if the Secretary of State is unconvinced of the efficacy of such a voluntary program, then the Code may be made mandatory. The code has not subsequently been made mandatory and requires only a small subset of data be kept for up to 12 months, principally consisting of subscriber information that would be necessary for billing.<sup>26</sup>

- 5.32 The Australian Mobile Telecommunications Association (AMTA) and the Communications Alliance noted that the costs of the voluntary data retention are fully borne by the UK Government, and that this is a part of the voluntary code

---

23 Law Council, *Submission No. 224*, p. 10.

24 Law Council, *Submission No. 224*, p. 10.

25 Law Council, *Submission No. 96*, p. 38.

26 NSW Young Lawyers, *Submission No. 133*, p. 10.

of practice.<sup>27</sup> Further, in order to have these costs borne by the government, UK service providers must be a part of the voluntary code.<sup>28</sup>

5.33 The UK Parliament is currently considering a *Draft Communications Data Bill* that will, amongst other things, make the retention of data mandatory for 12 months.<sup>29</sup> However, the UK Bill differs significantly from the potential reform being considered in Australia. For instance, the data to be collected and stored under the UK Draft Bill is limited only in terms of what is considered 'necessary' by the UK Home Office, which extends to data such as 'web logs'.<sup>30</sup>

5.34 In this regard, a report produced by the UK Intelligence and Security Committee (ISC), was broadly supportive of the need for reform:

The Agencies require access to communications data – in certain tightly controlled circumstances and with appropriate authorisation – in the interests of national security. We recognise that changing technology means that the Agencies are unable to access all the communications data they need, that the problem is getting worse, and that action is needed now. We accept that legislation to update the current arrangements governing the retention of communications data offers the most appropriate way forward.<sup>31</sup>

5.35 At the end of its inquiry the Committee was provided with the ISC report published in February 2013. The ISC reached three key conclusions:

- The intelligence agencies need to continue to have access to telecommunications data;
- There is a gap emerging in their ability to access this data; and
- While legislation is not a perfect solution, it is the best available option in contrast to other investigatory methods and a voluntary approach.<sup>32</sup>

5.36 Furthermore, the Joint Committee on the Draft Communications Data Bill of the UK Parliament has produced a report on the draft bill which was also broadly supportive of the need for reform. However, this report also cautioned:

27 AMTA and Communications Alliance, *Submission No. 114*, p. 14.

28 UK Home Office, *Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009*, pp. 1-2.

29 *Draft Communications Data Bill 2012*, United Kingdom.

30 Joint Committee on the Draft Communications Data Bill, UK Parliament, *Draft Communications Data Bill*, December 2012, p. 24.

31 UK Intelligence and Security Committee, Press release, 11 December 2012, viewed 18 December 2012, <<http://isc.independent.gov.uk/news-archive/11december2012>>.

32 UK Intelligence and Security Committee, *Access to Communications Data by Intelligence and Security Agencies*, UK Parliament, February 2013.

...the current draft Bill is too sweeping, and goes further than it need or should. We believe that, with the benefit of fuller consultation with CSPs than has so far taken place, the Government will be able to devise a more proportionate measure than the present draft Bill, which would achieve most of what they really need, would encroach less on upon privacy, would be more acceptable to CSPs and would cost the taxpayer less.<sup>33</sup>

## Responses to data retention

- 5.37 The potential data retention regime attracted a large amount of criticism and comment from organisations and concerned individuals. These organisations and individuals generally considered any potential data retention regime a significant risk to both the security of their information, and their privacy. In addition to these general comments, the Committee received a large volume of form letter correspondence. A collective sample of some of these comments and the form letters can be found in Box 5.1.
- 5.38 Conversely, the data retention regime received a high level of support from law enforcement and national security agencies. These agencies largely argued that data retention was necessary for them to maintain their current capabilities into the future.
- 5.39 This section outlines these perspectives by grouping them under the following headings:
- Privacy and civil liberties;
  - Security;
  - Feasibility and efficacy; and
  - Cost.

---

33 Joint Committee on the Draft Communications Data Bill, UK Parliament, *Draft Communications Data Bill*, December 2012, p. 74, viewed 18 December 2012, <[www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/](http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/)>.

**Box 5.1 Community responses to the mandatory data retention regime proposal**

'As both an Australian citizen and a small business owner I am seriously concerned about the over-reaching changes proposed by this reform. I believe it is inherently wrong to log and track activity via an individual's ISP and/or participation in social network/s.' (Mr Craig Veness, *Submission No. 13*, p.1 and other submitters (in common form).)

'By tracking and recording every single Australian online, and keeping these records for two years, this proposal will destroy our online privacy, make every Australian into a criminal, give too much power to the government, and go far and beyond what is necessary. Specifically, I oppose the proposals to: 1)Keep all Australians' online data for two years 2)Track everything said on Twitter, Facebook & other social media...' (Ms Rhonda Palmer, *Submission No. 20*, p. 1 and other submitters (in common form).)

'The proposal that internet services providers retain all data on all users for a period of two years turns all citizens into suspects. This proposal is undemocratic and unacceptable; it also creates a security risk as the preserved data can be made available and misused.' (Mr Josh Fergeus, *Submission No. 53*, p. 1 and other submitters (in common form).)

'[I] have a concern that the data collection proposed by the Australian government will increase the fear and nervousness that as people living in a free democratic country we should be free from feeling, an untrusted, and being watched for criminal behaviour by our own government, by businesses not designed to monitor the information its customers disclose to each other in private conversation.' (Ms Odette Stephens, *Submission No. 1*, p. 1.)

'I am strongly opposed to the draconian proposals from Australia's intelligence community, that telephone and internet data of every Australian be retained for up to two years and intelligence agencies be given increased access to social media sites such as Facebook and Twitter. Such data retention schemes are extremely unpopular, have been a subject of much global debate and outrage, most ISPs and the majority of Australians share these sentiments.' (Mr Mark Simpson, *Submission No. 2*, p. 1.)

'I don't believe national security justifies the proposed levels of intrusion into citizens' private lives.' (Mr Malcolm Rieck, *Submission No. 21*, p.1.)

'It would be a great shame if a country such as ours were to adopt such an invasive and unnecessary data retention policy that infringes on the basic privacies of citizens, which instead of presuming innocence until guilty, collects data on them and stores it as if they were criminals. Should it become law that conversations between two people walking down the street were to be recorded by the government, it would be considered a gross



invasion of privacy akin to the invasions of privacy that were present in Soviet era Russia.’ (‘James’, *Submission No. 7*, p. 1.)

‘This concept of long term data retention is especially concerning these days, considering how much of our life takes place on the internet.’ (Mr Peter Serwylo, *Submission No. 22*, p. 1.)

‘This is crazy. ALL customers, and ALL their data? The people who thought this up are sick.’ (Mr Joe Stewart, *Submission No. 32*, p. 1.)

‘We do not need our government to spy on us all the time. I would rather we had the occasional act of terrorism than live under an oppressive government.’ (Mr Sam Watkins, *Submission No. 29*, p. 1.)

‘I am a middle-aged, middle class, professional woman with no dark secrets to hide and nothing to fear from anyone knowing anything whatsoever about my online activities, but I can hardly believe that this is even being considered in Australia. When I first heard it I thought “Surely this is a joke.”’ (Ms Mary Annesley, *Submission No. 73*, p. 1.)

‘The vast majority of Australians are decent people and we do not need or want the spectre of the government hovering over our most intimate moments.’ (Dr James G. Dowty, *Submission No. 35*, p. 2.)

## Privacy and civil liberties

### Community views

- 5.40 A range of organisations and individuals objected to the potential data retention regime on civil liberties and privacy grounds.
- 5.41 The Law Council of Australia expressed its concerns about this proposal, stating:
- Introducing a requirement to retain certain data for up to two years, even with accompanying safeguards, constitutes a significant expansion of the telecommunications interception and access regime, and one that the Law Council considers has not yet been shown to be a necessary or proportionate response to investigating serious criminal activity or safeguarding national security, particularly given the very serious impacts such a reform will have on the privacy rights of many members of the community.<sup>34</sup>
- 5.42 The Institute of Public Affairs (IPA) was similarly strident in its criticism of the potential impacts of data retention, stating that the 'imposition of such an extraordinary, systematic and universal program would render any presumed or existent Australian right to privacy empty'.<sup>35</sup>
- 5.43 The IPA characterised any potential data retention regime as representing 'a significant incursion on the civil liberties of all Australians', stating that:
- Data retention would be a continuous, rolling, systematic invasion of the privacy of every single Australian, only justified because a tiny percentage of those Australians may, in the future, be suspects in criminal matters. Indiscriminate data retention is an abrogation of our basic legal rights.<sup>36</sup>
- 5.44 Blueprint for Free Speech shared the overall concerns about the impact of any data retention scheme on the privacy of internet users in Australia, stating 'this measure would dramatically reduce privacy in Australia, with very few demonstrated national security benefits'.<sup>37</sup>
- 5.45 The Pirate Party told the Committee that the data retention proposal was:
- ...indicative of a shift in focus by law enforcement and intelligence organisations from protecting the populace and the presumption of
- 

34 Law Council of Australia, Submission No. 96, p. 37.

35 Institute of Public Affairs, *Submission No. 139*, p. 4.

36 Institute of Public Affairs, *Submission No. 139*, p. 3.

37 Blueprint for Free Speech, *Submission No. 165*, p. 6.

innocence to one of constant surveillance and suspicion of the populace. Where the existing targeted surveillance is akin to spear fishing, mandatory data retention is more like drift net fishing. The risk to individual privacy is enormous.<sup>38</sup>

- 5.46 The Human Rights Law Centre took a similar view, stating that the ‘vast quantity of private data that could be stored and accessed’, coupled with its extension to ancillary providers, could ‘severely limit the right to privacy’. As such, any data retention scheme would need to be shown to be proportionate to the desired outcomes:

...if the Government wishes to limit the right to privacy, it must state the overriding public interest in limiting the right and establish that the means used are reasonable, necessary and proportionate. In this instance, the Government has not provided any significant information to show that there is an overriding public interest in implementing a data-retention system.<sup>39</sup>

- 5.47 In regard to maximising the privacy of consumers of telecommunications services, Mr Daniel Nazer raised the concept of ‘data minimisation’, noting that it is considered by privacy experts as ‘an essential tool for privacy protection’. Mr Nazer quoted the Canadian Privacy Commissioner, Dr Ann Cavoukian, on the benefits of data minimisation:

Data minimization is essential to effective privacy protection, and can save organizations the risk and expense of managing personal information they may have no need for. Where there is no personal information, there is no consequent duty of care, with all that it implies. Further, data minimization requirements assists organizations to think through what personal information is actually necessary for their purposes, and guards against secondary uses and possible function creep.<sup>40</sup>

- 5.48 Mr Nazer went on to note that:

Mandatory data retention flatly contradicts the principle of data minimisation. Instead, it forces service providers to store enormous amounts of data for which they have no business need.<sup>41</sup>

- 5.49 Similarly, Liberty Victoria told the Committee of its view that ‘the very collection of the data would in and of itself raise significant privacy concerns’.<sup>42</sup> It went on

---

38 Pirate Party, *Submission No. 134*, p. 26.

39 Human Rights Law Centre, *Submission No. 140*, p. 7.

40 Mr Daniel Nazer, *Submission No. 110*, p. 4

41 Mr Daniel Nazer, *Submission No. 110*, p. 4

42 Liberty Victoria, *Submission No. 143*, p. 5.

to state that data retention is 'inherently more invasive' than the traditional 'targeted interception' approach, noting:

It constitutes a significant intrusion into the privacy of each end user of telecommunications services and creates a situation in which a single security breach would have dramatic consequences. It represents a significant move away from the 'targeted' approach of the [TIA Act] which requires specific identification of communications and their relevance to an agency's activities before information can be collected.<sup>43</sup>

5.50 Furthermore, Liberty Victoria also submitted that 'it is inevitable that, once a database of retained communications data is established, efforts will be made to extend its use for new purposes'. As such, Liberty Victoria proposed that safeguards be put in place to ensure the retained data was used 'only where there is a demonstrated need'.<sup>44</sup>

5.51 The New South Wales Council for Civil Liberties (NSW CCL) noted similar concerns about the perceived diminution in privacy, and drew attention to the international experience:

...the present data retention laws contravene international standards. The German Constitutional Court in March 2010 declared the German data retention laws unconstitutional, because of lack of proportionality in balancing right of privacy against interest in prosecuting crime. One of the aspects which the Court held was disproportional was that it applied to too wide a range of crimes, and should be permitted only for investigation of crimes of the most serious kind.<sup>45</sup>

5.52 The Australian Interactive Media Industry Association's Digital Policy Group raised its concerns about the presumption of guilt which it perceived was inherent in any blanket data retention proposal. As a result, it suggested an alternative approach:

A system allowing for requests for preservation and retention of user data made by a judge or authorised law enforcement officials would lessen the risk from such blanket intrusion into privacy.<sup>46</sup>

5.53 Ms Stella Gray, submitting in a private capacity, shared the concern about the presumption of innocence, noting:

Pre-emptive surveillance of an entire population does away with the legal principle of the presumption of innocence. Any serious consideration of

43 Liberty Victoria, *Submission No. 143*, p. 2.

44 Liberty Victoria, *Submission No. 143*, p. 6.

45 NSW Council for Civil Liberties, *Submission No. 175*, p. 16.

46 Australian Digital Media Industry Association, *Submission No. 198*, p. 4.

implementing such a system, in a democratic country such as Australia, should be anathema to policy makers.<sup>47</sup>

- 5.54 Western Australian Greens Senator Scott Ludlum echoed these concerns about the presumption of innocence, saying that indiscriminate data retention is ‘unacceptable’ as it essentially treats all citizens as suspects.<sup>48</sup> The Institute of Public Affairs similarly characterised data retention regimes as making ‘internet users guilty until proven innocent’.<sup>49</sup>
- 5.55 The Victorian Privacy Commissioner, Dr Anthony Bendall, submitted that data retention was ‘characteristic of a police state’ as it goes against both the presumption of innocence, and ‘essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person’s life.’<sup>50</sup>
- 5.56 At a public hearing, Dr Bendall elaborated on this concern, noting that data retention:
- ...entirely undermines the fundamental underpinnings of privacy laws, which basically are that information should only be collected and stored where necessary and for a particular purpose, whereas these proposals seem to be that you store all the information just on the off chance that it might be useful down the track and you make up your mind how it would be useful at that point.<sup>51</sup>
- 5.57 The Law Council agreed that this approach ‘does not sit easily with the notion of the presumption of innocence or other traditional criminal law or human rights principles’, and thus may breach Australia’s obligations under United Nations human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR).<sup>52</sup>
- 5.58 The NSW CCL also suggested that any data retention regime would not conform to Australia’s obligations under the ICCPR.<sup>53</sup>
- 5.59 Similarly, Senator Ludlam linked the privacy concerns to human rights and Australia’s obligations under UN conventions. In particular, Senator Ludlam pointed to the resolution adopted by the UN Human Rights Council and the General Assembly in 2012, which noted the importance of ‘the right of

---

47 Ms Stella Gray, *Submission No. 152*, p. 6.

48 Senator Scott Ludlum, *Submission No. 146*, p. 26

49 Institute of Public Affairs, *Submission No. 139*, p. 3.

50 Victorian Privacy Commissioner, *Submission No. 109*, p. 7.

51 Dr Bendall, *Transcript*, 5 September 2012, p. 1.

52 Law Council of Australia, *Submission No. 96*, p. 39.

53 NSW Council for Civil Liberties, *Submission No. 175*, p. 16.

individuals to seek, receive and impart information and ideas of all kind through the internet'.<sup>54</sup>

- 5.60 Senator Ludlum quoted the UN Special Rapporteur on the importance of governments upholding this principle:

States are obliged to guarantee a free flow of ideas and information and the right to seek and receive as well as to impart information and ideas over the internet.<sup>55</sup>

- 5.61 In Senator Ludlum's view, any restrictions on this right must be demonstrated to be proportionate and necessary to the outcomes this restriction will achieve. He further contended that the Discussion Paper does not provide an adequate justification.<sup>56</sup>

- 5.62 The Law Council discussed the privacy implications of only retaining communications data, stating that even if it 'does not include the content and substance of a person's private communications', the communications data can still reveal 'crucial' information about a person, including such things as their associations and whereabouts.<sup>57</sup> As a result of these concerns, the Law Council recommended that the potential reform be rejected unless it could be clearly demonstrated that it is 'indispensable to protect the community from serious threats of criminal activity or national security'.<sup>58</sup>

- 5.63 iiNet agreed that any potential data retention regime could negatively impact privacy, and related this concern to Australia's National Privacy Principle (NPP) under the *Privacy Act 1988*.

- 5.64 iiNet noted that NPP 1.1 states that:

...an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. Therefore, if collection of telecommunications data or subscriber information is necessary for one or more of the functions or activities of a C/CSP (for example providing a telecommunications service), there will be no issue. However, if a C/CSP decided off its own bat (i.e. without any legal obligation to do so) to collect and retain data that is personal information solely because that data had the potential to be of use to law enforcement agencies, that C/CSP would likely be in breach of NPP 1.1. Therefore, the effect of the proposed reform is to effectively provide a

---

54 Senator Scott Ludlum, *Submission No. 146*, p. 2.

55 Senator Scott Ludlum, *Submission No. 146*, p. 2.

56 Senator Scott Ludlum, *Submission No. 146*, p. 2.

57 Law Council of Australia, *Submission No. 96*, p. 37

58 Law Council of Australia, *Submission No. 96*, p. 39.

statutory exemption to NPP 1.1 and allow personal information to be collected and retained where the sole reason for the collection and retention of that personal information is the fact that it may be of use to law enforcement agencies.<sup>59</sup>

5.65 The AMTA and the Communications Alliance shared this concern, noting:

Industry requires that any data retention legislation must also contain a caveat which expands upon the current concept of immunity to incorporate acting in good faith, and provide immunity to the reporting obligations under the *Privacy Act*.<sup>60</sup>

5.66 Mr Bernard Keane, submitting in a private capacity, argued that extending data retention from fixed line and mobile telephones to the internet constitutes a significant expansion of the powers held by law enforcement and security agencies, and thus would constitute a significant intrusion on privacy:

Australians, like citizen around the world, do not use online communications in the same way, or for the same purposes, as they used phones. They did not commit huge amounts of personal information to permanent storage on the phone. They did not leave crucial financial details on the phone. The phone was not their primary tool for interacting with communities that are important to them. The telephone did not enable contact with communities around the globe that are of critical importance to citizens.<sup>61</sup>

5.67 As such, Mr Keane posited that:

Any attempt therefore to impose the telecommunications interception laws on the internet represents not a logical extension of that law to 'keep up with technology' on a like-for-like basis but a dramatic extension of surveillance into citizens' lives far beyond that enabled by telecommunications interception.<sup>62</sup>

5.68 Mr Ian Quick, submitting in a private capacity, expressed a similar concern to that of Mr Keane, noting that if data on internet browsing is retained, this would constitute a much greater invasion of privacy than telecommunications data:

It is a massive invasion of everyone's privacy, as the usage database will contain every page they accessed – such as every article they have read on a newspaper site, any online political activity they have done, anything they have done on ebay, what books they have bought on Amazon, which

---

59 iiNet, *Submission No. 108*, p. 12.

60 AMTA and Communications Alliance, *Submission No. 114*, p. 16.

61 Mr Bernard Keane, *Submission No. 117*, p. 13.

62 Mr Bernard Keane, *Submission No. 117*, p. 14.

Facebook pages they have gone to, etc. - and a lot of information that is also often included in the URL.<sup>63</sup>

- 5.69 Electronic Frontiers Australia (EFA) took a similar view, and told the Committee that unlike the communications data associated with traditional telephony, internet communications data was far more intrusive:

Even if it were to be specified that the actual content of communications is not to be retained, information such as addresses of websites visited, email addresses and phone numbers to which messages are sent and received from, details of phone calls sent and received, and other online communications activities, along with associated dates, times and locations does amount, in many cases, to content and is highly personal data.<sup>64</sup>

- 5.70 EFA raised its concern that, in aggregate, examination of this type of data 'will reveal highly intimate details of a person's life', including such things as 'religious and political affiliations, sexual orientation, health issues' and other 'highly-sensitive information'.<sup>65</sup>

- 5.71 Mr Adrian Gasparini, submitting in a private capacity, shared the concern that the data to be retained could reveal intimate details about people's lives:

A person's browsing history is a very personal snapshot of that person's life and personality. A person should have the right to keep aspects of his personal life completely private. For example, take into consideration searches conducted on Google maps; the social networks a person may log into; medical symptom related searches on Google; and a snapshot of the adult content searched for on various websites. It would be easy to determine the identity and address of a person, their circle of friends and their partner, possibly identify any affairs being conducted, determine their sexual orientation, age, as well as any possible embarrassing medical conditions that the person may have searched for.<sup>66</sup>

- 5.72 Mr Daniel Judge, submitting in a private capacity, made a similar point about the potential privacy invasion inherent in retaining data on a person's internet browsing history:

The Internet today is used for a broad range of things and in many cases is the first port of call for people before seeing a doctor, or psychologist, or lawyer or marriage counsellor or any range of professional services all of

---

63 Mr Ian Quick, *Submission No. 95*, p. 14.

64 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

65 Electronic Frontiers Australia, *Submission No. 121*, p. 6.

66 Mr Adrian Gasparini, *Submission No. 88*, p. 1.



which are activities that would be captured and detailed by a mandatory data retention scheme. Any such information could be highly embarrassing to individuals should it fall into the wrong hands or become public knowledge. As such, the decision to retain this data is a highly dangerous endeavour when viewed within the context of the damage that could be done to people should the wrong information be leaked or stolen.<sup>67</sup>

- 5.73 EFA told the Committee that, when it comes to people's internet browsing, it is very difficult to separate data from content, and that this raises further questions about the privacy impact of any data retention regime:

A URL [uniform resource locator] will in many instances allow for the content of that website to be accessed well after the fact, providing a direct link to content. Many URLs contain sensitive information, such as user names and even passwords.<sup>68</sup>

- 5.74 iiNet made a similar point, noting that internet browsing data is often synonymous with content:

When we go to attachment A [of the Attorney-General's letter noted above], we see it includes that certain categories of data must be retained – namely, data necessary for identifying (a) the source of a communication and (b) the destination of a communication. This is where it comes to the interesting part for us. The only conclusion we can draw about the destination of a communication when considering internet access is that what must be retained are the IP addresses. As noted previously, little to no specific guidance is given by the Attorney-General's Department on the data to be gathered, so we will continue to make assumptions. As I have mentioned, each object or piece of content on each page also has an IP address, none of which can be distinguished from any other on the page. It is therefore a paradox that requires resolution when the Attorney-General's letter has declared that the data revealing content must not be retained but the destination data must be retained.<sup>69</sup>

- 5.75 The Law Council drew on an example of this from the constitutional challenge to Germany's data retention laws:

...even though the storage does not extend to the contents of the communications, the data may be used to draw content-related conclusions that extend into the users' private sphere. The observation

---

67 Mr Daniel Judge, *Submission No. 157*, p. 11.

68 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

69 Mr Dalby, *Transcript*, 27 September 2012, p. 48.

over time of recipient data, dates, times and place of telephone conversations permits detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. So, even if it is restricted to telecommunications data in that sense, in other jurisdictions that has been considered sufficient to indicate that the jurisdiction does not consider the scheme to be appropriate.<sup>70</sup>

5.76 Even when it comes to traditional telephony, EFA told the Committee that 'any numbers input after connection, in response to a phone tree or other verbal prompts' are essentially content, and in some cases will contain highly sensitive information such as personal identification numbers or credit card details.<sup>71</sup>

5.77 EFA went on to note that this presents a civil liberties issue, in that the existence of such 'large scale databases of communications activity' could be abused by governments and police. As such, EFA stated:

While we can earnestly hope that sufficient checks and balances would exist to prevent authorities abusing such databases to gather information on protesters (for instance), the only way to ensure that this never happens is to prevent the data being collected in the first place.<sup>72</sup>

5.78 Dr James Dowty, submitting in a private capacity, saw a similar potential for any data retention regime to 'be vulnerable to misuse by future governments'. Dr Dowty linked this to the amount of time the data is stored for, noting:

Once the data retention begins, legislative change could immediately give an unscrupulous government access to the web viewing histories, emails and text messages of their political opponents and constituents. While the current government might be staunchly opposed to such misuses of the retained data, there is no guarantee that the government of 2050 will be as trustworthy. Of course, the data which is currently retained by CSPs is also open to misuse in this way, but the inappropriate use of two years' worth of data is likely to be far more damaging than the misuse of a few weeks' worth.<sup>73</sup>

5.79 The Pirate Party made a similar argument, noting that the types of data to be retained were open to misuse:

---

70 Ms Budavari, *Transcript*, 14 September 2012, p. 14.

71 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

72 Electronic Frontiers Australia, *Submission No. 121*, p. 6.

73 Dr James Dowty, *Submission No. 35*, p. 1.

It would provide the opportunity for law enforcement and intelligence organisations to trawl through available data looking for something which might, on the surface, be of interest to them.<sup>74</sup>

- 5.80 The Pirate Party also linked this concern to the exercise of individual rights and political freedoms:

Analysis of the full data set could be used to map all connections and interactions of everyone in the country. Methods used to identify any criminal organisation or network could just as readily be applied to any group or organisation in the country. This could have a chilling effect on the exercise of individual rights and democratic participation. This type of analysis could then be exploited by law enforcement, intelligence organisations, elements within those organisations or other groups with which the analysis is shared to suppress organisations and groups which are not in and of themselves unlawful.

- 5.81 Blueprint for Free Speech raised similar concerns about political freedom, arguing that any potential data retention regime would have ‘a serious effect on freedom of speech’.<sup>75</sup>

- 5.82 Blueprint for Free Speech argued that:

Part of freedom of expression is the individual’s right to determine the manner in which they communicate. In other words, it is to determine who they wish to communicate with and when they wish to stop that communication or delete it.<sup>76</sup>

- 5.83 By making the retention of communications data mandatory, Blueprint for Free Speech contended that this right could be undermined:

People have a legitimate expectation that when they delete electronic information, it is gone. They do not expect their service provider to secretly retain it against their wishes. The [data retention] proposal is analogous to secretly collecting everyone’s garbage for two years and storing it in case it might assist a criminal investigation at some point in the future. In addition, it effectively prevents people from deleting their information, which is analogous to passing a law making it illegal to destroy your own documents.<sup>77</sup>

- 5.84 As such, Blueprint for Free Speech told the Committee that this diminution in privacy, coupled with the inability to, in essence, retract communications after

---

74 Pirate Party, *Submission No. 134*, p. 26.

75 Blueprint for Free Speech, *Submission No. 165*, p. 6.

76 Blueprint for Free Speech, *Submission No. 165*, p. 1.

77 Blueprint for Free Speech, *Submission No. 165*, p. 6.

the fact, 'would have a chilling effect on freedom of expression'.<sup>78</sup> Similarly, Dr Bendall stated that data retention could have 'an extreme chilling effect on online transactions'.<sup>79</sup>

- 5.85 Mr James McPherson elaborated on how data retention could lead people to not say or write things they might otherwise:

Even if the only data which was logged was email message headers, or a list of visited websites, there is more than enough information there to build accurate profiles of people, their opinions and their social networks. The most likely outcome of such surveillance is self-censorship, to avoid harassment by covert agencies 'just in case' an expressed opinion might fit some criteria which the agencies make up to justify invasive actions.<sup>80</sup>

- 5.86 Ms Stella Gray shared the concerns that any data retention regime would have a 'chilling effect on political speech and public discourse'.<sup>81</sup>

- 5.87 Australian Lawyers for Human Rights argued that, in order to maintain the 'expectation of privacy' of legitimate users of telephony and internet communications, 'the minimum amount of confidential data' should be 'retained for the smallest period of time possible'.<sup>82</sup>

- 5.88 AMTA and the Communications Alliance were similarly concerned about the privacy implications of retaining too much data:

There is likely to be some additional social cost, constituting both the cost of loss of privacy and a further additional risk to security as the retained data becomes itself a target for unlawful access. Industry believes it is generally better for consumers that service providers retain the least amount of telecommunications information necessary to provision, maintain and bill for services (including calls and transmissions).<sup>83</sup>

- 5.89 Ms Ashley Hull also suggested that, if privacy is to be maintained to the greatest possible extent, the data retained should be targeted:

ISPs shouldn't be told to keep data for customers whom have not yet been targeted by law enforcement with an open case and a warrant. As the lines between terrorism, civil disobedience and healthy dissent are deliberately blurred, our rights must be protected from these overarching sweeping reforms which target the select few while touching all of us. We

---

78 Blueprint for Free Speech, *Submission No. 165*, p. 1.

79 Dr Bendall, *Transcript*, 5 September 2012, p. 3.

80 Mr James C. McPherson, *Submission No. 28*, p. 4.

81 Ms Stella Gray, *Submission No. 152*, p. 6.

82 Australian Lawyers for Human Rights, *Submission No. 194*, p. 8.

83 AMTA and Communications Alliance, *Submission No. 114*, p. 15.

need to ensure there is no room for ambiguity - The crosshair must be aimed precisely.<sup>84</sup>

- 5.90 The IPA suggested that it would be possible to minimise the intrusion into privacy at the same time as maintaining the efficacy of law enforcement if the data was retained in a targeted fashion, stating that:

Strictly limited, supervised, and transparent data preservation orders on targeted suspects would strike the right balance between individual rights and law enforcement.<sup>85</sup>

- 5.91 Mr Nazer made a similar suggestion, noting that Australia should draw on the Canadian approach by instituting:

...a process whereby an agency can secure a temporary preservation order that remains in effect only for as long as it takes law enforcement to return with a warrant. While any data preservation program would still require safeguards to protect privacy, it is certain to be less invasive and costly than massive and indiscriminate data retention.<sup>86</sup>

### Law enforcement and security agencies' views

- 5.92 Law enforcement and national security agencies were adamant that any potential data retention regime does not represent an expansion of their powers, and thus does not translate into any serious diminution of privacy or a winding back of civil liberties.
- 5.93 As noted in the section describing the current regime above, law enforcement agencies are able to access telecommunications data (as distinct from content) under certain circumstances without a warrant. Collective examples arguing the importance of communications data to law enforcement agencies in investigations are included in Box 5.2.
- 5.94 As noted below, this access is tightly controlled by the C/CSPs themselves and is only disclosed when properly authorised, and no change is proposed to this aspect of the TIA Act by the AGD Discussion Paper. As such, mandating data retention will not lead to the removal of the presumption of innocence, as data will continue to be accessed only in connection with active investigations.
- 5.95 The Australian Federal Police (AFP) noted that access to communications data is both a necessary investigative tool and is far less privacy invasive than normal interception:

---

84 Ms Ashley Hull, *Submission No. 153*, p. 1.

85 Institute of Public Affairs, *Submission No. 139*, p. 4.

86 Mr Daniel Nazer, *Submission No. 110*, p. 7.

Non-content telecommunications data is an important investigative tool for the AFP. It can provide important leads for agencies, including evidence of connections and relationships within larger associations over time, evidence of targets' movements and habits, a snapshot of events immediately before and after a crime, evidence to exclude people from suspicion, and evidence needed to obtain warrants for the more intrusive investigative techniques such as interception or access to content.<sup>87</sup>

5.96 Furthermore:

There are no operational risks, and from a law enforcement perspective and as it relates to data about communications rather than its content, it raises fewer privacy concerns than the other covert investigative methods.<sup>88</sup>

5.97 Victoria Police noted that, as business practices change in the telecommunications sector, so does the length of time for which data is retained:

As carriers change their business practices from billing based on volume/length of calls made to billing based on data volumes, the need for carriers to retain such data is diminishing. This has enormous implications for law enforcement agencies reliant on this data to target suspects involved in serious crime.<sup>89</sup>

5.98 The Corruption and Crime Commission of Western Australian made the point that, if data retention is not made mandatory, they could face a diminution in their capabilities:

Agencies will face many challenges as telecommunications technologies migrate to IP networks. Investigations across almost all serious crime types including corruption, counter-terrorism and homicide rely significantly on telecommunications data. Without legislated data retention obligations the degradation of investigative capability will be significant.<sup>90</sup>

5.99 The AGD noted that there was evidence that this capability was already diminishing:

---

87 Australian Federal Police, *Submission No. 163*, p. 15. See also ASIO, *Submission No. 209*, p. 1; Attorney-General's Department, *Submission No. 218*, p. 1

88 Australian Federal Police, *Submission No. 163*, p. 15. See also Attorney-General's Department, *Submission No. 218*, p. 7

89 Victoria Police, *Submission No. 200*, p. 5. See also Attorney-General's Department, *Submission No. 218*, p. 7;

90 Corruption and Crime Commission of Western Australian, *Submission No. 156*, p. 11. See also Australian Competition and Consumer Commission, *Submission No. 192*, p. 1

Anecdotal reporting from agencies is that increasingly requests for telecommunications data are not being met as carriers do not retain the particular telecommunications data requested. Unfulfilled requests waste agency resources, inhibit the making of requests, and can lead to investigations being stalled or abandoned with crimes going unsolved.<sup>91</sup>

- 5.100 Furthermore, the AGD disagreed with the submitters who suggested that a data preservation scheme would be more appropriate:

Data preservation involves a C/CSP preserving specific telecommunications data identified by an agency that it has available on its network in relation to a relevant investigation or intelligence gathering activity on notification by an agency. Given the current authority under the TIA Act for agencies to access telecommunications data from a C/CSP when it has been identified as being relevant to a specific investigation or intelligence gathering activity, agencies already have the ability to access telecommunications data that the C/CSP has on hand at the time of the request or that comes into existence into the future, negating the need for data preservation.<sup>92</sup>

- 5.101 The AFP stated that a system of mandatory data retention would not mean any actual expansion in the powers of police and security agencies, and thus would not constitute an increased intrusion into the privacy of individuals:

The development of a data retention proposal is intended to ensure a national and systematic approach is taken for the availability of non-content telecommunications data for investigative purposes. Data retention would not give agencies new powers. Rather it would ensure that existing investigative capabilities remained available and were adapted to these changes in industry.<sup>93</sup>

- 5.102 Furthermore, the AFP emphasised that there are constraints on the use of communications data in the current legislation:

The TIA Act provides a high level of accountability and strict access requirements to obtain telecommunications information. These constraints recognise the responsibility of government to manage the competing interests of privacy and the expectations of the community that unlawful activity will be investigated and prosecuted, as well as the

---

91 Attorney-General's Department, *Submission No. 218*, p. 8.

92 Attorney-General's Department, *Submission No. 218*, p. 8.

93 Australian Federal Police, *Submission No. 163*, p. 16. See also NSW Government, *Submission No. 148*, p. 3

important role that the telecommunications industry plays in supporting law enforcement and investigative activities.<sup>94</sup>

- 5.103 The AFP argued that retaining limited data on internet use bears some similarity to the current regime:

Access to subscriber or account holder data is comparable in intrusiveness to open source information such as traditional fixed line telephone directories. It aids law enforcement in obtaining information to help establish further avenues of inquiry. For IP's where there are no analogous provisions to the directory service concept this non-content communications account data is imperative.<sup>95</sup>

- 5.104 Furthermore, the AFP, ASIO and the Australian Crime Commission (ACC) stated in their joint submission that they 'do not want the internet browsing history of every customer of an ISP to be retained'.<sup>96</sup>

- 5.105 These agencies recognised that browsing data may be considered the same thing as content, and thus noted that 'the TIA Act does not permit the disclosure of the contents or substance of a communication without a warrant', and further that they are not 'seeking any changes to this'.<sup>97</sup>

- 5.106 In regard to the difficulties of separating content from data in some cases, the AFP, ASIO and the ACC stated that the EU experience indicates that it is possible to separate the two, and further that 'the suggestion that it is not possible... is not consistent with information and feedback we have received from industry vendors'.<sup>98</sup>

- 5.107 Furthermore, the AGD told the Committee that there were safeguards in place in terms of separating data from content:

But the safeguard is that a law enforcement agency has to satisfy internally that they are seeking information that would fall within a definition of data, and it is very clear that they cannot ask for anything that is content. The final decision on that is with the industry player, and if they cannot extrapolate data from content, then they cannot disclose that. In relation to data retention, there has never been a suggestion that it would be anything to do with web browsing where this problem has been identified.<sup>99</sup>

---

94 Australian Federal Police, *Submission No. 163*, p. 16.

95 Australian Federal Police, *Submission No. 163*, p. 16.

96 AFP, ASIO and ACC, *Submission No. 227*, p. 3.

97 AFP, ASIO and ACC, *Submission No. 227*, p. 8.

98 AFP, ASIO and ACC, *Submission No. 227*, p. 8.

99 Ms Catherine Smith, *Transcript*, 2 November 2012, p. 3.



- 5.108 At a public hearing, the AFP told the Committee that privacy was central to any new or reformed regime around data retention:

I also want to be clear to the Committee that we understand the importance of individual privacy and we support this as a fundamental right in this country. I acknowledge that any reform in this area must be premised on maintaining appropriate levels of accountability for both intercepting agencies and industry in order to protect these rights.<sup>100</sup>

- 5.109 ASIO also told the Committee that there are currently safeguards in place when it comes to the use of communications data:

ASIO accesses telecommunications-associated data (i.e. not content) from carriers/carriage service providers under internal authorisations which may only be made where the relevant ASIO officer is satisfied that the disclosure of the data specified in the authorisation would be in connection with the performance of ASIO's legal functions (and for no other purpose).<sup>101</sup>

- 5.110 Similarly, AGD noted the privacy protections that are a part of the TIA Act:

The TIA Act contains numerous restrictions on the access, use and disclosure of communications lawfully obtained by agencies as well as comprehensive record keeping and reporting requirements with independent oversight. Broadly the prescriptive nature of the exceptions reflects the intrusive nature of the collection of the information as well as public expectations about how this information may be dealt with.<sup>102</sup>

- 5.111 Furthermore, ASIO noted that it always acts to ensure any access to communications data conform to the following guidelines:

- inquiries and investigations are to be undertaken using as little intrusion into individual privacy as possible;
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence.<sup>103</sup>

- 5.112 These protections notwithstanding, the AGD was supportive of the idea of inserting a privacy focused objects clause into the TIA Act as it 'will complement

---

100 Commissioner Negus, *Transcript*, 26 September 2012, p. 19.

101 ASIO, *Submission No. 209*, p. 3.

102 Attorney-General's Department, *Submission No. 218*, p. 10.

103 ASIO, *Submission No. 209*, p. 3.

the numerous safeguards built into the operation of the TIA Act by underpinning the ongoing interpretation of obligations under the Act.’<sup>104</sup>

**Box 5.2 Law enforcement and national security agencies’ use of communications data**

‘During a recent murder investigation there were a number of open lines of inquiry. When a human source provided information implicating a particular, previously unknown, person as responsible for the murder, telephone billing records were used to link the person nominated by the human source to another key suspect. The billing records also ultimately resulted in other lines of enquiry being discounted. The link between two of the principal offenders could not have been easily made without access to reliable telecommunications data. All the persons involved in that matter have been charged with the murder and associated offences and are currently before the courts.’ (Letter from Attorney-General Nicola Roxon to the Hon Anthony Byrne MP, 17 September 2012, Appendix E.)

‘For example, the [Queensland Crime and Misconduct Commission] CMC recently identified significant on-line sharing of child exploitation material by the principal target who declared that he was abusing children. The principal target was based in Queensland. The investigative team provided information to the ISP identifying the internet service being used. The Carrier was unable to advise the CMC of the subscriber details for the principal target, despite the on-line sharing of child exploitation material being less than 24 hours prior. This resulted in the CMC not being able to identify the principal target’s precise location or true identity.’ (Queensland Crime and Misconduct Commission, *Submission No 147*, p. 8.)

‘During 2010 an Operation obtained prospective call associated data (CAD) Authorisations in relation to a person suspected of war crime offences contrary to section 7(2)(a) of the Geneva Conventions Act 1957, namely torture, inhuman treatment and wilfully causing suffering or serious injury. The suspect was wanted for extradition to Croatia to face trial for these offences and was attempting to avoid location. The AFP’s CAD Authorisations did not involve the provision of any content of the suspect’s communications however the information the non-content data provided investigators regarding the general geographical location of the targets mobile handset was instrumental in assisting the AFP successfully locate the target.’ (Australian Federal Police, *Submission No. 163*, p. 17.)

‘ASIO receives intelligence that a particular IP address is subject to cyber attack. ASIO would need to identify who that IP address is assigned to before it could warn them that their computer has been taken over and their information stolen, and to commence working with them to improve their IT security.’ (ASIO, Australian Crime Commission and Australian Federal Police, *Submission No. 227*, p. 6.)

<sup>104</sup> Attorney-General’s Department, *Submission No. 218*, p. 10.

## Security

### Community views

5.113 A very large number of the objections to data retention related to the security of the data retained.

5.114 The Australian Privacy Foundation told the Committee that mandatory data retention was actually ‘contrary to security objectives’:

Mandating the creation and storage of records of communications that would not otherwise be kept increases risk and vulnerability, creating additional ‘honeypots’ of valuable personal information that would be a target for hackers and risk multiple abuses.<sup>105</sup>

5.115 Mr Bernard Keane told the Committee that such ‘honeypots’ would be a tempting target for criminals, regardless of the protections in place:

Even assuming a strong commitment to data security by providers and a statutory law for data protection by government, such repositories of information would be highly-prized treasure troves for organised crime, corporations and even foreign governments, and inevitably targeted by crackers.<sup>106</sup>

5.116 Senator Ludlam was also concerned about the potential for retained data to be hacked, noting:

The vast amounts of data that would be retained poses a security threat because it would be vulnerable to theft and hacking by unauthorised persons or governments, private entities or criminal actors.<sup>107</sup>

5.117 The potential for hackers and other criminals to access retained data was also raised by Dr Bendall:

Retaining the data would create a massive security risk if an ISP suffers a breach of security, including a significant risk of identity theft. The immense amount of data would also create an incentive for hackers to view ISPs as a target.<sup>108</sup>

5.118 Mr Nazer considered the risks posed by hackers and criminals to be far greater than those posed by government agencies accessing the data:

---

<sup>105</sup> Australian Privacy Foundation, *Submission No. 162*, pp. 9-10.

<sup>106</sup> Mr Bernard Keane, *Submission No. 117*, p. 15.

<sup>107</sup> Senator Scott Ludlam, *Submission No. 146*, p. 6.

<sup>108</sup> Victorian Privacy Commissioner, *Submission No. 109*, p. 8.

If all Australian's communications are stored, a security breach will expose data from hundreds of thousands, or even millions, of customers at once. Thus, while there is only very small probability that a particular user's retained data will ever be useful to law enforcement, there is a much larger probability that the user's data will be the subject of a security breach.<sup>109</sup>

- 5.119 AMTA and the Communications Alliance noted at a public hearing that different C/CSPs have different capabilities when it comes to the security of any retained data:

There are large entities within the industry that are very skilled and expert and experienced but, with the changing dynamics in this sector and the number of entities in the sector, under a data retention regime there would be a wide range of people who do not have those skills and there would be attendant risks to privacy.<sup>110</sup>

- 5.120 Furthermore, the security threats to the retained data may originate within the telecommunications service providers themselves. Electronic Frontiers Australia (EFA) raised a recent incident where Telstra allegedly harvested 'the URLs visited by customers of its NextG mobile service in order to provide this information to a foreign company'. According to EFA, this was illustrative of what could occur:

This incident also demonstrates the risk of misuse of data by organisations for their own internal marketing purposes, which is a serious likelihood as they will seek to offset the significant costs associated with maintaining storage facilities for such large volumes of data.<sup>111</sup>

- 5.121 Vodafone also commented on the potential for security breaches, particularly if the URLs associated with browsing histories were retained:

At the moment the information is not particularly interesting – it is just an event – so very few rogues would get a significant benefit from hacking into our billing records, whereas if it starts to be about which URLs you went to and tracking your location in a lot of detail then that would be quite problematic.<sup>112</sup>

- 5.122 EFA also noted that the security risks inherent in data retention vary according to the size and capabilities of the organisation retaining the data. In EFA's view,

---

109 Mr Daniel Nazer, *Submission No. 110*, p. 5.

110 Mr Chris Althaus, *Transcript*, 14 September 2012, p. 31.

111 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

112 Mr Matthew Lobb, *Transcript*, 27 September 2012, p. 18.

given that 'reports of significant data breaches' occur 'almost daily', it is 'all but guaranteed' that the retained data would be compromised.<sup>113</sup> NSW Young Lawyers noted that, in recent months, several major companies have had customer data stolen, including Twitter, Yahoo and LinkedIn.<sup>114</sup> Mr Quick noted his concern that, were Telstra to be similarly hacked, 'millions of Australians would have their personal information shared across the globe'.<sup>115</sup> Mr Daniel Black argued that C/CSPs do not have the 'sufficient skill level' to effectively protect data.<sup>116</sup>

- 5.123 The Internet Industry Association (IIA), an industry body representing a wide range of businesses and individuals involved in internet commerce, also saw a potential for any retained data to be hacked were it not stored securely, noting that:

...during the period of the Inquiry the international hacktivist group Anonymous has been reported to have laid claims to be responsible for a number of attacks on networks and websites to obtain secure data in protest of the [data retention] proposal.<sup>117</sup>

- 5.124 The IIA raised a similar concern:

Indeed most recently the vulnerability for further exposure was highlighted by the so-called hacktivist group 'Anonymous' who exposed data belonging to a prominent service provide.<sup>118</sup>

- 5.125 Furthermore, the IIA told the Committee that these attacks:

...highlight the need to ensure that any proposed reforms imposed on C/CSPs are cognisant of the level of security mechanisms required to protect such data.<sup>119</sup>

- 5.126 Australian Lawyers for Human Rights also emphasised the security threat to any retained data, and noted that even large C/CSPs have some problems protecting their data from hacking:

While the Committee's terms of reference which contain the proposals suggest guidelines on security of stored data, there have been a substantial number of recent breaches of security, resulting in the disclosure of private user data. These disclosures have not been by small

---

113 Electronic Frontiers Australia, *Submission No. 121*, p. 5.

114 NSW Young Lawyers, *Submission No. 133*, p. 11.

115 Mr Ian Quick, *Submission No. 95*, p. 14.

116 Mr Daniel Black, *Submission No. 97*, p. 6.

117 Internet Industry Association, *Submission No. 187*, p. 7.

118 Internet Society of Australia, *Submission No. 145*, p. 5.

119 Internet Industry Association, *Submission No. 187*, p. 7.

businesses or organisations which lack the financial means to employ or train staff who are capable of managing secure environments.<sup>120</sup>

- 5.127 Mr R Batten related his concerns about the security of retained data from hacking attempts to the privacy of customers. Mr Batten argued that data retention diminishes the ability of individuals to protect their information:

With data and identity theft now such a serious risk for the community, people have the right to protect their information. By mandating that all service providers retain user data, you remove the ability of citizens to effectively protect themselves from data and identity theft... This proposal would create virtual treasure troves for such thieves to raid and citizens would be able to do nothing to protect themselves.<sup>121</sup>

- 5.128 Likewise, Mr R Wigan was concerned about the enticing effect such a repository of personal data would have on criminals, noting that such a concentration of data places 'the community at risk', especially if it includes internet browsing data:

The ISP databases containing these materials will be a honeypot like no other, and breaches inevitable... with all the passwords and other security protocols undermined thereby.<sup>122</sup>

- 5.129 Mr Mark Newton also expressed reservations about the security implications of creating 'enormous silos' of data:

Data retention measures make our society less secure, by creating enormous silos of identifiable information in readily attackable locations. One single security breach risks losing everything, on a scale that leaves the United States' experience with Wikileaks in the shade. It is contemptible that the Government has learned no lessons from its own Wikileaks exposure, and still believes that concentrating large troves of leakable, attackable private data is a good idea.<sup>123</sup>

- 5.130 As a result of the concerns surrounding the ability of C/CSPs to effectively secure this data, and given that no C/CSP can ever be entirely certain the data is safe, Mr Daniel Black argued that it would be best if the data did not exist.<sup>124</sup>

- 5.131 Similarly, the IIA argued that the data collected should be kept to a minimum:

---

120 Australian Lawyers for Human Rights, *Submission No. 194*, p. 8.

121 Mr R Batten, *Submission No. 50*, p. 6.

122 Mr R Wigan, *Submission No. 178*, p. 2.

123 Mr Mark Newton, *Submission No. 87*, p. 9.

124 Mr Daniel Black, *Submission No. 157*, p. 12.

Where ever there is an incentive for criminals to gain access to certain types of data then protecting and securing access to that data becomes more of a time, cost and technology burden. It is therefore important to ensure that data is not collected unnecessarily and that any proposals for retention of that data for extended periods can be justified by clearly demonstrating the necessity of that data to law enforcement activities.<sup>125</sup>

5.132 Australian Lawyers for Human Rights agreed with this view, noting that:

Focusing on privacy, security standards and providing that the minimum amount of confidential data is retained for the smallest period of time possible would afford legitimate users a greater expectation of privacy, safety and less scope for exploitation of their data by unscrupulous third parties.<sup>126</sup>

5.133 According to Mr Bernard Keane, in some cases the data retained needs to be protected from lax processes within the organisations retaining the data:

It has become clear over the last 18 months that even large corporations with strong incentives to keep data secure are vulnerable to cracking by organised crime, other states or activists, or simply lazy about security of personal information. This has included the Australia telecommunications provider Vodafone, which was revealed in early 2011 to have allowed – not via cracking or illegal action by outside actors, but through its own poor internal processes – widespread access to personal information about its 4 million customers.<sup>127</sup>

5.134 These concerns about security could result in any retained data having limited evidentiary value, according to Mr Keane:

The recent history of personal information security in Australia and overseas suggests that both citizens and law enforcement agencies, intelligence agencies and prosecutors can have little confidence that information compiled under data retention laws would be effectively secured by all companies required to hold it, either from a privacy or from a investigative/prosecutorial point of view.<sup>128</sup>

5.135 Mr Black took a different approach, arguing that data breaches could lead to a loss of confidence of Australian internet users, and have a similar ‘chilling effect’ to that discussed in the previous section:

---

125 Internet Industry Association, *Submission No. 187*, p. 7.

126 Australian Lawyers for Human Rights, *Submission No. 194*, p. 8.

127 Mr Bernard Keane, *Submission No. 117*, p. 15.

128 Mr Bernard Keane, *Submission No. 117*, p. 15.

Should any number of high profile leaks or revelations occur in relation to data from this data retention scheme, then the confidence of the Australian internet user would be compromised. Such loss in public confidence could result in a 'chilling effect' as users turn away from using the Internet for personal affairs. Alternately some people could turn to more secure means of masking their identity such as proxies or [virtual private networks] which could actually result in a net negative effect on law enforcement efforts as people train themselves to become more conscious of potential surveillance and learn how to more effectively bypass such surveillance, mask their identity or cover their tracks.<sup>129</sup>

- 5.136 Despite its opposition to mandatory data retention more generally, Blueprint for Free Speech argued that C/CSPs should not be responsible for storing any data retained, as they were 'not adequately equipped to protect large quantities of information'. They elaborated on this concern:

Imposing an obligation on service providers to protect data is not an adequate solution to this problem. If anyone is going to keep data for government purposes – and we do not believe anyone should – it should be the Government, not the private sector, and appropriate constraints on its storage, access and disposal must be put in place.<sup>130</sup>

- 5.137 Senetas made a similar point, recommending:

...that the government mandate how collected and retained data is secured – both in motion (when moving between locations) and at rest (when stored) through certified encryption technology and a regime for data breach notification to ensure the interests of all stakeholders is aligned.<sup>131</sup>

- 5.138 The Pirate Party emphasised that the nature of the potential threats to the security of the data would require some form of controls to prevent unauthorised access:

Data retained under this policy would need to be stored in a secure manner which would be capable of preventing unauthorised access; either internally by employees of the company or organisation, or any external party (e.g. hackers, organised crime, foreign intelligence organisations, etc). Access controls would be required to prevent unauthorised access and to provide a thorough audit trail of all access to the system. Access controls and logging systems would need to be

---

129 Mr Daniel Black, *Submission No. 157*, p. 12.

130 Blueprint for Free Speech, *Submission No. 165*, p. 6.

131 Senetas, *Submission No. 237*, p. 1.



designed in a manner which prevents tampering with those logs in order to guarantee fidelity of those records.<sup>132</sup>

5.139 Similarly, in addition to making sure the data was stored securely, iiNet saw a need for effective accountability measures to make sure the retained data was secure from misuse. iiNet argued that the government needs to ‘assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms’.<sup>133</sup>

5.140 The Pirate Party noted that the data retained would ‘need to be securely backed up’ and that this backup system would be more complex than is the norm with backup systems. It posited that it would need to include the following:

- Backups older than the mandatory retention period would need to be purged in a similar manner to that of the data retention system.
- The backups would need to be protected by similar access controls to the data retention system.
- A means of ensuring that backups could not be ‘restored’ to another system by someone familiar with the system in order to freely access that data. Were that to occur they could retrieve any data, copy it and then wipe the system on which the backup had been restored to in order to conceal their actions.
- The amount of data retained, even when limited to traffic data, would be huge, even if compression and encryption were used when storing the data.<sup>134</sup>

5.141 The Pirate Party raised the need for the retained data to be securely destroyed once the retention period had expired:

The data would also need to be stored in a manner such that data no longer covered by the mandatory retention period (e.g. more than two years old) can be securely destroyed.<sup>135</sup>

## Law enforcement and national security agencies’ views

5.142 In regard to the security of the data captured and retained, the AFP, ASIO and the ACC stated that analogous data is retained and protected by providers already:

Some data, including personal information such as subscriber details, is already collected and retained by industry. The protection of this data remains paramount and is one of the main drivers behind the proposed

---

132 Pirate Party, *Submission No. 134*, p. 25.

133 iiNet, *Submission No. 108*, p. 13.

134 Pirate Party, *Submission No. 134*, pp. 25-6.

135 Pirate Party, *Submission No. 134*, p. 25

Telecommunications Sector Security Reform which aim to increase the level of security in telecommunications networks.<sup>136</sup>

5.143 Furthermore, the AFP, ASIO and the ACC noted that under the National Privacy Principles telecommunications and internet service providers are already required to 'take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access, modification or disclosure'.<sup>137</sup>

5.144 The Office of Australian Information Commissioner (OAIC) also related the need for retained data to be stored securely to the proposed telecommunications sector security reform, noting that:

...the OAIC supports possible amendments to the Telecommunications Act to create an industry wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference.<sup>138</sup>

5.145 The OAIC stated that this reform was particularly important in light of any future potential data retention regime.<sup>139</sup>

5.146 Dr Bendall told the Committee that Australia does not have a data breach notification scheme, stating:

...where there is a major data breach there is no specific legal impetus for those organisations to notify the individuals involved in order to mitigate their losses—for instance, even where it involves financial information and that sort of thing. My interpretation of the privacy legislation is that the information security principle would include some responsibility to do that because it mandates them to take reasonable steps to prevent misuse or unauthorised disclosure. But it is not a specific, unlike in other jurisdictions...<sup>140</sup>

5.147 The AGD made a similar point, noting:

Although many companies voluntarily report data breaches to the Office of the Australian Information Commissioner (OAIC), there is no requirement under the Privacy Act to notify the OAIC or any other individual in the event of a data breach.<sup>141</sup>

5.148 Similarly to Senetas, the OAIC suggested:

---

136 AFP, ASIO and ACC, *Submission No. 227*, p. 8.

137 AFP, ASIO and ACC, *Submission No. 227*, p. 9.

138 Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

139 Office of the Australian Information Commissioner, *Submission No. 183*, p. 16.

140 Dr Bendall, *Transcript*, 5 September 2012, p. 4.

141 Attorney-General's Department, *Submission No. 235*, p. 21.

While notification of a data breach is currently not required by the Privacy Act, the OAIC suggests that it be considered as part of the proposed framework as an important mitigation strategy against privacy risks.<sup>142</sup>

5.149 In this regard, the AGD noted the role that mandatory data breach notification requirements could play:

If enacted, mandatory data breach notification laws could complement the current legislative security requirements and a data retention regime in a least four ways by: (1) mitigating the consequences of a breach; (2) creating incentives to improve security; (3) tracking incidents and providing information in the public interest; and (4) maintaining community confidence in legislative privacy laws.<sup>143</sup>

5.150 As such, AGD noted that:

...on 17 October 2012, the Attorney-General released a Discussion Paper entitled Australian Privacy Breach Notification which has sought views by 23 November 2012 on the possible introduction of mandatory data breach notification laws. [...]The Government is currently considering responses to the discussion paper.<sup>144</sup>

5.151 Telecommunications sector security reform is discussed in Chapter Three of this report.

## Feasibility and efficacy

### Community views

5.152 Several submitters raised concerns about the feasibility of any potential data retention regime, and whether it would be an effective tool for law enforcement and national security agencies. For instance, the Law Council noted that it was 'not clear' how such a regime would be 'technically feasible or even useful'.<sup>145</sup>

5.153 In this regard, the Law Council raised several questions which it considered require an answer before any mandatory data retention regime is introduced:

Once the data has been retained, how will it be matched with a particular person or communication? How will it be verified, and if it is used as evidence in court, how will it be protected from public disclosure? In

---

142 Office of the Australian Information Commissioner, *Submission No. 183*, p. 20.

143 Attorney-General's Department, *Submission No. 235*, p. 21.

144 Attorney-General's Department, *Submission No. 235*, p. 21.

145 Law Council, *Submission No. 108*, p. 38.

addition, how will authorised agencies deal with the sheer volume of data retained when attempting to identify and request the data needed for a particular investigation?<sup>146</sup>

- 5.154 The Internet Society of Australia drew the volume of data that would be produced to the Committee's attention, noting that it would be difficult to deal with:

...the capacity of modern network equipment to produce terabytes of data with attendant storage, management and analysis costs for both the communications service providers as well as law enforcement agencies should not be underestimated. The potential for law enforcement agencies to be swamped by data is very real.<sup>147</sup>

- 5.155 Likewise, Ms Stella Gray also commented on the volume of data that would be generated by capturing data on web browsing:

A web browser hops through multiple IP addresses before reaching its destination to the page a user is navigating to. A web user is not in control of every IP address their web browser visits. Dozens of analytic trackers (measuring page view statistics) and advertising servers all run in the background on many websites that people frequent daily. That is a lot data that CSPs will need to be trusted to store, and a lot of data that law enforcement will need to sift through every time they are suspicious of someone.<sup>148</sup>

- 5.156 It should be noted that these views on feasibility, particularly as they relate to the amount of data that would be generated, were based on the assumption that the data would include URLs. Given that the Attorney-General has subsequently ruled out retention of data relating to internet browsing histories, the volume of data that would be retained is significantly reduced.

- 5.157 The Internet Industry Association raised the difficulties presented by the disaggregated nature of the data, particularly when it involves overseas countries:

Another key issue is that service supply in the internet environment is disaggregated – there are many over the top (OTT) services ranging from things like Hotmail, Gmail, instant messaging, etc. to social networking such as Facebook, to Cloud storage and application hosting. If those

---

146 Law Council, *Submission No. 108*, p. 38.

147 Internet Society of Australia, *Submission No. 145*, p. 4.

148 Ms Stella Gray, *Submission No. 152*, p. 5. See also Pirate Party, *Submission No. 134*, p. 26.

services are hosted outside of Australia, then data retention obligations have little to no effect.<sup>149</sup>

- 5.158 Telstra raised a similar issue at a public hearing, noting that even if Australian providers were required to capture and retain communications data, it would still not be able to capture data from over the top services like Skype and other voice over the internet telephony services, YouTube or Google. Telstra elaborated on the effect this would have:

The simple evolution of technology would mean that we could not capture or provide any metadata or any content around something like Gmail, because it is Google owned, it is offshore and it is over the top on our network. The real value of what we might have in our data-retention scheme would be greatly diminished as soon as the good, organised criminals and potential terrorist cells knew that we were not capturing that data.<sup>150</sup>

- 5.159 However, iiNet told the Committee that it was still feasible to retain data relating to the source and destination of a particular communication, be it via traditional telephony or internet browsing:

Technically anything is possible, it is just a question of how much money you want to throw at it. We have not said it is too expensive for us, but if we are forced to do it we will pass those costs through and that is normal.<sup>151</sup>

- 5.160 One possible method of capturing and extracting relevant data that was raised during the course of this inquiry was Deep Packet Inspection (DPI). Telstra noted that, should a mandatory data retention regime proceed:

Where additional information was required that does not form part of Telstra's available pool of data then DPI could be one of the mechanisms available to meet these obligations.<sup>152</sup>

- 5.161 Telstra described its understanding of DPI:

DPI equipment is typically deployed for the purposes of inspecting [IP] traffic in detail (deep inspection of the IP packets). The results of such an inspection may be used, along with policy enforcement technology, to manage certain types of traffic. [...] DPI equipment may be deployed either 'in-line' to achieve policy enforcement outcomes (manage traffic

---

149 Internet Industry Association, *Submission No. 187*, p. 8.

150 Mr James Shaw, *Transcript*, 27 September 2012, p. 12.

151 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 51. See also Mr Chris Althaus, *Transcript*, 14 September 2012, p. 31; Mr Andrew Pam, *Transcript*, 5 September 2012, pp. 62-3.

152 Telstra, *Submission No. 238*, p. 1.

based on its type or intended use, for example VOIP calls to the emergency call service) or DPI may be deployed 'off to the side'. Deploying DPI 'off to the side' is used when carriers are analysing (but not altering) IP traffic on their network.<sup>153</sup> However, Telstra noted that, while it 'would be possible for a carrier to capture and extract specific data using DPI', this would depend on the 'configuration of the DPI equipment' and it would mean that 'the volume of data subject to such capture and extraction would need to be constrained.'<sup>154</sup>

- 5.162 In the context of the *Draft Communications Data Bill* currently under consideration in the UK, the Joint Committee on the Draft Communications Data Bill noted:

[DPI] would be used to isolate key pieces of information from data packets in a CSP's network traffic. The Home Office seemed confident that this was technically possible.<sup>155</sup>

- 5.163 The UK Joint Committee went on to note that the main technical challenge in terms of the feasibility of using DPI was 'dealing with encrypted data' captured from over the top service providers such as Gmail and Skype.<sup>156</sup>

- 5.164 In terms of whether DPI could be used to capture only data and not content, Telstra advised the Committee that:

DPI is able to be configured to perform in a range of different roles. It may be possible to configure DPI equipment to examine header data without inspecting content. This configuration is highly dependent on the volumes of data and specific meta-data being sought...this is a question of traffic volumes, equipment performance and cost.<sup>157</sup>

- 5.165 In addition to stating that any potential data retention regime would be difficult, although not impossible, to implement due to the size and nature of the data needing to be retained, some groups also questioned whether the data would be effective in assisting to combat crime and terrorism.

- 5.166 For instance, Telstra raised the possibility that the means C/CSPs use to obtain the data could result in issues if it is presented as evidence in courts:

<sup>153</sup> Telstra, *Submission No. 238*, p. 1.

<sup>154</sup> Telstra, *Submission No. 238*, p. 1.

<sup>155</sup> Joint Committee on the Draft Communications Data Bill, UK Parliament, *Draft Communications Data Bill*, December 2012, p. 30, viewed 18 December 2012, <[www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/](http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/)>.

<sup>156</sup> Joint Committee on the Draft Communications Data Bill, UK Parliament, *Draft Communications Data Bill*, December 2012, p. 30, viewed 18 December 2012, <[www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/](http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/)>.

<sup>157</sup> Telstra, *Submission No. 238*, p. 2.

With very few exceptions, the current communications data that C/CSPs provide to the [law enforcement and national security agencies] can be validated, by defence counsel, by comparison with a defendant's telecommunications service account ('bill'). This will no longer be the case with 'created' communications data and Telstra believes that prosecutors are highly likely to be challenged in court to substantiate the accuracy of the data in evidentiary proceedings.<sup>158</sup>

- 5.167 EFA thought it 'highly questionable' whether data retention would aid in the investigation of terrorism, organised crime, or other serious illegal activities:

It is worth noting that determined criminals will have little difficulty disguising or anonymising their communications. There are many relatively simple and very effective tools available that allow for the protection of communications from surveillance. While these tools will not be appealing to the vast majority of users as they can degrade connection speeds and reduce functionality, they are a viable option for those individuals that are determined to communicate in secrecy.<sup>159</sup>

- 5.168 Dr Bendall also expressed scepticism as to whether data retention would aid law enforcement and national security agencies due to the incentive this would provide to anonymise communications:

There is some evidence that I am aware of, from having read various reports, of that happening in other jurisdictions where people have engaged less with electronic transactions or they have done it in a way where they have used various devices to encrypt and anonymise their transactions. One of the concerns with that, of course, is that that actually lessens the amount of information available to law enforcement organisations.<sup>160</sup>

- 5.169 iiNet was sceptical that data retention would be effective, due to the ease with which individuals can mask their identity. iiNet discussed one example with the Committee at a public hearing:

We think it should be noted that in the internet environment a range of applications – apps – may run simultaneously over the same servers. These apps can emulate telephony or video communications, texts and other communications on the same platform using what is called internet protocol. Many of these apps allow a person wishing to mask either their

---

158 Telstra, *Submission No. 189*, p. 11.

159 Electronic Frontiers Australia, *Submission No. 121*, p. 4.

160 Dr Anthony Bendall, *Transcript*, 5 September 2012, p. 4.

identity or location via wireless networks, proxy servers or other techniques to communicate in a covert way.<sup>161</sup>

- 5.170 Blueprint for Free Speech provided the Committee with a large volume of material relating largely to the efficacy of the EU Data Retention Directive in preventing crime. This material led Blueprint for Free Speech to conclude that:

There is no evidence to suggest data retention would assist with the prevention of crime or terrorism. A 2011 study of Germany's Data Retention Directive found it had no impact on either the effectiveness of criminal investigations or the crime rate. Further, the study specifically found that countries *without* data retention laws are not more vulnerable to crime.<sup>162</sup>

- 5.171 According to one analysis conducted by Arbeitskreis Vorratsdatenspeicherung of the effectiveness of data retention in Germany provided to the Committee by Blueprint for Free Speech:

Blanket data retention can actually have a negative effect on the investigation of criminal acts. In order to avoid the recording of sensitive information personal information under a blanket data retention scheme, citizens increasingly resort to internet cafes, wireless internet access points, anonymisation services, public telephones, unregistered mobile telephone cards, non-electronic communications channels and suchlike. This avoidance behaviour can not only render retained data meaningless but even frustrate targeted investigation techniques (eg wiretaps) that would possibly have been of use to law enforcement in the absence of data retention. Because of this counterproductive effect, the usefulness of retained communications data in some investigation procedures does not imply that data retention makes the prosecution of serious crime more effective overall.<sup>163</sup>

- 5.172 Mr Ben Lever cited the same report in his submission, noting that:

It seems that under the current model - wherein most people are not surveilled, but certain persons suspected of crime are surveilled with warrants - many criminals will fail to take appropriate precautions, will use various telecommunication services, and will have that communication intercepted; however, under a data retention model - wherein all communication between citizens is monitored - criminals

---

161 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 47.

162 Blueprint for Free Speech, *Submission No. 165*, p. 6. Emphasis in original.

163 Arbeitskreis Vorratsdatenspeicherung, *Data Retention Effectiveness Report*, 20 May 2011. See also Mr Chris Berg, *Transcript*, 5 September 2012, p. 45.



know this and deliberately avoid using telecommunications, to the detriment of those listening in.<sup>164</sup>

5.173 The Pirate Party agreed with these perspectives on efficacy, noting:

It is likely that implementing data retention in Australia would have similar effects to those observed in Germany. The effect would not be to prevent organised crime or terrorism; it would merely result in greater concerted effort by organised criminals and terrorists to conceal their activities and communication. Meanwhile, the privacy and security of innocent, law abiding citizens would certainly be threatened and probably breached.<sup>165</sup>

5.174 Similarly, Mr Ian Quick told the Committee that those seeking to commit crimes will simply use alternative methods to communicate:

If everyone knows all internet traffic is monitored, people with things to hide - or who are just irritated with the government spying on everyone - will simply bypass the monitoring by either hiding what they are browsing or who is doing the browsing.<sup>166</sup>

5.175 Furthermore, Mr Quick listed a range of ways to avoid having communications data retained:

- Browsing with a public internet service ie internet café, public library.
- Using some else's wifi connection (many are not properly secured).
- Using someone else's computer, ie a friends or work colleague.
- Using Tor or a similar online anonymity tool.
- Using any number of open proxy services.
- Using a [virtual private network] to somewhere outside of Australia and browsing over that.<sup>167</sup>

5.176 Tor, originally developed by the US Navy, uses:

...a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that

---

<sup>164</sup> Mr Ben Lever, *Submission No. 71*, p. 3.

<sup>165</sup> Pirate Party, *Submission No. 134*, p. 28.

<sup>166</sup> Mr Ian Quick, *Submission No. 95*, p. 14. See also Liberty Victoria, *Submission No. 109*, p. 7; Pirate Party, *Submission No. 213*, p. 3; Mr Patrick Potter, *Submission No. 212*, p. 4; Mr Daniel Judge, *Submission No. 157*, p. 12;

<sup>167</sup> Mr Ian Quick, *Submission No. 95*, p. 14.

allow organizations and individuals to share information over public networks without compromising their privacy.<sup>168</sup>

5.177 Virtual Private Networks (VPNs) are similar, in that they allow users to anonymise their internet use by 'encrypt and tunnel their traffic to another country for retransmission'.<sup>169</sup>

5.178 Likewise, Mr Johann Trevaskis notes that there are yet more ways in which persons seeking to do so can mask their identity during online communications:

- A person who intended to communicate something about a serious offence on the internet could generate 'millions' of dummy exchanges on the internet. While those exchanges would all be recorded and available to law enforcement, the person could die of old age before the last exchange had been checked out by law enforcement.
- Every person who objected to the data retention proposal on principle could generate 'millions' of dummy exchanges on the internet thereby making the data retention mechanism itself less practical.
- Data retention for stored communications that are email can be avoided by anyone merely by not using the ISP for email. This is to be recommended anyway because anyone who uses their ISP's email address then finds it more difficult to change ISP. That is, national economic efficiency says that people should not use an email address provided by their ISP. (Hence, for example, if a person used the gmail.com web site for all their email needs, the ISP would never see a single email. It is true that the web traffic to gmail.com instead would be seen by the ISP but that raises a number of practical difficulties for 'data retention' as compared with simply keeping copies of emails that are being handled by the ISP.)<sup>170</sup>

5.179 In light of the questions about whether any data retention regime would be worthwhile pursuing, Mr Nazer considered that a cost-benefit analysis should be conducted.<sup>171</sup>

## Law enforcement and security agency views

5.180 The AGD responded to the concerns raised by telecommunications companies about over the top services, and the fact that the companies would have great difficulty capturing any data generated by these at a public hearing. The AGD noted that, because many of these over the top service providers are based in the United States:

168 Tor Project website, *About Tor*, viewed 15 November 2012, <[www.torproject.org/about/overview.html.en](http://www.torproject.org/about/overview.html.en)>.

169 Mr Cameron Blackwood, *Submission No. 208*, p. 3.

170 Mr Johann Trevaskis, *Submission No. 62*, p. 9.

171 Mr Daniel Nazer, *Submission No. 110*, p. 3.

There are ways through mutual assistance that we are able to access this information that has been held onto by the US providers. If they do retain the information offshore then it is unlikely that any law about data retention would apply to them, because the US law would actually override ours in that context. However, I think what we want to be satisfied of is that we can get access to the information. From what we understand from talking to the social network providers and these different providers in the US, they are happy to retain information as long as they are satisfied that a lawful order will come along at some point...<sup>172</sup>

5.181 Furthermore, the AGD noted that:

We have been advised, in the policy development work we were previously doing on this, that, if there is an obligation under Australian law which has extraterritorial application for these foreign service providers, they will actually be required – and we can compel them – to assist us in relation to the services they provide to Australians or provide in Australia. There will have to be a geographical boundary around this sort assistance. We cannot go and ask for assistance about something which is happening in another country. But, if the assistance is related to communications which, at some point, pass through the Australian telecommunications system, the advice we have had – or that we are working on – is that generally they will be able to be compelled. There are certainly ways – some as simple as terms and conditions of service. If they are Australian terms and conditions of service when you sign up in Australia, they will have the force of Australian law rather than the force of US law.<sup>173</sup>

5.182 In regard to whether data retention would be an effective tool for law enforcement, the AFP told that Committee that it already is a vital tool. Furthermore, the AFP argued that, as the telecommunications sector changes, their ability to draw on communications data could potentially diminish:

In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications content and data, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity. The diversification of the sector and technological change mean that while a greater array of non-content communications data is being created increasingly less is being retained. This negatively impacts investigations and is exploited by individuals involved in the commission of a range of serious offences including

---

172 Ms Catherine Smith, *Transcript*, 2 November 2012, p. 6.

173 Ms Catherine Smith, *Transcript*, 2 November 2012, pp. 6-7.

cybercrime, terrorist activity and the exchange of child exploitation material.<sup>174</sup>

- 5.183 Given that, as stated by ASIO, the AFP and the ACC, communications data is 'essential for the majority of investigations':

Loss of access to such data, for technical or legal reasons, would result in a loss of a fundamental investigative capability and the ability of security and law enforcement agencies to function effectively.<sup>175</sup>

- 5.184 The AFP considered that if data retention were *not* made mandatory, it would lose important capabilities that would result in:

- Limited ability to track and pursue offenders in a timely and effective way;
- Limited ability to conduct thorough and complete investigations;
- Inability to present best evidence to courts;
- Inability for police to react to some life threatening situations;
- Inability to follow through on potential leads and gather evidence and identify criminals, and
- Ability for criminal enterprises / organised crime groups to exploit this vulnerability.<sup>176</sup>

- 5.185 Thus, it was submitted that mandatory data retention will not necessarily result in a direct decrease in crime or terrorism, or a direct increase in clearance rates for criminal investigations, but that failure to mandate data retention will result in a diminution of law enforcement and security agencies' ability to fulfil their functions over time.

- 5.186 The AGD contested the view presented above that data retention in the EU has not assisted in investigations:

The European Directive included a requirement for an evaluation of the application of the Directive and its impact which was to be prepared by the European Commission. This report was published on 18 April 2011. The report concluded that overall, the evaluation had demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU. The evaluation highlighted the lack of harmonisation in transposition of the directive in areas such as purpose limitation, retention periods and reimbursement of costs for industry (which is outside the scope of the Directive).<sup>177</sup>

---

174 Australian Federal Police, *Submission No. 163*, p. 18.

175 AFP, ASIO and ACC, *Submission No. 227*, p. 6.

176 Australian Federal Police, *Submission No. 163*, p. 17.

177 Attorney-General's Department, *Submission No. 218*, p. 9.

5.187 In response to concerns about criminals and terrorists turning to anonymisers like Tor and VPNs, the AGD told the Committee that:

...we are well aware that there are, unfortunately, as you mentioned, Tor and suchlike ways to very cleverly evade any level of detection. The advice that I have had from agencies is that still being able to determine patterns of behaviour through access to data, even if it is to get feels of where they are setting up their blockages, gives a pattern of particular behaviour.<sup>178</sup>

## Cost

5.188 A range of individuals and organisations – particularly C/CSPs – raised concerns in regard to the potential costs that any data retention regime could impose on C/CSPs and consumers of telecommunications services.

5.189 Telstra told the Committee that mandatory data retention would impose costs on C/CSPs:

Telstra believes that the costs involved in any new data creation and retention regime will be significant and we will need to undertake large scale and detailed technical feasibility studies in order to understand what network, IT, vendor changes would be necessary and the costs of implementation and compliance with any new data creation and retention regime.<sup>179</sup>

5.190 However, Telstra also noted that:

...it is impossible for Telstra to speculate on the significant costs or timeframes for compliance until Government has settled on the final form of any data retention regime.<sup>180</sup>

5.191 Mr Bruce Arnold, a lecturer in privacy law at the University of Canberra but submitting in a private capacity, discussed the reasons why mandatory data retention would impose costs on C/CSPs:

It involves substantial costs for connectivity providers and content hosts in the public and private sectors (eg mobile phone service providers, webhosting services, libraries and universities) that are being asked to act as agents of the state. The network management systems used by those organisations typically feature billing and customer support facets. They are not concerned with long-term data storage, particularly storage in

---

178 Ms Catherine Smith, *Transcript*, 2 November 2012, p. 4.

179 Telstra, *Submission No. 189*, p. 11. See also Mr Zull, *Transcript*, 5 September 2012, p. 10.

180 Telstra, *Submission No. 189*, p. 12.

forms that can be readily parsed by government agencies. Restructuring those systems to provide storage is non-trivial. Its implications involve a reduction of competition in the ISP sector, driving small ISPs out of business, and imposing a tangible regulatory burden on entrants to the social network service market along with other entities whose clients engage in electronic communication.<sup>181</sup>

5.192 EFA was similarly concerned about the costs to ISPs:

ISPs log certain types of data as part of their normal operations and for the purposes of billing or providing other services. However, maintaining records of all accessible data for long periods of time, as well as servicing law enforcement requests to access the data, would impose costs far above those of normal operations.<sup>182</sup>

5.193 EFA also raised the cost estimates of UK C/CSPs in relation to the UK data retention scheme, and that these costs would inevitably be passed on to consumers:

According to the UK Internet Service Providers' Association one large UK-based ISP estimated that it would cost £26m a year to set up a data retention system along with £9m a year in running costs. These are costs that would inevitably be passed directly on to Australian businesses and consumers in the form of higher connectivity and other service charges.<sup>183</sup>

5.194 AMTA and the Communications Alliance, basing their estimates on a data set similar to that of the EU Directive, attempted to quantify the likely setup costs to industry:

In terms of setup costs industry estimates place the cost of capture and retention at close to one hundred million dollars. If the source and destination IP addresses were to be included in the capture and retain requirement the setup costs would be likely to approach a figure in the region of five hundred to seven hundred million dollars (\$500 million - \$700 million). The inclusion of a single additional data element has the potential to increase the capture and retention cost by tens of millions of dollars.<sup>184</sup>

5.195 Mr Nazer commented on the disproportionate effect mandatory data retention would have on smaller providers:

---

181 Mr Bruce Arnold, *Submission No. 137*, p. 2.

182 Electronic Frontiers Australia, *Submission No. 121*, p. 7.

183 Electronic Frontiers Australia, *Submission No. 121*, p. 7.

184 AMTA and Communications Alliance, *Submission No. 114*, p. 14.

Smaller providers may not yet have the infrastructure to store the additional data. Large scale data storage requires expensive hardware, software, and data security expertise. This burden would be especially devastating to online service providers (such as social networking sites) that would not otherwise track the source data of communications. Moreover, many such companies are small start-ups and compete against companies from all over the world. Ultimately, the burden of data preservation could drive smaller communications companies out of business and send innovation overseas.<sup>185</sup>

- 5.196 At a public hearing, iiNet discussed the likely costs it would incur as a smaller provider. Basing this estimate on several assumptions, including that internet browsing data would be retained and that the volume of data generated by internet browsing will continue to increase at current rates:

We believe \$20 million for the IT equipment and \$10 million for the data centre building. That is to meet current levels. If we amortise the hardware over two years and the data centre over ten years, we estimate a cost of about \$1 million per month, plus power and overheads.<sup>186</sup>

- 5.197 Furthermore, Mr Dalby elaborated on the costs iiNet, and its customers, were likely to incur:

...assuming that we are efficient about it, we would still need, because of the growth in traffic, to double that to cater for two years, and we are therefore looking at something more like \$60 million for a start. That flows through to our customers. If we take that cost and determine what it will cost our customers when we pass it through, we are assuming an increase in the cost of a service – any one of our services – of about \$5 per month. That would be an increase to our customers.<sup>187</sup>

- 5.198 Telstra advised the Committee that even larger providers will incur significant costs as a result of mandatory data retention:

There are significant costs involved in all of this. There is a variety of costs. There is the cost of collating the data: collecting it off the network to begin with. Then there is the cost of putting it into storage. Then we have the cost of putting the security around that such that we have the integrity of the data in terms of the privacy of the customers and also the integrity of the data for evidentiary reasons for the agencies. Then we have the cost of making that data available to the agencies in a form that they can use for their investigations. Then, not to be overlooked – and it can be a

---

185 Mr Daniel Nazer, *Submission No. 110*, pp. 6-7.

186 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 48.

187 Mr Stephen Dalby, *Transcript*, 27 September 2012, p. 49.

significant cost – at the end of the whole life cycle of this we have the cost of construction of that data in a way in which the customers and others can be sure that we are looking after their interests. Equally, on the other side – and I do not think that this is a point should be lost in the debate here – is that the agencies themselves will face significant costs in that they will have costs of accessing that data and then manipulating and investigating it in a way that makes it usable for them and also their own destruction costs at the end of the process.<sup>188</sup>

- 5.199 Vodafone commented that the costs expand significantly when URLs or internet browsing data needs to be captured and retained:

In the case of data, the problem with data in this space is that a data stream can cover a whole number of URLs, a whole number of places you go onto the web. In location terms, if you are talking just about the cell, that is manageable; if you are talking about location within the cell and you are asking us to capture that data, that is an enormous expense. If it is as simple as a data session occurred and maybe if it went to the first URL then that is manageable. It would be expensive but it would be manageable. If it was every single URL they went to, the amount of data that was used in particular downloading events and similarly with the location, that is when the costs across all your categories increase dramatically and capture becomes extremely expensive – actually having the systems to get information for the agencies that we would not otherwise be interested in storing or capturing.<sup>189</sup>

- 5.200 Similarly, iiNet noted that there is a big difference between capturing data relating to internet telephony and other internet services:

...when iiNet provide a telephony service to a customer we have a similar range of information available to us. Whether we are providing that service over a conventional copper loop or via an internet service, we know the IP address of our customer making the call. When we start shifting into other internet content, if we provide that service via a mobile phone and we resell services from Vodafone's network and Optus's network, then all we see from those carriers is that our customer used the internet for an unstated purpose generally – there is a little exception to that. All we see as the reseller is that they used it for an unstated purpose and moved a certain amount of data. So we know that our customer did something, we do not know what they did. We do not know what website

---

188 Mr James Shaw, *Transcript*, 27 September 2012, p. 4.

189 Mr Matthew Lobb, *Transcript*, 27 September 2012, p. 21.



they connected to; we do not know what they downloaded; we just know that access happened.<sup>190</sup>

- 5.201 Furthermore, a large part of these costs were not in retaining data, but rather in generating and retrieving the data to begin with, as much of the data to be retained is not currently captured for business purposes. According to Telstra:

The storage of data is one of the lesser elements of the cost, although it does give rise, as I have said, to the privacy and security risks to protect that data and, not least, to protect its integrity also. But, certainly, the costs—for the system to retrieve it and to then create a way of retaining it and then making it accessible and then on the other side, the agency side, creating the ability for them to access, understand and use it—would be substantial, in our view.<sup>191</sup>

- 5.202 Ms Gray expressed a concern that potentially increased costs to consumers could ‘deprive people of lower socio-economic backgrounds’ of their ability to connect to the internet.<sup>192</sup>

- 5.203 In order to prevent any data retention regime negatively impacting C/CSPs and consumers, AMTA and the Communications Alliance noted their preference was for government to pay:

...so far as data retention is concerned, we believe that any move down the track of additional data retention requirements should be based on full cost-recovery from government, just as is occurring today in the UK.<sup>193</sup>

- 5.204 Similarly, the Australian Interactive Media Industry Association recommended:

The costs of fulfilling law enforcement requests should be met by the law enforcement authorities that request the information, and not directly or indirectly on service users.<sup>194</sup>

## Committee comment

- 5.205 The Committee received a great deal of evidence on the issue of a mandatory data retention regime. In addition to the public evidence presented in this

---

190 Mr John Lindsay, *Transcript*, 27 September 2012, p. 50.

191 Mrs Jane Van Beelen, *Transcript*, 27 September 2012, p. 11.

192 Ms Stella Gray, *Submission No. 152*, p. 5.

193 Mr John Stanton, *Transcript*, 14 September 2012, p. 29.

194 Australian Interactive Media Industry Association, *Submission No. 198*, p. 4. See also Mr Lobb, *Transcript*, 27 September 2012, p. 19.

chapter, the Committee took classified evidence. Both the public and the classified evidence have informed the Committee's consideration of this issue.

- 5.206 Throughout its deliberations, the Committee has grappled with the issue of how best to reconcile the important national security interests which, the agencies were unanimous, would be served by an appropriate mandatory data retention regime, and on the other hand with the very significant alteration of the relationship between the state and the citizen, which the introduction of such a regime would arguably involve. As well, the Committee has had to approach this task in the absence of any draft legislation, which would have enabled it to focus its consideration with greater precision. This was a serious constraint upon the capacity of the Committee to form recommendations.
- 5.207 There is no doubt that the enactment of a mandatory data retention regime would be of significant utility to the national security agencies in the performance of their intelligence, counter-terrorism and law enforcement functions. As well, it is clear that changes in the data retention practices of telecommunications providers mean that much data which was previously retained, in particular for billing purposes, is no longer retained; this has resulted in an actual degradation in the investigative capabilities of the national security agencies, which is likely to accelerate in the future.
- 5.208 However, the utility of such a regime to the national security agencies is not the only consideration. A mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed.
- 5.209 Ultimately, the choice between these two fundamental public values is a decision for Government to make.
- 5.210 The Committee would have been in a better position to assess the merits of such a scheme, and the public better placed to comment, had draft legislation been provided to it.
- 5.211 There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:
- any mandatory data retention regime should apply only to meta-data and exclude content;

- the controls on access to communications data remain the same as under the current regime;
- internet browsing data should be explicitly excluded;
- where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
- the data should be stored securely by making encryption mandatory;
- save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;
- the costs incurred by providers should be reimbursed by the Government;
- a robust, mandatory data breach notification scheme;
- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
- oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

## **Recommendation 42**

There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- any mandatory data retention regime should apply only to meta-data and exclude content;
- the controls on access to communications data remain the same as under the current regime;
- internet browsing data should be explicitly excluded;
- where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
- the data should be stored securely by making encryption mandatory;
- save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;
- the costs incurred by providers should be reimbursed by the Government;
- a robust, mandatory data breach notification scheme;
- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
- oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

**Recommendation 43**

**The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:**

- **there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;**
- **there should be an annual report on the operation of this scheme presented to Parliament; and**
- **the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.**

Hon Anthony Byrne MP

Chair





## Appendix A – List of submissions

1. O Stevens
2. M Simpson
3. M Britton
4. G Warrener
5. 'Adrian'
6. C Mather
7. 'James'
8. J Archer
9. S Ford
10. Office of the Inspector of the Independent Commission Against Corruption
11. S Clark
12. C Rose
13. C Veness (and three others in common form)
14. A Butcher
15. A Bartlett
16. D Turner
17. C Rogers
18. M Ginn
19. P Stevens
20. R Palmer (and 2,967 others in common form)
21. M Rieck
22. P Serwylo
23. M Angelico
24. V Knight
25. E Collins
26. R Leeman
27. Confidential
28. J McPherson
29. S Watkins

30. C Eden
31. K Grundy
32. J Stewart
33. Tasmania Police
34. P McKeon
35. Dr J Dowty
36. Gilbert + Tobin Centre for Public Law
37. Confidential
38. B Terry
39. R Varney
40. G Lloyd-Smith
41. Andrew Brunatti and Neveen Abdalla, Brunei Centre for Intelligence and Security Studies, Brunei University
42. Dr G Carne
43. P Kentwell
44. Name withheld
45. Confidential
46. Confidential
47. J Vallentine
48. M Abbey
49. E Roberts
50. R Batten
51. J Holmes
52. Confidential
53. J Fergeus (and 2,348 others in common form)
54. J Burnside AO QC
55. Name withheld
56. D Auchterlonie
57. Public Interest Advocacy Centre
58. B Ryan
59. Dr A Fry
60. N Jackson
61. S De Silva
62. J Trevaskis
63. R Bishop
64. R Williams
65. J Taylor
66. A Bettison
67. M Steele
68. L Virr
69. T Edwards
70. R Rzechowicz



- 
71. B Lever
  72. S Knox
  73. M Annesley
  74. W Tattersal
  75. R Stuart
  76. P Fraser
  77. Dr P Scully-Power AM
  78. G Capone
  79. Name withheld
  80. K Riley
  81. K Copsey
  82. M Roberts
  83. Australian Society of Archivists
  84. A O'Neill
  85. D Ruegg
  86. Hon P Dowding QC
  87. M Newton
  88. A Gasparini
  89. J Pavy
  90. B Griffiths
  91. A McDonnell
  92. A Judeh
  93. L Roscic
  94. A Blond
  95. I Quick
  96. Law Council of Australia
  97. D Black
  98. Media, Entertainment and Arts Alliance
  99. Confidential
  100. J Sinnamon
  101. N Hondros
  102. Commonwealth Ombudsman
  103. C Minassian
  104. Engineers Australia
  105. J Embury
  106. R Reid
  107. New South Wales Ombudsman
  108. iiNet
  109. Office of the Victorian Privacy Commissioner
  110. D Nazer
  111. F Glaum
  112. Cisco System Australia Pty Ltd

113. Vodafone Hutchison Australia
114. Australian Mobile Telecommunications Association and Communications Alliance
115. Macquarie Telecom
116. Unisys
117. B Keane
118. Department of Broadband, Communications and the Digital Economy
119. B O'Flaherty
120. Australian Taxation Office
121. Electronic Frontiers Australia
122. Australian Communications Consumer Action Network
123. A Pollard
124. Hobart Community Legal Service
125. Youngman Consultancy
126. A von Brasch
127. J Smith
128. Confidential
129. D Pickett
130. K Duddy
131. E Slayter
132. D Phillips
133. New South Wales Young Lawyers/ The Law Society of New South Wales
134. Pirate Party Australia
135. I Graham
136. K Lovett and M De Saxe
137. B Arnold
138. S Versteeg
139. Institute of Public Affairs
140. Human Rights Law Centre
141. Queensland Council of Civil Liberties
142. Castan Centre for Human Rights Law
143. Liberty Victoria
144. K Tranter
145. Internet Society of Australia
146. Senator S Ludlam
147. Queensland Crime and Misconduct Commission
148. New South Wales Government
149. Huawei Technologies Australia Pty Ltd
150. Confidential
151. J Vrakas

152. S Gray
153. A Hull
154. S Walker
155. D Georgette
156. Corruption and Crime Commission of Western Australia
157. D Judge
158. Name withheld
159. Confidential
160. B Allen
161. The Religious Society of Friends
162. Australian Privacy Foundation
163. Australian Federal Police
164. Professor J Wainer
165. Blueprint for Free Speech
166. Northern Territory Police
167. A Halter
168. Australian Customs and Border Protection Service
169. Confidential
170. S Brown
171. N Pastalatzis
172. Confidential
173. Confidential
174. Australian Commission for Law Enforcement Integrity
175. New South Wales Council for Civil Liberties
176. Confidential
177. Confidential
178. R Wigan
179. Confidential
180. Australian Industry Group
181. Confidential
182. Privacy International
183. Office of the Australian Information Commissioner
184. Tasmanian Association of Community Legal Centres
185. Inspector General of Intelligence and Security
186. Police Integrity Commission
187. Internet Industry Association
188. Confidential
189. Telstra
190. Confidential
191. Confidential
192. Australian Competition and Consumer Commission
193. Electronic Frontier Foundation

194. Australian Lawyers for Human Rights
195. D du Prie
196. L Lyons
197. Confidential
198. Australian Interactive Media Industry Association, Digital Policy Group
199. Confidential
200. Victoria Police
201. Confidential
202. N Crichton-Browne
203. Western Australia Police
204. Australian Crime Commission
205. N Crichton-Browne
206. Optus
207. Dr A Berglas
208. C Blackwood
209. Australian Security Intelligence Organisation
210. C Poole
211. Confidential
212. P Potter
213. Pirate Party Australia
214. Australian Mobile Telecommunications Association and Communications Alliance
215. Confidential
216. Confidential
217. Confidential
218. Attorney-General's Department
219. Australian Secret Intelligence Service
220. Office of the Victorian Privacy Commissioner
221. Western Australian Corruption and Crime Commission
222. New South Wales Council of Civil Liberties
223. Department of Immigration and Citizenship
224. Law Council of Australia
225. Australian Taxation Office
226. Australian Federal Police
227. Australian Security Intelligence Organisation, Australian Federal Police and Australian Crime Commission
228. Confidential
229. Confidential
230. Confidential
231. Confidential
232. Confidential

- 
- 233. P Burke
  - 234. Liberty Victoria
  - 235. Attorney-General's Department
  - 236. K Selvarajah
  - 237. Senetas Corporation
  - 238. Telstra
  - 239. Confidential
  - 240. Confidential



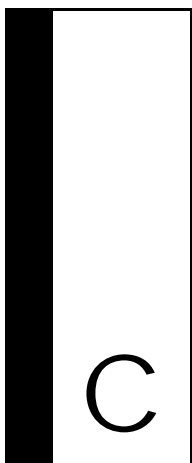


## Appendix B – List of exhibits

1. Hon. Peter Dowding SC  
*Article entitled 'Hidden Agenda', by Sally Neighbour, The Monthly Magazine*
2. Hon. Peter Dowding SC  
*Letter to the Monthly Magazine*
3. Hon. Peter Dowding SC  
*Letter to the Inspector General of Intelligence & Security*
4. James Sinnamon  
*Submission to the National Human Rights Consultation*
5. Janis Embury  
*Paper entitled 'Evaluation of Biomass Potential of some Australian Native Grasses'*
6. Janis Embury  
*Paper entitled 'Oil, Divestiture and National Security'*
7. Confidential
8. Stephen Brown  
*Article entitled 'Do we need a big online vacuum cleaner?'*
9. Stephen Brown  
*Article entitled 'Policy spying on internet, phone use without warrant'*
10. Stephen Brown  
*Article entitled 'Town halls to lose their snooping powers'*
11. Stephen Brown  
*Document entitled 'Constitution of the United States – Amendments – Bill of Rights'*
12. Stephen Brown  
*Letter entitled 'A Stasi state'*
13. Kellie Tranter  
*Transcript of interview, entitled 'Whistleblower: The NSA Is Lying–U.S. Government Has Copies of Most of Your Emails'*

14. Australian Greens  
*United Nations document entitled 'The promotion, protection and enjoyment of human rights on the Internet'*
15. Australian Greens  
*United Nations document entitled 'Promotion and protection of the right to freedom of opinion and expression'*
16. Janis Embury  
*The Security Threat of Unchecked Presidential Power*
17. Huawei Technologies (Australia) Pty Ltd  
*Cyber Security Perspectives: 21st century technology and security – a difficult marriage*
18. Cisco Systems Australia Pty Ltd  
*Cisco Company Profile*
19. Cisco Systems Australia Pty Ltd  
*Supply Chain Security at Cisco: An Overview*
20. Cisco Systems Australia Pty Ltd  
*BT Assure Adds Intelligence and Innovation for the New Security Reality*
21. Cisco Systems Australia Pty Ltd  
*Perspective: Not all Vendors and Products are Created Equal*
22. Cisco Systems Australia Pty Ltd  
*Cisco 2011 Annual Security Report – Highlighting Global Security Threats and Trends*
23. Cisco Systems Australia Pty Ltd  
*Insecure SCADA kit has hidden factory account, password*
24. Australian Crime Commission  
*Communication Complexity*
25. Australian Federal Police  
*Historical Subscriber Requests, Historical CCR Requests, Historical Telecommunications Requests*
26. Blueprint for Free Speech  
*The EU Experience (Human Rights and Efficacy)*
27. Confidential





## Appendix C – Witnesses who appeared at public hearings

**Melbourne, 5 September 2012**

**Office of the Victorian Privacy Commissioner**

Dr Anthony Bendall, Acting Privacy Commissioner

Mr Jason Forte, Senior Policy and Compliance Officer

**Macquarie Telecom**

Mr Matthew Healy, National Executive, Industry and Policy

Mr Christopher Zull, Senior Manager, Industry and Policy

**Monash University**

Dr Patrick Emerton, Associate, Castan Centre for Human Rights Law, Faculty of Law

**South Australia & Victoria Police**

Detective Superintendent Noel Bamford, Officer in Charge, Investigation Support Branch, South Australia Police

Senior Sergeant Darren Hamilton-Scott, Policy, Training and Governance, Special Projects Unit, Covert Services Division, Intelligence and Covert Support Department, Victoria Police

Acting Deputy Commissioner Jeff Pope, Victoria Police

Detective Inspector Gavan Seagrave, Officer in Charge, Special Projects Unit, Intelligence and Covert Support Department, Victoria Police

Detective Superintendent Paul Sheridan, Victoria Police

**Human Rights Law Centre**

Mr Benjamin Schokman, Director, International Human Rights Advocacy

**Institute of Public Affairs**

Mr Chris Berg, Director, Policy

Mr Simon Breheny, Director, Rule of Law Project

**Liberty Victoria**

Mr Michael Griffith, Policy Committee Member

Ms Lucy Maxwell, Member

Professor Spencer Zifcak, President

**Electronic Frontiers Australia**

Mr Andrew Pam, Board Member and Life Member

**Canberra, 14 September 2012****Australian Taxation Office**

Mr William Day, Assistant Commissioner, Criminal Law Treatments, Serious Non-compliance

Mr Greg Williams, Deputy Commissioner, Serious Non-compliance

**Law Council of Australia**

Mr Philip Boulten SC, Member, National Criminal Law Liaison Committee

Ms Rosemary Budavari, Co-Director, Criminal and Law and Human Rights

**Huawei Technologies (Australia) Pty Limited**

Mr John Lord (Rear Admiral (Rtd)), Chairman

Mr David Wang, Director, Business Development

**Australian Mobile Telecommunications Association**

Mr Chris Althaus, Chief Executive Officer

Ms Lisa Brown, Policy Manager

**Communications Alliance Ltd**

Mr Peter Froelich, Member Representative

Mr Michael Ryan, Member Representative

Mr John Stanton, Chief Executive Officer

Mr Visu Thangavelu, Project Manager

**Sydney, 26 September 2012****New South Wales Crime Commission**

Mr Peter Singleton, Commissioner

**Police Integrity Commission**

Ms Anne Marie Bauer, Manager, Telecommunications Interception Unit

Ms Michelle O'Brien, Commission Solicitor

**NSW, SA and Australian Federal Police Forces**

Commissioner Gary Burns, Commissioner of Police, South Australia Police

Acting Deputy Commissioner David Hudson, Special Operations, NSW Police Force

Commissioner Tony Negus, Australian Federal Police

Deputy Commissioner Michael Phelan, Australian Federal Police

Commissioner Andrew Scipione, Commissioner of Police, NSW Police Force

**Blueprint for Free Speech**

Mr Simon Wolfe, Head of Research

**New South Wales Council for Civil Liberties**

Mr David Bernie, Vice President

Dr Richard Bibby, Executive member and co-convenor, civil and Indigenous rights, police, security and antiterrorism powers and criminal justice subcommittee

Mr Stephen Blanks, Secretary

**Crime and Misconduct Commission Queensland**

Ms Kathleen Florian, Assistant Commissioner, Crime

**NSW Young Lawyers**

Mr Liam Boyle, Member, Public Law and Government Committee

Mr Patrick Gardner, Chair, Public Law and Government Committee

Miss Rebecca Welsh, Member, Public Law and Government Committee

**Ericsson Australia**

Mr Kursten Leins, General Manager, Strategic Marketing

**Sydney, 27 September 2012****Telstra Corporation Ltd**

Mr James Shaw, Director, Government Relations

Mrs Jane Van Beelen, Executive Director, Regulatory Affairs

Mr Darren Kane, Director, Corporate Security and Investigations

Ms Rachael Falk, Manager, Digital Privacy, Telstra Security Operations

**Vodafone Hutchison Australia**

Mr Matthew Lobb, General Manager, Industry Strategy and Public Policy

Mr David Moss, Agency Liaison Manager

**Australian Securities and Investments Commission**

Mr David Lusty, Special Counsel – Criminal Law

Mr Greg Tanzer, Commissioner

**Internet Society of Australia**

Ms Narelle Clark, President

**Gilbert and Tobin Centre of Public Law, University of New South Wales**

Dr Fergal Davis, Senior Lecturer

Ms Nicola McGarrity, Lecturer

**iiNet Ltd**

Mr Stephen Dalby, Chief Regulatory Officer

Mr John Lindsay, Chief Technology Officer

Mr David Ohri, Herbert Geer Lawyers, External Legal Counsel

**Canberra, 2 November 2012**

**Attorney-General's Department**

Mr Geoff McDonald, First Assistant Secretary, National Security Law and Policy Division

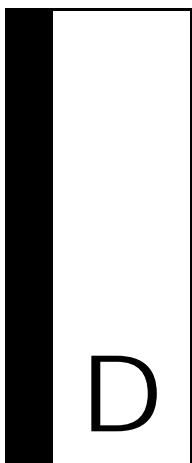
Mr Andrew Rice, Assistant Secretary, Cyber and Identity Security Policy Branch

Mr Mike Rothery, First Assistant Secretary, National Security Resilience Policy Division

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Mr Roger Wilkins AO, Secretary

Ms Annette Willing, Assistant Secretary, Security Law Branch



## Appendix D – Witnesses who appeared at private hearings

### Canberra, 14 September 2012

#### **Optus**

Mr David Epstein, Vice President, Corporate and Regulatory Affairs

Mr Gary Smith, Head, Regulatory Compliance

#### **Cisco**

Mr Tim Fawcett, General Manager, Government Relations and Policy

Mr Glenn Welby, Regional Manager, Security

### Canberra, 21 September 2012

#### **Inspector-General of Intelligence and Security**

Dr Vivienne Thom, Inspector-General of Intelligence and Security

Mr Jake Blight, Assistant Inspector-General of Intelligence and Security

#### **Australian Crime Commission**

Mr John Lawler AM APM, Chief Executive Officer

Dr David Lacey, Executive Director, People, Business Support and Stakeholder Relations

Miss Pip De Veau, National Manager, Legal Services

Mr Tim Wellsmore, Manager, Advanced Capabilities, Collections and Analytics Branch

#### **Commonwealth Ombudsman**

Ms Alison Larkins, Deputy Ombudsman

Mr Rodney Lee Walsh, Senior Assistant Ombudsman  
Ms Erica Welton, Director, Inspections

**Australian Federal Police**

Deputy Commissioner Michael Phelan APM  
Assistant Commissioner Neil Gaughan APM

**Australian Commission for Law Enforcement Integrity**

Mr Philip Moss, Integrity Commissioner  
Mr Stephen Hayward, Executive Director, Operations  
Ms Sarah Baker-Goldsmith, Principal Lawyer  
Mr Nicholas Sellars, Acting Executive Director, Strategic and Secretariat

**Canberra, 29 October 2012**

**Australian Security Intelligence Organisation**

Mr David Irvine AO, Director-General  
Assistant Director-General, Telecommunications Interception Capabilities  
First Assistant Director-General, Legal

**Australian Secret Intelligence Service**

Mr Nick Warner AO PSM, Director-General  
Deputy Director-General, Operations  
Deputy Director-General, Capability and Corporate Management  
General Counsel

**Defence Signals Directorate**

Mr Stephen Meekin, Deputy Secretary, Intelligence and Security  
Mr Ian McKenzie, Director, Defence Signals Directorate

**Canberra, 2 November 2012**

**Australian Security Intelligence Organisation**

Mr David Irvine AO, Director-General  
Assistant Director-General, Telecommunications Interception Capabilities  
First Assistant Director-General, Legal



## **Appendix E – Discussion paper**



Australian Government  
Attorney-General's Department

# **EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS**

A Discussion Paper to accompany consideration by the  
Parliamentary Joint Committee on Intelligence and Security  
of a package of national security ideas comprising proposals  
for telecommunications interception reform,  
telecommunications sector security reform and Australian  
intelligence community legislation reform

**July 2012**



**Table of Contents**

INTRODUCTION .....	3
TERMS OF REFERENCE - INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION. 6	
INTERCEPTION AND THE TIA ACT .....	12
1. Introduction .....	12
1.1 Effectiveness of lawful covert access to communications.....	14
1.2 The national security environment.....	14
1.3 Serious offences and serious contraventions – Commonwealth and State .....	15
1.4 Organised crime .....	16
1.5 Fundamentals of the current Act.....	17
2.1 Problems with the current approach.....	20
2.2 Creating a contemporary regime .....	22
3. Next Steps .....	28
TELECOMMUNICATIONS SECURITY SECTOR REFORM .....	29
1. Introduction .....	29
2. The Context .....	30
2.1 Australia’s Telecommunications Industry .....	30
2.2 National Security Risks .....	31
2.3 Current telecommunications regulatory environment .....	32
2.4 Analysis .....	33
3. Proposed Approach .....	33
3.1 Industry Consultation .....	34
3.2 Compliance Framework .....	35
3.3 Directions and penalties .....	37
3.4 Transition Arrangements .....	39

---

4. Next Steps .....	39
AUSTRALIAN INTELLIGENCE COMMUNITY LEGISLATION REFORM .....	40
1. Introduction .....	40
2. Matters the Government wishes to progress .....	41
2.1 Modernise and streamline ASIO's warrant provisions .....	41
2.2 Modernise the ASIO Act employment provisions .....	42
2.3 Clarify the authority of the Defence Imagery and Geospatial Organisation .....	44
3. Matters the Government is considering .....	46
3.1 Amend the ASIO Act to create an authorised intelligence operations scheme .....	46
3.2 Modernise and streamline ASIO's warrant provisions .....	47
3.3 Clarify ASIO's ability to cooperate with the private sector .....	49
3.4 Amend the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act.....	49
4. Matters on which the Government expressly seeks the views of the PJCS .....	50
4.1 Modernise and streamline ASIO's warrant provisions .....	50
4.2 Amend the Intelligence Services Act 2001 .....	51
5. Next Steps .....	55
CONCLUSION .....	56
GLOSSARY OF KEY TERMS .....	57

## INTRODUCTION

---

At the forefront of the Government's commitment to Australia is protecting our national security. In recent years terrorism has been an enduring national security threat. The world and our region have suffered numerous major attacks. And significant terrorist plots have been foiled on our soil. We have developed significant national security capability in the fight against terrorism and other enduring threats such as espionage, serious and organised crime, and cyber crime. Our challenge is to ensure that, as Australia evolves as a 21<sup>st</sup> century society and economy, our national security capability similarly evolves with high levels of agility and adaptability and continues to meet emerging threats.

As Australia advances, so too do threats to our wellbeing. Meeting the challenges of new technologies and methodologies is a key priority for the Australian Government in the national security sphere. Our law enforcement and security capabilities must keep ahead of terrorists, agents of espionage and organised criminals who threaten our national security and the safety of our citizens. So our law enforcement and intelligence agencies must be equipped with contemporary skills and technologies, and backed by necessary powers – coupled with the appropriate checks and balances and oversight mechanisms society rightly demands.

This package of reform proposals, which comprises telecommunications interception reform, telecommunications sector security reform and Australian intelligence community reform, seeks to do just that. The common thread of national security runs through the proposals, which seek to respond to threats from international state and non-state based actors, terrorism, serious and organised crime and cyber crime.

Just as technology and methodology employed by terrorists, agents of espionage and organised criminals adapts and advances so too must the capabilities and powers of our law enforcement and security agencies. In the absence of action, significant intelligence and evidence collection capabilities will be lost providing criminal elements with a technological upper hand.

Telecommunications interception reform recognises that there are significant challenges facing intelligence and law enforcement agencies in accessing communications, particularly in keeping pace with rapid changes in the telecommunications environment. New, emerging and future technologies impact on the ability of these agencies to access communications to collect intelligence and effectively detect and prosecute crimes. The Australian Crime Commission's *Future of Organised Criminality in Australia 2020* assessment reveals that access to highly effective software, ciphers and other methodologies are increasingly being utilised by organised crime to impede detection by law enforcement. Lawful interception, therefore, is the most important tool in the investigation and

prosecution of serious and organised and other technology-enabled crime, and is vital to effectively collect security intelligence. Proposed reforms seek to allow those agencies to utilise modern technologies to maintain effective investigative techniques.

Telecommunications sector security reform seeks to address the national security risks posed to Australia's telecommunications infrastructure. The security and resilience of such infrastructure significantly affects the social and economic well-being of the nation. While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy or alter critical infrastructure and the information held on it. As Australia's telecommunications landscape continues to evolve, it is appropriate and timely to consider how best to manage risks to the data carried and stored on our telecommunications infrastructure to secure its availability and integrity in the long term. The ideas included in this discussion paper build on consultation with industry earlier in 2012 about the most effective way to manage national security risks to telecommunications infrastructure.

Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats. At least four planned terrorist attacks designed to achieve mass casualties on Australian soil have been thwarted by agencies since 11 September 2001. To continue this crucial role, it is imperative that Australia's intelligence agencies remain robust and can effectively deal with the challenges presented by today's and tomorrow's international security environment. Following the 2008 Report of the Review of Homeland and Border Security conducted by Mr Ric Smith AO PSM, the Attorney-General's Department has worked with relevant agencies to determine the powers required to deal with current and future national security challenges. Australian intelligence community reform is about appropriately equipping and enhancing the operational capabilities of these agencies.

This Discussion Paper contains the terms of reference for the PJCIS inquiry at Chapter One, followed by chapters on each of the proposals which comprise the package of proposals. Chapter Two, 'Interception and the TIA Act', deals with telecommunications interception reform and outlines the problems facing law enforcement and intelligence agencies that have arisen from the operation of the *Telecommunications (Interception and Access) Act 1979*. Chapter Three, 'Telecommunications Sector Security Reform' considers possible amendments to the *Telecommunications Act 1997* to establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure. Chapter Four considers ideas for reform of the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*.

Although the package is referred to the PJCIS in its totality, in considering the ideas the Attorney-General has organised the proposals in three separate groupings: those the Government wishes to progress, those the Government is considering, and those on which the Government expressly seeks the PJCIS' views. Chapter One elaborates on the content of each group. Chapters Two, Three and Four refer to the groups within which the ideas sit, as determined by the Terms of Reference.

## CHAPTER ONE

### TERMS OF REFERENCE - INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION

---

Having regard to:

- the desirability of comprehensive, consistent and workable laws and practices to protect the security and safety of Australia, its citizens and businesses,
  - the need to ensure that intelligence, security and law enforcement agencies are equipped to effectively perform their functions and cooperate effectively in today's and tomorrow's technologically advanced and globalised environment, and
  - the fact that national security brings shared responsibilities to the government and the private sector:
- 1) The Parliamentary Joint Committee on Intelligence and Security is to inquire into potential reforms of National Security Legislation, as set out in the attachment and which include proposals relating to the:
    - a) *Telecommunications (Interception and Access) Act 1979*
    - b) *Telecommunications Act 1997*
    - c) *Australian Security Intelligence Organisation Act 1979*
    - d) *Intelligence Services Act 2001*
  - 2) The inquiry should consider the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet:
    - a) the challenges of new and emerging technologies upon agencies' capabilities
    - b) the requirements of a modern intelligence and security agency legislative framework, and to enhance cooperation between agencies, and
    - c) the need for enhancements to the security of the telecommunications sector.
  - 3) The Committee should have regard to whether the proposed responses:
    - a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector
    - b) apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the

telecommunications sector and the potential for follow on effects to consumers, the economy and international competition, and

- c) will address law enforcement reduction of capabilities from new technologies and business environment, which has a flow-on effect to security agencies.
- 4) The Committee should take account of the interests of the broad range of stakeholders including through a range of public, *in camera* and classified hearings.
- 5) The Committee should provide a written report on each of the three elements of the National Security Legislation referral to the Attorney-General.

The National Security Legislation the subject of the inquiry has three different elements and Objectives. They relate to:

- modernising lawful access to communications and associated communications data
- mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers, and
- enhancing the operational capacity of Australian intelligence community agencies.

The proposals across the three different packages are separated into three different groupings:

- A. those the Government wishes to progress
- B. those the Government is considering progressing, and
- C. those on which the Government is expressly seeking the views of the PJCIS.

**A - Government wishes to progress the following proposals:**

*Telecommunications (Interception and Access) Act 1979*

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This would include the examination of:
  - a. the legislation's privacy protection objective

- b. the proportionality tests for issuing of warrants
  - c. mandatory record-keeping standards
  - d. oversight arrangements by the Commonwealth and State Ombudsmen
- 2. Reforming the lawful access to communications regime. This would include:
  - a. reducing the number of agencies eligible to access communications information
  - b. the standardisation of warrant tests and thresholds
- 3. Streamlining and reducing complexity in the lawful access to communications regime. This would include:
  - a. simplifying the information sharing provisions that allow agencies to cooperate
  - b. removing legislative duplication
- 4. Modernising the TIA Act's cost sharing framework to:
  - a. align industry interception assistance with industry regulatory policy
  - b. clarify ACMA's regulatory and enforcement role

*Australian Security Intelligence Organisation Act 1979*

- 5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions
  - a. to update the definition of 'computer' in section 25A
  - b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.
- 6. Modernising ASIO Act employment provisions by:
  - a. providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'
  - b. Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent



- c. Modernising the Director-General's powers in relation to employment terms and conditions
- d. Removing an outdated employment provision (section 87 of the ASIO Act)
- e. Providing additional scope for further secondment arrangements

*Intelligence Services Act 2001*

- 7. Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies.

**B. Government is considering the following proposals:**

*Telecommunications (Interception and Access) Act 1979*

- 8. Streamlining and reducing complexity in the lawful access to communications regime – this would include:
  - a. Creating a single warrant with multiple TI powers
- 9. Modernising the Industry assistance framework –
  - a. Implement detailed requirements for industry interception obligations
  - b. extend the regulatory regime to ancillary service providers not currently covered by the legislation
  - c. implement a three-tiered industry participation model

*Australian Security Intelligence Organisation Act 1979*

- 10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.
- 11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:
  - a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

- b. Align surveillance device provisions with the Surveillance Devices Act 2007
  - c. Enable the disruption of a target computer for the purposes of a computer access warrant
  - d. Enable person searches to be undertaken independently of a premises search
  - e. Establish classes of persons able to execute warrants
12. Clarifying ASIO's ability to cooperate with the private sector.
13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.

**C. Government is expressly seeking the views of the Committee on the following matters:**

*Telecommunications (Interception and Access) Act 1979*

14. Reforming the Lawful Access Regime
- a. expanding the basis of interception activities
15. Modernising the Industry assistance framework
- a. establish an offence for failure to assist in the decryption of communications
  - b. institute industry response timelines
  - c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

*Telecommunications Act 1997*

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:
- a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference
  - b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs

- c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers
- d. Creating appropriate enforcement powers and pecuniary penalties

*Australian Security Intelligence Organisation Act 1979*

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:
- a. Using third party computers and communications in transit to access a target computer under a computer access warrant.
  - b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant
  - c. Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.
  - d. Introducing an evidentiary certificate regime.

*Intelligence Services Act 2001*

18. Amending the Intelligence Services Act to:
- a. Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.
  - b. Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required.
  - c. Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

## CHAPTER TWO

### INTERCEPTION AND THE TIA ACT

---

#### 1. Introduction

The primary objective of the current legislation governing access to communications is to protect the privacy of users of telecommunications services in Australia by prohibiting covert access to communications except as authorised in the circumstances set out in the TIA Act.

The exceptions to the general prohibition against interception recognise the need for national security and law enforcement agencies to access the information necessary to protect community safety and security. The limited focus of the exceptions reflects Parliament's concern to balance the competing right of individuals to freely express their thoughts with the right of individuals to live in a society free from threat to personal safety.

Interception of telecommunications content and data is a powerful and cost effective tool for law enforcement and security agencies to reduce threats to national security and to assist in the investigation and prosecution of criminal offences.<sup>1</sup> Access to interception is tightly regulated and, in relation to content, is limited to the investigation of serious offences under the authority of an independently issued warrant and subject to a range of oversight and accountability measures.

However, the interception regime provided by the current Act reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act.

In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity.

The Government is therefore considering the need for a new interception regime that better reflects the contemporary communications environment and is seeking the views of the Committee on the content of that regime. Priority issues for consideration by the Committee are set out in the Terms of Reference, grouped into:

---

<sup>1</sup> See *Report of the Review of the regulation of access to communications* (2005) (the Blunn Report) at <http://www.ag.gov.au/Publications/Pages/BlunnreportofthereviewoftheregulationofaccessstocommunicationsAugust2005.aspx>

- Matters the Government wishes to progress;
  - Examining the legislation's privacy protection objective, the proportionality test for issuing warrants, mandatory record-keeping standards, and oversight arrangements by the Commonwealth and State Ombudsmen
  - Reducing the number of agencies eligible to access communications information
  - Standardising warrant tests and thresholds
  - Simplifying the information sharing provisions that allow agencies to cooperate
  - Removing legislative duplication
  - Aligning industry interception assistance with industry regulatory policy
  - Clarifying the AMCA's regulatory and enforcement role
- Matters the Government is considering
  - Creating a single warrant with multiple TI powers
  - Implementing detailed requirements for industry interception obligations
  - Extending the regulatory regime to ancillary service providers not currently covered by the legislation
  - Implementing a three-tiered industry participation model; and
- Matters on which the Government expressly seeks the views of the Committee.
  - Expanding the basis of interception activities
  - Establishing an offence for failure to assist in the decryption of communications
  - Instituting industry response timelines
  - Applying tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts

This chapter of the discussion paper describes the role played by access to communications content and data in protecting the community from threats to security and serious crime, summarises the key features of the current legislative regime and the challenges it is facing. The chapter concludes by suggesting that, to achieve a legislative regime that is effective in the contemporary communications environment, reforms may be developed to:

- Strengthen the safeguards and privacy protections of the interception regime in line with contemporary community expectations;
- Reform the lawful access regime for agencies;
- Streamline and reduce complexity in the lawful access regime; and
- Modernise the cost sharing framework.

### **1.1 Effectiveness of lawful covert access to communications**

Lawful interception and access to telecommunications data are cost-effective investigative tools that support and complement information derived from other methods.

In 2010-2011 there were 2441 arrests, 3168 prosecutions (2848 for serious offences) and 2034 convictions (1854 for serious offences) based on lawfully intercepted material.<sup>2</sup> Law enforcement agencies made 91 arrests, 33 prosecutions and obtained 33 convictions based on evidence obtained under stored communications warrants.<sup>3</sup>

These figures may underestimate the effectiveness of interception because a conviction can be recorded without entering the intercepted material into evidence.<sup>4</sup> Interception also allows agencies to identify criminal connections, co-conspirators and organised crime associates and assists in establishing the methodology of criminal enterprises. It also plays an important role in identifying child exploitation material, sexual slavery and terrorist organisations. The figures are specific to law enforcement agencies and do not take into account the use of intercepted information by ASIO in carrying out its functions (which is reflected in ASIO's classified annual report).

Telecommunications data is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest.

### **1.2 The national security environment**

Under the TIA Act, the Australian Security Intelligence Organisation (ASIO) can ask the Attorney-General to issue an interception warrant in order to investigate activities prejudicial to security or to collect foreign intelligence.

Australia is, and will remain, a terrorist target for the foreseeable future with jihadist terrorism being the most immediate threat.<sup>5</sup> The threat of a terrorist attack in Australia or

---

<sup>2</sup> AGD, *TIA Act Report for the year ending 30 June 2011*, p. 46.

<sup>3</sup> AGD, *TIA Act Report for the year ending 30 June 2011*, p. 60.

<sup>4</sup> AGD, *TIA Act Report for the year ending 30 June 2011*, p. 47.

<sup>5</sup> ASIO, *ASIO Report to Parliament 2010-11*, p. xviii.

against Australian interests overseas remains real.<sup>6</sup> Since 2001, four mass casualty attacks within Australia have been disrupted because of the joint work of intelligence and law enforcement agencies.<sup>7</sup>

Since 2001, 38 people have been prosecuted in Australia as a result of counter-terrorism operations and 22 people have been convicted of terrorism offences under the *Criminal Code Act 1995* (the Criminal Code).<sup>8</sup>

Intercepted information has played an important role in recent counter-terrorism prosecutions and in preventing planned terrorist attacks. In 2008, several men who faced trial in Melbourne were convicted of being a member of a terrorist organisation. The evidence that the group was engaged in preparing or fostering a terrorist act was largely contained in 482 intercepted conversations that were put before the jury. Some of these communications were covertly recorded in the home of the organisation's leader.

While terrorism is a key issue, the *ASIO Report to Parliament 2010-11* notes that espionage is an enduring security threat to Australia, both through the traditional form of suborning persons to assist foreign intelligence agencies and new forms such as cyber espionage. Nation states, as well as disaffected individuals and groups, are able to use computer networks to view or siphon sensitive, private or classified information for the purpose of espionage, political, diplomatic or commercial advantage. As the actors involved undertake this activity within 'cyberspace', the lawful interception of their communications is often a crucial aspect of any investigation aiming to resolve the nature of the activity and the identity of the perpetrators.

### **1.3 Serious offences and serious contraventions – Commonwealth and State**

The precursor to the TIA Act focused on national security but with the emerging national drug crisis in the 1970s the current Act was passed to ensure that interception powers were also available to the Australian Federal Police to investigate narcotic offences. Since its enactment the TIA Act has been amended to allow a broader range of law enforcement agencies to intercept communications to investigate other serious offences.

Under the TIA Act, serious offences generally include Commonwealth, State and Territory offences punishable by imprisonment for seven years or more. Particular examples of serious offences for which interception can be obtained are murder, kidnapping and offences involving serious personal injury. There are also a range of other offences defined

---

<sup>6</sup> ASIO, *ASIO Report to Parliament 2010-11*, p. ix.

<sup>7</sup> ASIO, *ASIO Report to Parliament 2010-11*, pp. xviii, 5.

<sup>8</sup> PM&C, *Counter-Terrorism White Paper*, 2010, p. 7.

as serious offences in the TIA Act where the use of the Australian telecommunications system is integral to the investigation of the offence.<sup>9</sup>

According to the Australian Institute of Criminology (the AIC), in 2010 there were 260 victims of homicide in Australia. There were also:

- 171,083 victims of assaults,
- 17,757 victims of sexual assaults; and
- 14,582 victims of robberies<sup>10</sup>

## 1.4 Organised crime

An interception warrant can also be sought to detect, investigate, prevent and prosecute persons involved in organised crime. Serious and organised crime refers to offences that involve two or more offenders, require substantial planning and organisation and the use of sophisticated methods and techniques and are committed in conjunction with other serious offences.

The Australian Crime Commission (ACC) in its 2010 report *Organised Crime in Australia*, assessed the overall threat to Australia from organised crime as “High”,<sup>11</sup> estimating the cost of such crime at \$10 to \$15 billion per year.<sup>12</sup>

The rapid adoption of telecommunications technology and high speed broadband internet has the potential to increase high-tech crime in Australia, including both the use of technology to facilitate traditional crime and specific crimes directed at information and communication technologies.<sup>13</sup> High tech crime covers a range of offences such as identity crime, sales of illicit products, credit card fraud, money laundering and child exploitation material.

The individuals involved in many of these activities are highly sophisticated in their operations using multiple technologies and frequently changing their methodology to avoid detection. Their adaptiveness means that the tools available under the interception regime provide the only investigative technique capable of identifying and disrupting their activities, many of which are conducted at the global level.

---

<sup>9</sup> See s 5D of the TIA Act.

<sup>10</sup> AIC 2011 *Australian crime: Facts & figures* <http://www.aic.gov.au/documents/0/B/6/%7B0B619F44-B18B-47B4-9B59-F87BA643CBAA%7Dfacts11.pdf>, p2.

<sup>11</sup> ACC, *Organised Crime in Australia 2011*, <http://www.crimecommission.gov.au/sites/default/files/files/OCA/2011/oca2011.pdf>, p. 7.

<sup>12</sup> ACC, *Organised Crime in Australia 2011*, p. 3.

<sup>13</sup> ACC, *Organised Crime in Australia 2011*, p. 25.



Over the past 18 months, information obtained through interception activities in relation to a single money laundering investigation has helped the AFP to arrest 35 offenders and to seize 421 kilograms of drugs and over \$8,000,000 in cash.

Many transnational crimes, such as money laundering, also pose a threat to Australia's national security interests with clear links between the proceeds of such crimes and the funding of terrorist activities overseas.

### **1.5 Fundamentals of the current Act**

Research suggests that access to and the use of intercepted information will continue to play an important role in supporting the functions of national security and law enforcement agencies. The conduct of national security and law enforcement investigations demonstrates that lawful interception is a critical capability that cannot be replaced by other investigative methods.

In the thirty years since its inception, the TIA Act has been able to accommodate emerging threats and changes in criminal behaviour because the legislation does not limit the concept of interception to a particular technology (such as a telephone). By couching the Act this way the currency of the legislation has been maintained through amendments that have clarified the application of the Act as the telecommunications environment and what is necessary for agencies to properly protect the community have changed.

#### ***Towards a new approach***

The pace of change in the last decade has meant the Act has required frequent amendment resulting in duplication and complexity that makes the Act difficult to navigate and which creates the risk that the law will not be applied as Parliament intended.

Much of the need to amend the TIA Act stems from the contextual foundations of the Act.

Many of those foundations no longer apply, creating significant challenges for agencies to maintain current investigative capabilities. Agencies continue to adapt their capabilities within the constraints of the current legal framework but this has not ameliorated the impact of the rapid changes in the telecommunications environment and the ability of agencies to access communications.

In recent years there have been significant advancements in technology and changes to industry structure, practices and consumer behaviour. The communications landscape of the 1970s which was dominated by a single provider and focused on communications made by telephone no longer exists.

The magnitude of change to the telecommunications environment suggests that further piecemeal amendments to the existing Act will not be sufficient. Rather, holistic reform that

reassesses the current assumptions is needed in order to establish a new foundation for the interception regime that reflects contemporary practice.

### ***Telecommunications in 2012***

When the TIA Act was enacted, an agency could expect that it would be able to lawfully intercept most, if not all, of a person's communications. Today, changes in the way communications technology is delivered and used mean that the expectation is much lower.

At the end of June 2011, there were 287 fixed-line telephone service providers, three mobile network operators, 176 Voice over Internet Protocol (VoIP) service providers, 33 satellite providers and 97 Internet Service Providers (only including ISPs with at least 1000 subscribers).<sup>14</sup>

Together they provided 29.28 million mobile services and 10.54 million fixed-line telephone services and supported some 10.9 million internet subscribers.<sup>15</sup> Around 12.7 million Australians (69% of the population) had access to a broadband internet connection at home, while around 3.9 million Australians (21% of the population) accessed the internet from their mobile phone.<sup>16</sup>

Australian consumers are increasingly accessing multiple technologies and services to communicate. As at June 2011, 57% of Australians were using at least three communications technologies (fixed-line telephone, mobile phone and internet) and 26% of adults were using at least four communications technologies (fixed line telephone, mobile phone, VOIP and the internet).<sup>17</sup>

There has also been a trend towards high speed internet services, with the proportion of internet subscribers on services of eight megabits per second or more increasing from 26% to 33% in 2009-10.<sup>18</sup> The increase in internet speed has resulted in a rise in data downloads. The average user downloaded 25.1 gigabytes of data in the June quarter of 2011, 56% more than in the June quarter of 2010.<sup>19</sup>

In the June 2011 quarter, Australians downloaded 274,202 terabytes of data from fixed-line wireless internet services, an increase of 76% from the June 2010 quarter. Fixed-line broadband accounted for 254,947 terabytes (around 93%), while wireless broadband

---

<sup>14</sup> ACMA, *Communications report 2010-11*, p. 24.

<sup>15</sup> ACMA, *Communications report 2010-11*, p. 25.

<sup>16</sup> ACMA, *Communications Report 2010-11*, p. 18.

<sup>17</sup> ACMA, *Communications report 2010-11*, p. 153.

<sup>18</sup> ACMA, *Communications Report 2009-10*, p. 15.

<sup>19</sup> ACMA, *Communications Report 2010-11*, p. 17.

accounted for 19,194 terabytes (around 7%). There was an additional 3,695 terabytes of data downloaded on mobile handsets in the June 2011, an increase of 415% on the June 2010 quarter.<sup>20</sup>

Along with the increased use of multiple technologies, mobile phones are becoming a 'truly converged consumer device'.<sup>21</sup> The availability of iPhone and Smartphone technology has allowed handset models to offer a number of services including voice, SMS, internet access, email, e-payment, video, music, photography, GPS, VOIP and access to social networking sites. In 2010, smartphones represented 43% of all mobile phones sold in Australia.<sup>22</sup>

Increased network coverage, speed and availability have allowed consumers to access VOIP services more effectively. This technology involves communicating and transporting voice messages over the internet, rather than via the public switched telephone network. VOIP is available on many smartphones and internet devices, so mobile phone users can make calls or send text messages over the internet. VOIP usage in Australia has increased from 2.9 million users in June 2010 to 3.8 million users in June 2011.<sup>23</sup> In the year leading up to June 2011, mobile VOIP usage increased by 226%, with 274,000 users in June 2011.<sup>24</sup>

Social media use has also increased, resulting in more user generated content and providing alternative communication channels to traditional voice services. During June 2011, 8.6 million Australians accessed online social network sites from home, compared to 8.0 million during July 2010.<sup>25</sup>

These trends are expected to continue. In addition, the implementation of the NBN is likely to increase the amount of material that can be accessed through telecommunications devices, encourage competition and technological and service innovation, and drive further industry restructuring. Work on the NBN rollout is planned to commence in over 1500 communities and pass 3.5 million premises throughout Australia by 30 June 2015 and is scheduled to be completed by 2021.<sup>26</sup>

---

<sup>20</sup> ACMA, *Communications Report 2010-11*, p. 26.

<sup>21</sup> ACMA, *Communications report 2009-10*, p. 147.

<sup>22</sup> The Australian, 'Apple's iPhone leads Australia's huge smartphone growth', 15 March 2011, <http://www.theaustralian.com.au/australian-it/apples-iphone-leads-australias-huge-smartphone-growth/story-e6frgakx-1226021287594>

<sup>23</sup> ACMA, *Communications report 2010-11*, p. 25.

<sup>24</sup> ACMA, *Communications report 2010-11*, p. 16.

<sup>25</sup> ACMA, *Communications report 2010-11*, p. 26.

<sup>26</sup> NBN Co. Media Release, 29 March 2012 at <http://www.nbnco.com.au/news-and-events/news/nbn-co-announces-three-year-rollout-plan.html>

***Legacy assumptions***

The complexity of the contemporary communications environment is not reflected in the current interception regime which instead assumes that:

1. Communications to be intercepted are easily identified;
2. A stream of traffic to be intercepted can be isolated from the rest of the communications passing over the network;
3. Carriers and carriage service providers (telecommunications companies and internet service providers) control the traffic passing over their networks;
4. Carriers and carriage service providers are the only entities which control public telecommunications networks;
5. Intercepted communications are easily interpreted or understood;
6. There are reliable sources of associated communications data that link people with identifiers and identifiers to communications; and
7. A 'one size' approach to industry obligations is appropriate.

These assumptions mean the TIA Act takes a technical approach to defining when an interception takes place which was appropriate to the prevailing technologies of the 1960s and 1970s but, with the rise of internet protocol communications, now causes uncertainty about the scope of the general prohibition against interception and fails to recognise the particular demands created by a diverse telecommunications sector.

**2.1 Problems with the current approach**

The limitations created by the assumptions inherent in the TIA Act impact on the capacity of agencies to:

1. Reliably identify communications of interest and to associate them with telecommunications services;
2. Reliably and securely access communications and associated data of interest within networks; and
3. Effectively interpret the communications to extract the intelligence or evidence

***Identifying communications***

The TIA Act is based on an assumption that there is a unique, non-ambiguous identifier, such as a phone number, linking the target of an interception warrant to the service (or device) to be intercepted and in turn to the carrier required to give effect to the warrant.

However, typically there are no longer clear, one-to-one relationships between the target of an interception warrant, telecommunications services used by the person, and telecommunications service providers because users of telecommunications services may have multiple 'identities', each of which may only be meaningful to a particular service provider.

Persons seeking to avoid surveillance commonly exploit this situation.

### ***Access to communications content and communications data***

The TIA Act is also based on the assumption it is possible to reliably access communications which are the subject of an interception warrant at a convenient point on a carrier's network through which the data must flow. This is problematic as most networks are now based on Internet protocol (IP). With this technology users can access communications via multiple access technologies (fixed networks, wireless, satellite, etc.), multiple physical locations and multiple access service providers, some part of which need not be owned, operated or accessible to regulated participants in the telecommunications industry, such as carriers and carriage service providers (or C/CSPs). As a result, communications cannot be guaranteed to pass over any particular path and therefore it may be necessary to attempt to direct the communications over a particular path to facilitate interception.

In addition, whereas telecommunications services were once provided by a single carrier, in many cases now each communication event typically involves a number of service providers. In a single communications session, a person may access many application services such as a Google search engine portal, a webmail account, a Facebook account, and an online storage repository. Each of these services is provided by a different service provider under separate subscriber accounts and with different unique subscriber 'identities'. In general, the ISP and the access service providers have no knowledge of the application services passing over their infrastructure. Further, many application service providers operate from offshore making the provision of assistance to Australian agencies challenging.

Currently, authorised access to telecommunications data, such as subscriber details, generated by carriers for their own business purposes is an important source of information for agencies. As carriers' business models move to customer billing based on data volumes rather than communications events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations.

At least part of the complexity can be ascribed to changes in the telecommunications industry. It is no longer possible to always be able to clearly identify the industry participant

with a single target 'identity'. The ready availability of anonymous pre-paid services, inter-carrier roaming agreements, resold services, calling cards and on-line facilities to subscribe to new services all make it necessary for agencies to seek data from multiple providers to ascertain whether any data exists.

### ***Interpreting communications and communications data***

All of these variables, particularly when combined with increased data flows and volumes, mean it is now extremely complex and costly to reliably identify and access communications.

Furthermore, once a communication has been accessed, its content is not necessarily clear. In IP-based communications, the content of communications is embedded in data packets in a form which is not readily able to be reconstructed and interpreted outside of the transmitting and receiving terminal devices and the applications running on them. Data used to route, prioritise and facilitate the communications is also embedded along with the content, in the communications packets. This means that agencies must further process communications accessed under an interception warrant to extract and reconstruct the content.

The use of encryption and propriety data formats and typically large data volumes, makes reconstructing communications into an intelligible form difficult for agencies.

## **2.2 Creating a contemporary regime**

In order to preserve the effectiveness of lawful covert access to electronic communications as an investigative tool in the face of rapid developments in technology and the globalisation of the telecommunications industry, the assumptions underpinning the current legislative framework need to be reassessed to ensure they reflect the contemporary communications environment. Realigning the foundations of the regime will address key operational challenges.

Four main areas have been identified as requiring review:

1. Strengthening the safeguards and privacy protections in line with contemporary community expectations;
2. Reforming the lawful access regime for agencies;
3. Streamlining and reducing complexity; and
4. Modernising the cost sharing framework

***Strengthening the safeguards and privacy protections in line with contemporary community expectations***

Historically, the TIA Act has protected the privacy of communications by prohibiting interception except as allowed under the Act.

Over time the position of privacy in the interception regime has been affected by the balancing inherent in the Act between protecting privacy and enabling agencies to access the information necessary to protect the community. Where the balance between these objectives should lie is left to Parliament to decide.

The need to amend the Act to adapt to changes in the telecommunications environment has seen the range of exceptions to the general prohibition grow. Accordingly, it may be timely to revisit whether the privacy framework within the Act remains appropriate.

As people's use and expectations of technology have changed since the TIA Act was enacted in 1979, so community views about the types of communications that can be accessed and the purposes for which they can be accessed may also have changed.

Reviewing the current checks, balances and limitations on the operations of interception powers will ensure that the privacy needs of contemporary communications users are appropriately reflected in the interception regime.

Consideration is also being given to introducing a privacy focused objects clause that clearly underpins this important objective of the legislation and which guides interpretation of obligations under the Act. By taking these steps, the legislation will be positioned to meet the objective of protecting the privacy of Australian communications from unlawful access.

***Reforming the lawful access regime***

Telecommunications interception and access to communications data are unique and fundamental tools that cannot be replaced by other investigative techniques. They are cost effective, timely, low risk and extremely successful tools in obtaining intelligence and evidence. Substantial and rapid changes in communications technology and the business environment are rapidly eroding agencies' ability to intercept. Adapting the regime governing the lawful access to communications is a fundamental first step in arresting the serious decline in agencies' capabilities.

The TIA Act provides for four warrants for law enforcement agencies to access content. Three warrants relate to accessing real-time content and one warrant relates to accessing 'stored communications' (which includes emails and text messages accessed from the carrier after they have been sent).

Real-time content based warrants are available to 17 Commonwealth and State and Territory agencies. ASIO's ability to intercept communications supports its functions relating to security. The AFP and State and Territory police forces have access to interception powers as part of a nationally consistent approach to combating serious crime. The remaining agencies are a mix of agencies whose functions relate to investigating police integrity, anti-corruption and serious and organised crime.

While traditionally limited to an offence that carries a penalty of at least 7 years' imprisonment (a 'serious offence'), over time numerous legislative amendments have confused the policy in relation to the circumstances in which interception is available. There are occasions where the general penalty threshold is too high to cover a range of offences for which it is already recognised that general community standards would expect interception to be available. For example, child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks (including offences committed using a computer or involving telecommunications networks) do not meet the general 7 year imprisonment policy threshold.

The stored communications regime allows 'enforcement agencies' (criminal law enforcement agencies, civil penalty enforcement agencies and public revenue agencies) to access the content and associated data of a communication held by a carrier. In addition to interception agencies, enforcement bodies include a range of regulatory bodies such as the Australian Customs and Border Protection Service, the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, the Australian Taxation Office, Centrelink and a range of State and Territory government organisations.

A stored communications warrant can only be issued for the investigation of an offence carrying a penalty of at least three year's imprisonment or a fine of 180 penalty units. The threshold for access is lower than for interception because it was considered at the time the provisions were introduced that communicants often have the opportunity to review or to delete these communications before sending them, meaning covert access can be less privacy intrusive than real-time listening. However, this logic, while valid several years ago, has become less compelling as technology use and availability has changed.

Implementing a standard threshold for both content and stored communications warrants would remove the complexities inherent in the current interpretation of what is a serious offence, recognise the growing number of online offences and provide consistent protection for 'live' and 'stored' content. Consideration is also being given to reducing the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so.



Interception and stored communications warrants provide authority to receive the content of the communication and associated data. The concept of 'data' is not defined in the TIA Act but is generally understood to refer to information about a communication that is not the content or substance of a communication. Data is increasingly understood as falling into two categories: subscriber data, which provides information about a party to a communication such as name or billing address; and traffic data, which relates to how a communication passes across a network, such as the location from which the communication was made.

How and for what purposes an interception agency can intercept a communication depends on limited characteristics or features of the communication relating to the type of service or device used or the name of a person. Defining attributes by communicant, carrier-provided service or technology made sense in an era where carriers, device types and users were limited but is more complex in the current environment where the carrier or means of conveyance is not always readily apparent. This is both time-consuming and costly for agencies in terms of analysing unnecessary information and potentially invasive from a privacy perspective as the communications of innocent parties may be unduly affected. One way to address these concerns would be to introduce a simplified warrant regime that focuses on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest.

### ***Streamlining and reducing complexity in the law***

The use and disclosure of information obtained from exercising powers under the TIA Act is strictly regulated.

The Act prohibits the use and communication of information obtained under a warrant except for the purposes explicitly set out in the legislation. Information obtained under the TIA Act is subject to more rigorous legislative protections than other forms of information in an agency's possession. The provisions are detailed and complex in relation to record keeping, retention and destruction and can present a barrier to effective information sharing both within an agency and between agencies. This was not an issue when the Act was enacted and applied only to ASIO and the AFP, but with more agencies now defined as interception agencies and the national and transnational nature of many contemporary security and law enforcement investigations, effective co-operation within and between agencies is critical.

Simplifying the current information sharing provisions would support co-operative arrangements between agencies and consideration could be given to the ways in which information sharing amongst agencies could be facilitated.

Record keeping and accountability obligations require law enforcement agencies<sup>27</sup> to keep records relating to documents associated with the warrants issued and particulars relating to warrant applications (such as whether an application was granted or refused) and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed. Agency heads must also report to the Attorney-General on the use and communication of intercepted information within three months of a warrant ceasing to be in effect. The Attorney-General's Department must prepare an annual statistical report about the use of powers under the TIA Act, which the Attorney-General tables in Parliament.

Different record keeping requirements apply to stored communications.

Oversight of law enforcement agencies' use of powers is split between the Commonwealth Ombudsman and equivalent State bodies in relation to interception activities. The Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications. This split in responsibility contrasts with the *Surveillance Devices Act 2004*, where the Commonwealth Ombudsman inspects all agencies.

The requirements are aimed at ensuring that agencies keep appropriate records necessary to demonstrate that agencies are using their powers lawfully. However, many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate.

The current regime is focused on administrative content rather than recording the information needed to ensure that a particular agency's use of intrusive powers is proportional to the outcomes sought. The existing provisions take a one size fits all approach, resulting in a lack of flexibility for each agency to determine the best way to record and report on information having regard to individual practices, procedures and use of technology.

The same provisions also impede the Ombudsman's ability to report on possible contraventions and compliance issues by prescribing detailed and time limited procedures that need to be checked for administrative compliance, rather than giving the Ombudsman scope to determine better ways of assisting agencies to meet their requirements.

Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes.

---

<sup>27</sup> The focus of the discussion about record keeping and accountability is on law enforcement agencies..

***Modernising the cost sharing framework***

Carriage and carriage service providers (C/CSPs), which are telecommunications industry participants subject to regulatory obligations under the TIA Act and the *Telecommunications Act 1997*, play an irreplaceable role in enabling agencies to access communications. Under the Telecommunications Act, C/CSPs have an obligation to provide such help to agencies as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting the public revenue and safeguarding national security.

The TIA Act places an obligation on each C/CSP to have the capability to intercept communications and requires carriers and nominated carriage service providers to submit an annual interception capability plan outlining their strategy for complying with their obligation to intercept and to deliver communications to interception agencies. The obligation extends to maintaining the capability to intercept communications that are carried by a service that they provide and to deliver those communications to the requesting agency consistent with a warrant.

However, as networks have become more complicated and the types of services available have expanded, often beyond the C/CSPs' own networks, challenges have evolved in applying a general obligation. Consideration should be given towards introducing measures that implement more specific technical requirements to cater for a diverse and sophisticated telecommunications environment. This includes developing requirements around administrative needs such as the timeliness of cost sharing to agencies and the security measures to be applied to the handling of sensitive information relating to interception operations.

The capital cost of interception is shared between both industry and agencies. The cost of developing, installing and maintaining interception capability is borne by the C/CSP. The cost of developing, installing and maintaining delivery capability is borne by agencies. Costs have been split on that basis because industry is best placed to find efficiencies and to minimise costs. C/CSPs can recover the costs of providing day-to-day assistance to agencies on a no profit, no loss basis.

The TIA Act only covers C/CSPs, rather than the broad range of current telecommunications industry participants, consistent with the Act's focus on traditional services such as landline telephones. However, the exclusion of providers such as social networking providers and cloud computing providers creates potential vulnerabilities in the interception regime that are capable of being manipulated by criminals. Consideration should be given to extending the interception regime to such providers to remove uncertainty about the application of industry obligations in relation to agency requests and to better position Australia to meet domestic and international demands.

In reforming cost sharing, consideration must also be given to the current make-up of the telecommunications industry. The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers.

A tiered model would also recognise that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant and less capacity to store and retain information about communications and customers.

Requirements on industry to retain current information and to assist agencies to decrypt information would greatly enhance agencies' abilities to detect and disrupt criminal and other behaviours that threaten national wellbeing but should be implemented in a way that does not compromise business viability.

The merits of introducing a tiered model should be considered, including the role such an approach could play in defining industry obligations in relation to activities such as retaining data. A future framework for industry obligations would take into account not only regulatory best practice, but do so in a manner that minimises compliance costs for industry and maintains competitive neutrality. The Committee should also consider whether there are any broader competition impacts arising from the framework and its effect on prices.

Consideration should also be given to clarifying the role of the Australian Communications and Media Authority (ACMA) in regulating industry obligations under the interception regime. The ACMA has rarely used its powers to enforce compliance with the TIA Act because the only effective power available to it under the Act is court action. Court action is usually inappropriate or excessive in the circumstances and unhelpful from an agency perspective because it may publicly disclose that a particular C/CSP is not complying with its TIA Act obligations. The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply.

### **3. Next Steps**

Access to communications content and data plays an important role in protecting the community against threats to security and serious criminal activity. It is vital that the legislation regulating the use of this investigative tool be kept up to date with developments in technology and the contemporary communications environment. Comprehensive reform of the current legislation is necessary, focusing particularly on the issues referred to the Committee by the Government and discussed in detail above.

## **CHAPTER THREE**

### **TELECOMMUNICATIONS SECURITY SECTOR REFORM**

---

#### **1. Introduction**

Australia's national security, economic prosperity and social wellbeing is increasingly reliant on the Internet and other information and communications technologies (ICT).

Underpinning our use of these technologies is our telecommunications infrastructure.

However, there are very real challenges to ensuring its security in the face of criminal and strategic threats. Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental mis-configuration, external hacking and even trusted insiders.

Australian citizens, businesses and public entities rely on telecommunication carriers and carriage service providers (C/CSPs) to handle information and data on their networks, including customer information, securely. Telecommunications users, including businesses and consumers, reasonably expect that the information they store on, and transmit across, telecommunications networks is adequately protected from national security threats. Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.

The Australian Government is considering whether telecommunications legislation, such as the *Telecommunications Act (1997)* (Telecommunications Act) and other relevant legislation should be amended to establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure.

The desired outcomes of the proposed framework are that:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,
- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,
- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities,

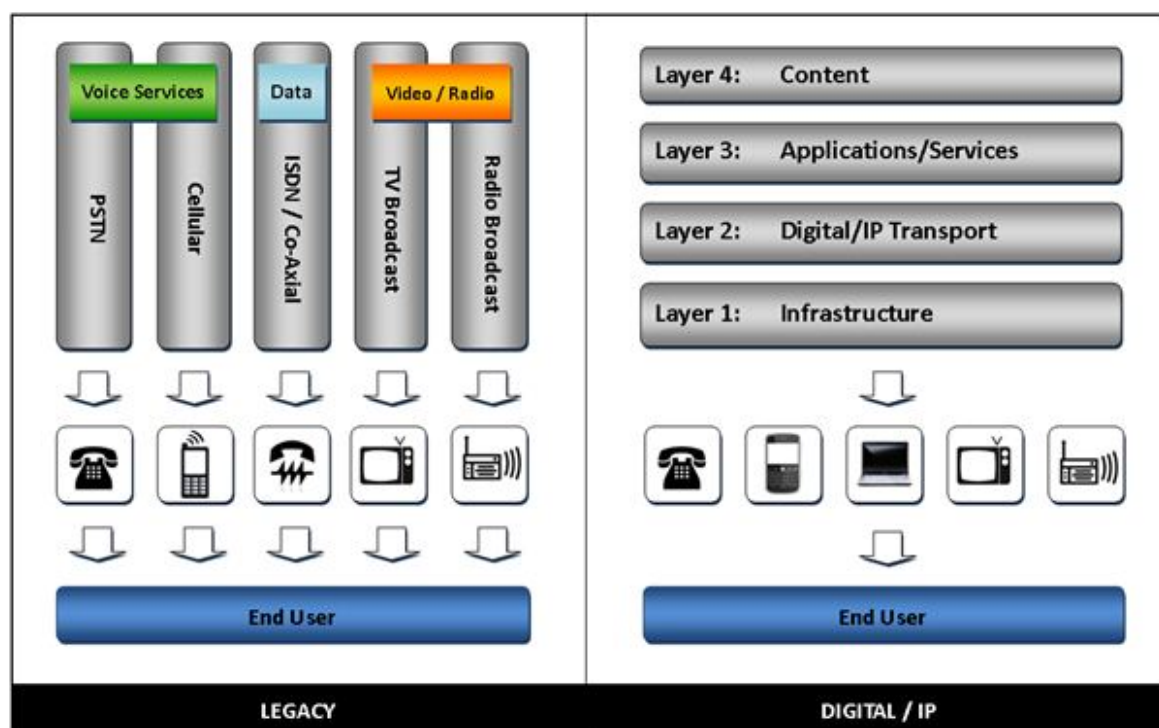
- the protection of information, including customer information and information about customers, contained on or transmitted across telecommunications networks is better assured, and
- compliance costs for industry are minimised.

## **2. The context**

While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy, degrade or alter the functioning of our critical telecommunications infrastructure and the information held on it. A clear understanding of the current telecommunications environment is essential to identifying network vulnerabilities and managing them effectively. This includes the composition and operation of the telecommunications industry, national security risks, and the current regulatory environment.

### **2.1 Australia's telecommunications industry**

Australia's telecommunications industry consists of a wide range of services and participants — an increasing number of which are based outside Australia. The telecommunications industry is a highly dynamic one, and C/CSPs usually operate network environments that have been significantly expanded and modified from their original specifications. In a broad sense, global telecommunications network architecture has evolved over the past 30 years from a 'siloe'd' services model to one of 'layered' convergence (figure 1). In Australia today, our telecommunications industry has evolved to reflect this shift, while the standardisation and mass-production of network equipment has also cut costs and opened up the range of suppliers with new entrants to the market gaining a stronger presence.

**Figure 1: Convergence in network and service layers<sup>28</sup>**

The National Broadband Network (NBN) rollout will further transform Australian telecommunications infrastructure, with changes to the telecommunications market's structure and functionality creating new opportunities for market participation. As such, Australia's telecommunications industry is increasingly diverse, with a range of overlapping and interconnected platforms and networks. The Australian Government recognises that C/CSPs operate in an increasingly competitive, commercial environment and that security is only one factor in procurement and investment decision-making. Although there are market incentives and customer expectations for network providers to ensure their infrastructure and services are secure, C/CSPs are working with incomplete information about the national security environment. There will always be information available to Government which is beyond industry's reach.

## 2.2 National security risks

The *ASIO Report to Parliament 2010-2011* states that espionage by foreign intelligence services is an enduring security threat to Australia, both conventional and new forms, such

<sup>28</sup> Australian Communications and Media Authority, 2011, Broken Concepts: The Australian Communications legislative landscape, p6 [http://engage.acma.gov.au/wp-content/uploads/2011/08/ACMA\\_Broken-Concepts\\_Final\\_29Aug1.pdf](http://engage.acma.gov.au/wp-content/uploads/2011/08/ACMA_Broken-Concepts_Final_29Aug1.pdf)

as cyber espionage. Our increasing reliance on communications technology to conduct the business of Government, commerce and our daily lives makes Australians more vulnerable to malicious attack. As such cyber security has emerged as a serious and widespread concern.<sup>29</sup> States, as well as disaffected individuals or groups, are able to use computer networks to view or siphon sensitive, private, or classified information for the purpose of, political, diplomatic or commercial advantage.

Individual records or files stored or transmitted on telecommunications networks may not be classified or particularly sensitive in and of themselves but, in aggregate, they can give foreign states and other malicious actors a range of intelligence insights not otherwise readily available. This threat extends to information vital to the effective day-to-day operation of critical national industries and infrastructure, including intellectual property and commercial intelligence.<sup>30</sup>

### 2.3 Current telecommunications regulatory environment

For the purposes of security, Australia's telecommunication industry is regulated primarily under two pieces of legislation — the *Telecommunications Act (1997)* administered by the Minister for Broadband, Communications and the Digital Economy and the *Telecommunications (Interception and Access) Act (1979)* (TIA Act) administered by the Attorney-General.

Section 581 of the Telecommunications Act provides the Attorney-General (in consultation with the Prime Minister and the Minister for Broadband, Communications and the Digital Economy) the power to give written direction to C/CSPs to cease supply of a carriage service if the use of that service is or would be prejudicial to security. It is recognised that such action, would impact on both businesses and consumers. Section 581 is non-specific, is not triggered by a specific set of circumstances and does not allow a practical graduated response to security risks. This sanction is a blunt instrument, and is not effective in encouraging C/CSPs to consider national security risks when making business decisions about the design of their networks.

Under section 202B of the TIA Act, C/CSPs are obliged to notify Government of planned changes to a telecommunications service or system where these changes may affect their capacity to comply with their obligations under the TIA Act. The TIA Act does not specifically address supply chain risks, hardware and software vulnerabilities or security risks to the confidentiality, integrity and availability of telecommunications infrastructure.

---

<sup>29</sup> ASIO, Director-General's speech at the Security in Government Conference, 7 July 2011

<sup>30</sup> ASIO, Director-General's speech at the Security in Government Conference, 7 July 2011



## **2.4 Analysis**

Engagement between Government and the telecommunications industry about national security risks currently occurs on an informal basis, relying on co-operation between security agencies and C/CSPs in cases where security agencies become aware of potential risks. In most cases engagement between security agencies and C/CSPs has been constructive. However there is a lack of awareness of national security risks in business decisions by many C/CSPs, which means engagement often occurs late in the decision making process. A more defined framework for government's engagement with industry would minimise disruption and resource impacts for industry and government. It would also provide greater clarity for industry during a time of considerable structural change in the telecommunications industry.

Government is concerned that the telecommunications industry is not fully informed about national security risks and is therefore not equipped to respond adequately to these risks. As both businesses and consumers are also exposed to the consequences of potential security risks, there is a compelling case to act now. Australia is at a critical stage of telecommunications infrastructure development driven by the NBN's construction. Delaying action to make C/CSPs aware of managing national security risks will complicate long term management decisions made on the design and procurement of major telecommunications infrastructure, with potential negative impacts on national security.

Accordingly, Government has a responsibility to intervene in the market to educate and assist C/CSPs to maintain a minimum level of security for the purpose of protecting the data on their networks and, ultimately to ensure mechanisms are in place to support the integrity and security of Australia's national telecommunications infrastructure.

## **3. Proposed approach**

One approach to address national security risks relating to telecommunications infrastructure may be achieved using a regulatory framework. Such an approach was developed earlier in 2012 for consultation with industry.

A regulatory approach could be achieved by making amendments to telecommunications legislation, such as the Telecommunications Act and other relevant legislation, such that C/CSPs protect their networks from unauthorised interference with the following elements:

1. an industry-wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;

2. a requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and
3. powers of direction and a penalty regime to encourage compliance.

In designing a regulatory framework, the following principles are considered important elements of an effective regulatory system:

- be adaptable to a changing environment;
- be clear to industry;
- provide incentives for compliance;
- be reasonably equitable and competitively neutral; and
- not be resource-intensive for industry to comply or for government to administer.

The advantages of such a framework include that it could:

- focus on security outcomes rather than absolute technical requirements, making it adaptable to changes in technology and the telecommunications market,
- provide greater clarity, control and certainty for industry by focusing on self-governance and demonstration of compliance,
- can be applied equitably across the telecommunications sector, and
- provide a more effective incentive for industry to place greater emphasis on national security considerations in its business decisions.

The Government is aware that such a framework may have significant impacts for industry and agencies and welcomes input as it explores how such an approach could work in practice and what these impacts may be. Government would also welcome input on any broader competition impacts that the proposal may have on the telecommunications market and consumers more generally.

It should be noted that some classified national security information will only be able to be shared with companies that have entered into security agreements with Government, which have been negotiated on the basis of risk to the national interest.

### **3.1 Industry consultation**

Preliminary targeted consultation with industry occurred in early 2012, during which C/CSPs demonstrated an understanding of the importance of protecting the confidentiality, integrity and availability of their networks.

Other points raised by industry included:

- the desire for a level playing field across the industry,
- a desire for clear guidance about Government's expectations and requirements for industry compliance,
- the need for certainty to enable C/CSPs to undertake business decisions with confidence, and
- flexibility for industry to explore and experiment with efficient and effective solutions for managing security risks.

During the consultation about a possible regulatory framework that originally included a notification obligation in place of the requirement to provide information to Government on request, industry expressed a preference for an approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it. As a consequence an alternative regulatory framework designed with less focus on administrative processes and technical requirements, but greater emphasis on outcomes, has been developed for consideration.

### **3.2 Compliance framework**

C/CSPs are obliged to protect the privacy of their customers' information; however there are many different ways that a C/CSP may be organised which will affect its ability to be able to confirm the security of its network and the information held on it. Where a C/CSP relies heavily on sub-contracted, outsourced or off-shored maintenance or services it will be more complicated to oversee the maintenance of security than a C/CSP that manages its network and information held on it in-house.

The industry consultation has led to consideration of whether a compliance framework, based on requiring C/CSPs to be able to demonstrate competent supervision and effective controls over their networks, may be a more effective approach. Such an approach would focus on the ability of a C/CSP to manage the security of its infrastructure and the information held on it. Information about a possible 'compliance framework' is provided below.

**Competent supervision** refers to the ability of a C/CSP to maintain technically proficient oversight (either in-house or through a trusted third party) of the operations of their network, and the location of data; awareness of, and authority over, parties with access to network infrastructure ;and a reasonable ability to detect security breaches or compromises.

**Effective control** refers to the ability of a C/CSP to maintain direct authority and / or contractual arrangements which ensure that its infrastructure and the information held on it is protected from unauthorised interference (which refers to network access). This might include arrangements to:

- cease contracts where there has been a security breach,
- direct contractors to carry out mitigation or remedial actions,
- oblige contractors to monitor and report breaches to the C/CSP, and
- repatriate information and network systems where unauthorised interference to a network has occurred.

Under such a compliance framework, Government would provide guidance to assist industry to understand and meet its obligation, and to inform C/CSPs how they can maintain competent supervision and effective control over their networks. Guidance would be tailored to C/CSP service types (for example internet service providers (ISP), backhaul service providers, and mobile virtual network operators) and distributed to C/CSPs prior to commencement of a framework.

The aim of such a regulatory framework would be to promote risk informed management of security in the telecommunications sector. This could be achieved by educating C/CSPs on national security risks and encouraging ongoing awareness and responsibility for network security, reducing the need for government intervention. Provision of general security advice, briefings and the development of guidance would be intended to be an ongoing, iterative process conducted in cooperation with industry, which would reflect evolving technologies and markets.

Under a regulatory framework Government would also disseminate information on specific security threats to affected C/CSPs on an as needs basis, including:

- targeted briefings (specific threat and risk information), and
- provision of specific mitigation information.

In order to monitor compliance with the obligations under a framework C/CSPs would be required upon request, to demonstrate compliance to Government. This could be done by compliance assessments and audits, based on a risk assessment to inform the level of engagement required. The level of engagement would be informed by factors such as:

- market share;
- customer base; and
- service offerings.

Government is giving consideration to the means by which it could be assured that industry had taken reasonable mitigations steps to address security risks. It would benefit from the Committee's advice on appropriate assurances mechanisms. These might include accreditation of industry for self-assessment purposes or a role for third parties in providing audit and assurance services. For example, in-depth compliance assessment and audits could focus on C/CSPs that security agencies consider are at greater risk of national security threats. Less intensive compliance assessment and audits would apply to selected C/CSPs from the broader pool of lower risk entities. This approach would monitor and evaluate industry-wide governance arrangements to ensure C/CSPs maintain competent supervision and effective control over their networks and facilities.

### **3.3 Directions and penalties**

Government would seek to use advice and guidance to encourage risk informed management of security concerns. Where potential issues of concern are identified, the preferred approach would be to engage with the relevant C/CSPs to establish whether national security concerns can be co-operatively addressed. Where this is not possible, one way to proportionately address various levels and forms of non-compliance could be to provide a graduated suite of enforcement measures (including the power of direction). The availability of enforcement measures would provide industry with greater incentive to engage co-operatively with Government.

Under such an approach, in cases where engagement with C/CSPs proves to be ineffective, or a blatant disregard of security information jeopardises the Government's confidence in the security and integrity of Australia's telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance. To safeguard such a power, it could require the Secretary of the Attorney General's Department, to seek the concurrence of the Director General of Security and the Secretary of the Department of Broadband, Communications and the Digital Economy, before directing a C/CSP to alter its business practices or undertake other actions considered necessary to protect national security interests. This would generally follow a period of more direct and intensive engagement with the C/CSP concerned.

Directions could involve targeted mitigation or remediation of security risks, including modifications to infrastructure, audit, and ongoing monitoring, with costs to be borne by the relevant C/CSP. Grounds for directing mitigation or alternative actions would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. The powers of direction would serve as a means to support the existing powers in the Telecommunications Act relating to national interest matters.

To encourage C/CSPs' recognition and compliance with their security obligations under this regulatory framework, financial penalties are proposed. Financial penalties could be used in situations where, for example, a C/CSP fails to take reasonable action to protect its infrastructure and the information held on it. These penalties could be modelled on existing civil penalties contained in the Telecommunications Act.

As described earlier, the current provision under subsection 581(3) of the Telecommunications Act would remain available for the most serious security breaches. This enables the Attorney-General, in consultation with the Prime Minister and Minister for Broadband, Communications and the Digital Economy, to direct C/CSPs to not use or supply, or cease using or supplying, particular services where such use or supply would be prejudicial to security. As this direction only applies to a service as a whole, however; it cannot be used to restrict service use or supply to a particular organisation, group or person. As such, subsection 581(3) is considered an option of last resort, applicable in very limited circumstances.

Should a graduated suite of enforcement measures be made available under a regulatory framework, the following circumstances provide an illustration of where the Government may consider taking enforcement action:

- **where a breach has occurred**, for example a CSP's data is accessed and published, demonstrating a failure to protect its infrastructure and the information held on it from unauthorised interference;
- **where a C/CSP fails to provide reasonable assistance to Government to demonstrate compliance when requested;**
- **where there is failure by a C/CSP** to undertake mitigation activities that Government has determined are necessary to protect its infrastructure and the information held on it from unauthorised interference; or
- **where there is failure by a C/CSP to otherwise satisfactorily demonstrate it has competent supervision or effective control over its networks.**

The framework is intended to maximise cooperative engagement between C/CSPs and Government on matters of national security. Where such a relationship works effectively, there may be no need to invoke more formal directive powers. Administrative penalties or directions to C/CSPs would only be imposed where a risk has been assessed as significant and prior engagement has proved ineffective.

### **3.4 Transition arrangements**

Should any legislative changes be agreed, this would require all C/CSPs to comply with the security obligations. In some instances this will require the application of mitigation measures to existing infrastructure. The security obligations would apply to existing and new infrastructure. Government recognises that it would need to work closely with industry to ensure that there is a reasonable transition period.

## **4. Next Steps**

Government recognises that a regulatory framework would include a cost to industry, which may increase prices for consumers and it is working to understand these costs through targeted consultation. This work will be complemented by the Parliamentary Joint Committee on Intelligence and Security's consideration.

## CHAPTER FOUR

### AUSTRALIAN INTELLIGENCE COMMUNITY

### LEGISLATION REFORM

---

#### 1. Introduction

It is the responsibility of Government to protect society against threats to our national security. The Government must be vigilant and take appropriate action to ensure that any threats to our national security do not materialise. Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats.

However, the security environment is continually evolving and becoming increasingly diversified. Security legislation, and the ability of intelligence agencies to protect the security and safety of Australians and our democratic institutions, must also adapt and keep pace with these changes. To enable Australia's intelligence agencies to continue to protect national security, it is imperative that these agencies are appropriately equipped with the necessary statutory powers to uphold Australia's vital national security interests.

The Attorney-General's Department and Australian Intelligence Community agencies — including the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), and the Defence Imagery and Geospatial Organisation (DIGO)—have identified a number of practical difficulties with the legislation governing the operation of these agencies, specifically the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

Addressing the problems outlined in this chapter of the Discussion Paper is necessary to maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.

At the same time, it is important that legislation governing intelligence agencies continues to include appropriate checks and balances on the exercise of their powers. Ensuring these agencies remain accountable for their actions helps to maintain public confidence in and support for the crucial work of intelligence agencies. The proposed reforms seek to maintain a strong and accountable legislative regime under which intelligence agencies can respond effectively when threats to our community emerge.



This chapter of the Discussion Paper outlines the problems identified in the operation of both the ASIO and IS Acts and contains three sections relating to matters the Government wishes to progress, matters the Government is considering, and matters on which the Government expressly seeks the views of the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

## **2. Matters the Government wishes to progress**

### **2.1 Modernise and streamline ASIO's warrant provisions**

Division 2 of Part III of the ASIO Act contains a range of powers that ASIO can use under warrant in carrying out its statutory functions. The powers include search warrants, computer access warrants, listening and tracking device warrants, and the power to inspect postal or delivery service articles. Although there have been several amendments to each of these powers in the past, the amendments have been piecemeal and have not kept pace with technological advancements. To maintain effective intelligence gathering techniques and capabilities, these powers require modernising to provide a statutory framework which facilitates intelligence collection by the most technologically effective and efficient means.

#### ***References to 'computer' in section 25A***

Computer access warrants under section 25A of the ASIO Act are limited to data stored on 'a computer' ('computer' is defined to mean a computer, a computer system or part of a computer system). Therefore, if an individual has more than one computer which is not part of the same computer system, or data is stored on a computer network, more than one warrant may be necessary. For example, if there are multiple computers on a premises, and it is only discovered upon entering the premises for the purpose of executing a warrant that a particular computer is not connected to the computer system specified in the warrant, it would be necessary to seek another warrant (and enter the premises a second time) to access the data on that particular computer. This is inefficient and does not increase the level of accountability around the issue of warrants.

A possible solution to this issue could be to amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.

#### ***Variation of a warrant***

Currently, the ASIO Act does not specifically provide for a warrant to be varied if the circumstances justify such a variation. A new warrant is required in every instance where there is a significant change in circumstances. A variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability.

***Duration of warrants***

All warrants under the ASIO Act currently last for a maximum of six months, except for a search warrant which must be executed within 90 days. A warrant enabling a search to take place within a six month period would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors. Indeed, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control, and a new warrant would be required. .

To address this, the maximum duration of a search warrant could be increased from 90 days to six months, making it consistent with the other warrant powers in the ASIO Act.

***Renewal of warrants***

Certain threats to security can endure for many years, requiring a significant proportion of warrants issued under the ASIO Act to continue beyond the initial authorisation period. However, the current provisions in the ASIO Act do not enable a warrant to be extended.

In such circumstances, ASIO must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant change to either, and where the assessment of the intelligence case remains unchanged. A renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources.

**2.2 Modernise the ASIO Act employment provisions**

Part V of the ASIO Act provides for the employment of ASIO officers and employees. These provisions do not align with the Australian Public Service (APS) framework as they were largely drafted over 30 years ago. Specific examples are discussed below.

***Requirement to hold an “office”***

Section 85 of the ASIO Act provides that the Director-General may determine the designation of officers in ASIO. Under subsection 85(1) of the ASIO Act, an officer must hold an ‘office’ that has been designated by the Director-General. With the exception of the Director-General, ASIO employees are no longer employed under the concept of the designation of ‘office’. In practice, ASIO employees are employed under a concept of level. As it is no longer relevant, this section could be considered for deletion from the ASIO Act.

***Descriptors of employment in the ASIO Act***

The ASIO Act uses several descriptors to denote a person as an ‘employee’ of ASIO. These descriptors include ‘officer,’ ‘employee’ and ‘staff’ and are not separately defined in the ASIO Act. The use of the separate terms reflects the various amendments made to the ASIO

Act since 1979 but causes confusion as to whether differences between the terms are intended.

The use of the single term 'employee' throughout the ASIO Act would clarify and ensure consistency in the Act.

### ***Special provisions relating to ASIO employees***

Section 87 of the ASIO Act provides that the terms and conditions, under which ASIO employees were employed immediately before the date of commencement of the ASIO Act, continue to apply until they are varied by agreement. There are no longer any ASIO employees affected by section 87 and it could be considered for deletion from the Act.

### ***Modernise the Director-General's powers in relation to employment terms and conditions***

The Director-General's powers and responsibilities could be modernised so they are similar to those given to the CEO of a Commonwealth department or agency under the Public Service Act. This would ensure that, subject to guidelines issued by the Attorney under paragraph 8A(1)(b) of the ASIO Act, the Director-General has the power to engage employees on behalf of the Commonwealth, the rights, duties and powers of an employer and may determine terms and conditions of employment.

### ***Proposed secondment arrangements***

In order to access specialist skills and as part of arrangements whereby ASIO works closely with other agencies, ASIO often places staff of other agencies to work within ASIO, or agrees to its staff members working in other agencies. Legal complexities can arise in making such arrangements because of the specified scope of the functions and powers of ASIO and the other organisation involved.

If the ASIO Act were amended to expressly enable staff to be 'seconded' to and from ASIO and to clarify that, during the secondment, a seconded staff member carries out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation, it would enhance ASIO's ability to engage with other agencies, and overcome administrative difficulties ASIO currently experiences in relation to existing secondment arrangements.

Such a secondment regime would operate independently from section 19A of the ASIO Act and section 13A of the IS Act. Section 19A enables ASIO to cooperate with and assist intelligence agencies, law enforcement agencies and prescribed Commonwealth and State authorities. An ASIO officer working in a multi agency task force operating under section 19A continues to carry out the functions of ASIO. Those functions would (as a consequence

of section 19A) include carrying out the functions of the other agencies involved in the task force. It is suggested that, unlike section 19A arrangements, these secondment arrangements would not be limited to intelligence, law enforcement and prescribed agencies.

### **2.3 Clarify the authority of the Defence Imagery and Geospatial Organisation**

Minor amendments to DIGO's function under section 6B(e) of the IS Act would make some minor clarifications to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions.

At present the IS Act enables DIGO under its subsection 6B(e) function to:

- a. provide imagery and geospatial data to produce non-intelligence products for use by Commonwealth, State and Territory authorities, as well as for certain non government bodies and foreign governments approved by the Minister (paragraph 6B(e)(i))
- b. provide technical assistance to the Australian Defence Force, Commonwealth, State and Territory agencies (as well as to certain approved non-government bodies and foreign governments approved by the Minister) in relation to the production and use of imagery and geospatial products, not being 'intelligence information' obtained for the purposes of subsections 6B(a), (b) or (c) (para. 6B(e)(ii)), and
- c. provide assistance in relation to Commonwealth, State and Territory authorities (as well as for certain non-government bodies and foreign governments approved by the Minister) in relation to the performance of these authorities or bodies of emergency response functions (as defined by the IS Act).

DIGO's work under this function may therefore involve collecting imagery and other data in relation to locations inside and outside Australia, but what distinguishes its subsection 6B(e) function from DIGO's 'intelligence functions' under subsections 6B(a) to (d), is that the work is not done for the purpose of providing information about a particular person or entity. This does not mean that intelligence sources or capability are not utilised for the function, but rather DIGO's intent, or the activities which are undertaken for the purposes of this function, do not fall within the scope of 'intelligence information' purposes (as defined by the IS Act.)

It is proposed that, amending paragraph 6B(e)(ii) of the IS Act would clarify the activities that are included in the scope of this function. These amendments would seek to:

a. Clarify the scope of application of paragraph 6B(e)(ii) - The current wording of paragraph 6B(e)(ii) is; 'assistance in relation to the use of such imagery and products'. The inclusion of the word 'such' in this subsection has given rise to an unintended encumbrance, as it has the effect of linking this function to the preceding paragraph 6B(e)(i) function. The original intent of paragraph 6B(e)(ii) was to enable DIGO to provide expert technical assistance and advice on the production and use of all DIGO imagery and geospatial products, not only with respect to its 'non-intelligence information' activities and products covered by paragraph 6B(e)(i).

Paragraph 6B(e)(ii) could be amended to remove the word 'such', so as to avoid any doubt that DIGO is enabled to provide Commonwealth and State authorities, and other approved bodies, assistance in relation to the production and use of both non intelligence and intelligence imagery and geospatial products.

b. Include an express reference to specialised imagery and geospatial technologies - DIGO has an express function under paragraph 6B(e)(ii) to provide assistance in relation to the production and use of imagery and other geospatial products to Commonwealth, State and Territory authorities and bodies approved in writing by the Minister.

In line with this function (and implied under DIGO's 'communication' function in subsection 6B(d) for the purposes of subsections 6B(a) to (d)), DIGO assists Commonwealth, State and Territory authorities (as well certain non-government bodies and foreign governments as approved by the Minister) with the use and application of specialised imagery and geospatial technologies, including geospatial web-based services. However, this is not expressly provided for as a function of DIGO.

An express reference to this activity would avoid any doubt that DIGO is able to assist in this way and to ensure the prevention of any perceived gaps in DIGO's functions. These changes would further provide DIGO with the scope and flexibility to meet White Paper objectives, including the proposed acquisition of domestic satellite collection capability by Defence.

The proposed amendments do not change the original intended operation of section 6B of the IS Act. The existing safeguards in the IS Act would remain unaffected and in place. The suggested changes involve minor clarifications to provide more certainty and practical utility. By making the legislation clearer, it would be easier for the Inspector-General of Intelligence and Security to effectively review whether DIGO is operating within its powers, and ensure accountability is maintained.

### 3. Matters the Government is considering

#### 3.1 Amend the ASIO Act to create an authorised intelligence operations scheme

ASIO's continued ability to collect useful and relevant intelligence on the most serious threats to the security of Australia and Australians, hinges on its capacity to covertly gain and maintain close access to highly sensitive information. This activity often involves engaging and associating closely with those who may be involved in criminal activity and therefore has the potential to expose an ASIO officer or human source to criminal or civil liability, in the course of their work.

With the enactment of broad overarching laws criminalising security related issues, many of those targets under investigation are involved in activities that breach the criminal law. Increasingly, those laws are capable of capturing the activities of persons who are associating covertly with targets, notwithstanding that their activities are for lawful intelligence collection purposes.

For example, under Part 5.3 of the Criminal Code, it is an offence to intentionally provide training to or receive training from a terrorist organisation where the person is reckless as to whether the organisation is a terrorist organisation. Therefore, if an ASIO officer or human source is tasked to collect covert intelligence in relation to a terrorist organisation, they may be open to criminal liability under the Criminal Code if, in the course of collecting the relevant intelligence, they receive training from that organisation.

An authorised intelligence operations scheme would significantly assist covert intelligence operations that require undercover ASIO officers or human sources to gain and maintain access to highly sensitive information concerning serious threats to Australia and its citizens. A scheme similar to the controlled operations scheme under the *Crimes Act 1914* could be developed to apply to ASIO officers and human sources operating under the ASIO Act, with appropriate modifications and safeguards that recognise the scheme would operate in the context of covert intelligence gathering investigations or operations.

Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility and appropriate oversight and accountability. Key features that may contribute to such could include:

- the Director-General of Security to issue authorised intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months)

- oversight and inspection by the Inspector-General of Intelligence and Security (IGIS), including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General
- specifying conduct which cannot be authorised (eg, intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person), and
- independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement.

### **3.2 Modernise and streamline ASIO's warrant provisions**

#### ***Named person warrants***

In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types, which is administratively burdensome.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.

#### ***Surveillance Devices – use of optical devices***

Legislation governing ASIO's capabilities with respect to electronic surveillance has not been updated to align with legislation governing the use of electronic surveillance by law enforcement. ASIO's ability to use optical surveillance devices is tied to its ability to use listening devices. This is a relic of the time in which the ASIO Act was first drafted. Additionally, the administrative and procedural provisions governing the use of listening and tracking devices in the ASIO Act are not aligned with provisions governing the use of surveillance devices by law enforcement.

In practice, this acts as an impediment to effective cooperation and collaboration with law enforcement partner agencies. For example, the differences in scope and terminology between the ASIO Act and the Surveillance Devices Act limit actions which can be taken by each agency in working with partner agencies. Aligning the surveillance device provisions in the ASIO Act with the more modern Surveillance Devices Act could assist in overcoming these impediments to cooperation.

***Authority for acts necessary to execute a computer access warrant***

The increasingly complex nature of the global information technology environment and the use by some targets of sophisticated computer protection mechanisms can adversely impact ASIO's ability to execute a computer access warrant for the purpose of obtaining access to data relevant to security.

Subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.

To address this, section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant.

***Person searches***

The ASIO Act currently contains the power to search a premises (section 25). Contained within this is the power to search a person who is *at or near* the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to the security matter (subsection 25(4A)).

Where ASIO assess that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched. However, it is not always feasible to execute a search warrant on a person of interest while they are '*at or near*' the premises specified in the warrant.

For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible. The existing limitation could be addressed by enabling ASIO to request a warrant to search a specified person rather than premises (subject to existing safeguards in subsections 25(4B) and 25AA) so that there would be sufficient operational flexibility while maintaining appropriate accountability via the warrant process.

***Authorisation lists for warrants***

Section 24 of the ASIO Act provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of this section) may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act.



The requirement to maintain a list of the individual names of each officer who may be involved in executing a warrant can create operational inefficiencies for ASIO. For example, sometimes the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to quickly expand the list of authorised persons.

The problem could be overcome in large part if the Director-General could approve classes of people to execute a warrant. For example, the Director-General could authorise officers of a certain level within a particular Division of ASIO. Such persons at any one time would be readily ascertainable ensuring the level of accountability is not diminished, while improving operational efficiency.

### **3.3 Clarify ASIO's ability to cooperate with the private sector**

Subsection 19(1) of the ASIO Act enables ASIO to cooperate with authorities of the Commonwealth, as well as Departments, police forces and authorities of the States, where it is necessary or conducive to the functions of ASIO. It is unclear whether section 19 could be read to imply that ASIO should not cooperate with organisations outside of government.

This concerns ASIO given the important role the private sector plays in Australia's national security, including by owning and operating a significant proportion of Australia's critical infrastructure. Furthermore, it is conducive to ASIO's functions to cooperate with the private sector. For example, ASIO's Business Liaison Unit (BLU), provides an interface between Australian business and the Australian Intelligence Community. The BLU provides intelligence backed reporting that can be used for risk management decision making. Such reports include reporting on the current security environment and threats to particular industry sectors.

It may be desirable to amend subsection 19(1) to avoid any doubt about ASIO's ability to cooperate with the private sector.

### **3.4 Amend the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act**

Section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their association with ASIO. In particular, information may only be passed to law enforcement agencies in relation to a 'serious crime' (defined as an offence punishable by imprisonment exceeding 12 months). Section 92, which makes it an offence for a person to publish the identity of an ASIO officer, is punishable by 12 months imprisonment. By virtue of section 18, ASIO is precluded from passing information about the possible commission of this offence to law enforcement agencies.

## **4. Matters on which the Government expressly seeks the views of the PJCIS**

### **4.1 Modernise and streamline ASIO's warrant provisions**

#### ***Use of third party computers and communications in transit***

The ASIO Act recognises the importance of ensuring ASIO is able to access computers where necessary for the performance of its statutory functions and where approved by the Attorney-General.

However, advancements in technology have made it increasingly difficult for ASIO to execute its computer access warrants. Where a target is security conscious, innovative methods of achieving access to the target computer have to be employed. In the same way that access to a third party premises may be necessary to execute a search warrant, it may be necessary to use a communication that is in transit or use a third party computer for the purpose of executing a computer access warrant.

To overcome this problem, it may be appropriate to amend the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer. Noting that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.

#### ***Incidental Entry***

Sections 25 and 25A of the ASIO Act currently enable an officer, in the execution of a search or computer warrant, to do any thing that is reasonably incidental to the exercise of powers under that warrant. It is not clear whether this incidental power includes entry to a third party's premises for the purposes of executing the search or computer warrant.

Additionally, it may be necessary to enter a third party premises for the purposes of installing a surveillance device. Clarification of the scope of the incidental power would assist ASIO in executing search and computer warrants.

#### ***Use of force***

Subsections 25(7), 25A(5A), 26B(4) and 26C(4) relate to the use of force when exercising a power under a warrant and when entry into a premises is authorised under the warrant. The headings to each of those subsections suggest that the powers in those subsections are limited to entry to the target premises. The provisions relating to use of force are not limited in such a way. Technical amendments may therefore be necessary to correct this drafting anomaly.

### ***Evidentiary Certificates***

Currently, protecting information that reveals sensitivities about the identity of ASIO officers and capabilities used in the course of exercising special warrant powers relies on successful public interest immunity claims or, where available, orders obtained under the *National Security Information (Criminal and Civil Proceedings) Act 2004*. Unlike the *Telecommunications (Interception and Access Act) 1979* (TIA Act) and the *Surveillance Devices Act 2004* (SD Act), there is no consistent regime to protect ASIO information, capabilities and officer identities under the ASIO Act.

An evidentiary certificate regime could be introduced in the ASIO Act, similar to those which exist under the TIA and SD Acts, to provide a legislative basis for assisting ASIO to protect the identity of officers and sensitive capabilities involved in the execution of warrant powers.

## **4.2 Amend the Intelligence Services Act 2001**

Australia's foreign intelligence agencies, ASIS, DSD and DIGO, collect intelligence in accordance with requirements set by Government and operate under the IS Act. These agencies have identified problems arising out of the operation of the IS Act, which are considered below.

### ***Ministerial Authorisations***

The IS Act imposes strict controls on the ability of those agencies to produce intelligence on an Australian person. The Minister responsible for each Australian foreign intelligence agency is required to direct that the agency obtain authorisation from the Minister before undertaking an activity, or a series of activities, for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person.

Before giving an authorisation to produce intelligence on an Australian person, the responsible Minister must be satisfied under section 9(1) that:

- any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned, and
- there are satisfactory arrangements in place to ensure that
  - nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency, and
  - the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

According to section 9(1A)(a), before giving an authorisation to produce intelligence on an Australian person, the responsible Minister must be satisfied that the Australian person is, or is likely to be, involved in one or more of the following activities:

- activities that present a significant risk to a person's safety;
- acting for, or on behalf of, a foreign power;
- activities that are, or any likely to be, a threat to security (for this ground the Minister must also obtain the agreement of the Attorney-General);
- activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
- committing a serious crime by moving money, goods or people;
- committing a serious crime by using or transferring intellectual property;
- committing a serious crime by transmitting data or signals by means of guided and/or unguided electromagnetic energy; and
- activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law.

These activities do not specifically cover the situation where a person is or is likely to be involved in intelligence or counter-intelligence activities.

A new item could be added to the list in section 9(1A)(a) of the IS Act which would allow the Minister to give an authorisation if he or she is satisfied that the person is, or is likely to be, involved in intelligence or counter-intelligence activities. This would allow the Minister to issue an authorisation where the current grounds, for example, 'activities that present a significant risk to a person's safety,' are not available because the risk is to ASIS operations or is not specific to a person's safety.

In particular, this would assist ASIS to perform its existing function of conducting counter-intelligence activities under section 6(1)(c) of the IS Act and allow DSD and DIGO, at the request of ASIS and with approval from their Minister, to assist ASIS. In turn this would enable these agencies to protect their operations and those involved in them by allowing the agencies to produce intelligence on a person who the Minister is satisfied is, or is likely to be, involved in intelligence or counter-intelligence activities. This activity may detect the interference of a foreign power, in which case ASIO would normally become involved in assessing any threat to security.

It is imperative that Australia's intelligence agencies are appropriately equipped to protect Australia's vital national security interests. This includes the ability for Australia's foreign intelligence and security services to interact and work seamlessly together.

In March 2011, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* made amendments to the ASIO Act and the IS Act to enable Australia's intelligence agencies to more closely cooperate and assist one another in the performance of each other's functions. Specifically, section 13A of the IS Act was introduced to facilitate greater cooperation in multi-agency teams, such as under the Counter Terrorism Control Centre, which is hosted by ASIO, and enable agencies to harness resources in support of key national security priorities.

However, there are differences in the legislative regimes which apply to ASIS, DSD and DIGO under the IS Act and to ASIO under the ASIO Act when they produce intelligence on Australian persons. In part these differences reflect the different nature and functions of the IS Act agencies and ASIO. When the agencies are cooperating and assisting ASIO in the performance of ASIO's functions, these differences have led to situations being identified where ASIO is able to undertake an activity for the purposes of its functions but an agency subject to the IS Act may not be able to fully cooperate with and assist it.

To better meet the intention of enabling Australia's intelligence agencies to cooperate and assist each other in the performance of each other's functions to protect Australia and Australians, section 13A of the IS Act could be amended. For example, section 13A could be amended to enable the Minister responsible for an IS Act agency to authorise specified activities where the agency is cooperating with ASIO in the performance of an ASIO function. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required. This change would create greater consistency between the ministerial approval regime that applies to the IS Act agencies and the approval regime which applies to ASIO.

The proposal is principally intended for ASIS and ASIO cooperation relating to the capabilities, intentions and activities of people or organisations outside Australia. Given existing Defence agencies' functions and capabilities, and the nature of the activities to which the proposal is sought to address, it is unlikely that Defence would utilise the proposed change.

The existing safeguards in the IS Act could apply to the proposed section 13A authorisation. These include the requirement for all ministerial authorisations to be provided to the IGIS who oversees the legality and propriety of the operations of the intelligence agencies. Additionally, the communication and retention of intelligence collected under the ministerial authorisation would be subject to the Privacy Rules.

The proposed changes to section 13A could also operate in a limited set of circumstances:

- A ministerial authorisation under the proposed changes to section 13A would usually only be issued for a discrete activity for a specified purpose where ASIS is cooperating with ASIO in connection with the performance of its functions. This category of ministerial authorisation will not be able to be issued to ASIS, DSD and DIGO to assist another IS Act agency, or a prescribed Commonwealth authority, or a State authority.
- A ministerial authorisation under section 13A will not replace the need to obtain a warrant where a warrant would currently be required under the ASIO Act or the TIA Act.
- Renewal could be sought, but where a ministerial authorisation under a section 9(1A) ground could be sought, further ministerial authorisation would need to be sought under sections 8 and 9 of the IS Act rather than as a renewal of the section 13A authorisation.

### ***ASIS co-operation on self-defence and weapons training***

ASIS operates in a number of very dangerous locations overseas. In recognition of this, the IS Act was amended in 2004 to enable ASIS staff members and agents to receive training in the use of weapons and self-defence techniques, subject to a number of important safeguards (schedule 2).

However, under this regime, ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. The IS Act does not currently enable ASIS staff members to participate in joint training in the use of weapons with persons cooperating with ASIS, even though ASIS staff members are authorized to use weapons to protect such persons. At a practical level, the current inconsistency restricts joint training activities because ASIS trainers cannot run training that includes individuals who are not ASIS staff members.

Such cooperation would not enable ASIO officers to carry weapons or receive training from ASIS in the use of weapons. Co-operation on weapons training would be limited to Commonwealth, State and Territory bodies that have, under some other law, a right to carry weapons in the course of their duties. This will cover training with law enforcement and military personnel.

Such cooperation would enable ASIS to cooperate with a limited number of approved overseas authorities in the delivery of training in self defence and weapons. Such cooperation could be limited to authorities approved by the Foreign Minister under section

13(1A) of the IS Act. Such an approval requires the Foreign Minister to first consult with the Prime Minister and Attorney-General.

## **5. Next Steps**

This Chapter has discussed the Australian Intelligence Community legislative reform aspect of the package of reform proposals referred to the PJCS for inquiry and consultation. The Government recognises that some of the reforms are controversial and may attract significant media interest. To avoid public misunderstanding as to the nature of these reforms, it is imperative that the PJCS take into account a wide range of views on the proposals from public stakeholders and government agencies. This will ensure that any measures brought forward to enhance the intelligence gathering capabilities of our intelligence agencies continue to be subject to appropriate checks and balances on these powers.

## **CONCLUSION**

---

The preceding chapters of this Discussion Paper have elaborated on the complex international security environment in which our intelligence and law enforcement agencies operate. Ideas for telecommunications interception reform (Chapter 2), telecommunications sector security reform (Chapter 3) and Australian intelligence community reform (Chapter 4) seek to equip these agencies with the capability to meet today's emerging national security challenges.

In light of the issues discussed, the Government seeks the views of the PJCIS on the package of ideas. This Discussion Paper will prove useful as a basis for stakeholder consultation. A number of key industry representatives and Government agencies will seek to provide their views on the proposals to the PJCIS.



---

## GLOSSARY OF KEY TERMS

---

### **The ACMA – The Australian Communications and Media Authority**

#### **Ancillary service providers**

Telecommunications industry participants who are not carriers or carriage service providers.

#### **Anonymous pre-paid services**

A mobile phone or other communications service where credit is purchased in advance of the service being used. In circumstances where the pre-paid service can be obtained without providing personal details, or by providing false details, the service is an ‘anonymous’ pre-paid service.

#### **ASIO – Australian Security Intelligence Organisation**

#### **ASIS – Australian Secret Intelligence Service**

#### **ASIO Act – Australian Security Intelligence Organisation Act 1979**

#### **Calling cards**

Otherwise known as telephone cards, are pre-paid cards which allow payment for telephone services. Calling cards are typically intended for use by travellers.

#### **Carriage service providers**

A CSP is an entity that supplies a carriage service to the public using a telecommunications network unit. CSPs can include organisations that resell time on a carrier network for phone calls, provide access to the internet (Internet Service Providers) or provide telephone services over the internet (VoIP service providers).

#### **Carrier**

A carrier is an owner of a telecommunications network unit that is used to supply carriage services to the public. Carrier licences are granted by the Australian Communications and Media Authority (ACMA) under section 56 of the Telecommunications Act.

#### **Ciphers**

A method of transforming text in order to conceal its meaning.

#### **Communications Packets**

A formatted unit of data which comprises a communication passing over a packet-switched network.

#### **Content**

The substance of a communication, for example the subject line and body of an e-mail or what is said during a phone call

**Data**

Information about a communication that is not the content or substance of a communication

**Data retention**

The storage of telecommunications data for prescribed periods of time.

**Data set**

The specific set of data that would be required to be retained under a data retention regime

**Decryption**

The act of decoding of encrypted information into a meaningful form.

**DIGO – Defence Imagery and Geospatial Organisation**

**DSD – Defence Services Directorate**

**Encryption**

The encoding of data so that it cannot be decoded without appropriate software or hardware, so as to prevent authorised access.

**e-payment**

Payment for buying and selling goods or services offered through the Internet, or more broadly, any type of electronic funds transfer.

**Gigabytes**

For digital information or computer storage a gigabyte represents 1 billion bytes.

**GPS - The Global Positioning System**

A space-based satellite navigation system that provides location and time information anywhere on Earth

**ICT – Information and communications technology**

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

**Identifiers to communications**

Information such as a phone number or email address, linking the target of an interception warrant to the service or device to be intercepted.

**Industry Participant**

Any member of the telecommunications industry, including carriers, carriage service providers and ancillary service providers.

### **Inter-carrier roaming agreements**

An agreement between carriers to ensure that wireless devices remain connected to the network despite changing locations.

### **IS Act – Intelligence Services Act 2001**

### **ISP – Internet Service Provider**

An ISP is any entity that provides access to the Internet.

### **IP – Internet Protocol**

A standard protocol for transmission of data from source to destinations in packet switched communications networks and interconnected systems of such networks.

### **Megabits**

For digital information or computer storage a megabit represents 1 million bits.

### **NBN – National Broadband Network**

The National Broadband Network is a next-generation broadband network. The network comprises three technologies – optic fibre, fixed wireless and next-generation satellite – and will provide more reliable, high-speed broadband access to all Australians.

### **Penalty Units**

An amount of money used to determine a pecuniary penalty – currently \$110.

### **Propriety data formats**

A file or communication format that is the intellectual property of an individual or organisation.

### **PSTN - Public switched telephone network**

The network of the world's public circuit-switched telephone networks. It consists of telephone lines, fibre optic cables, microwave transmission links, mobile networks, communications satellites, and undersea telephone cables, all inter-connected by switching centres, allowing any telephone in the world to communicate with any other.

### **Resold services**

A service which is provided by a wholesaler and resold to customers via another telecommunications industry participant.

### **SD Act – Surveillance Devices Act 2004**

### **Serious offence**

An offence that carries a penalty of at least 7 years' imprisonment or a range of offences for which it is already recognised that general community standards would expect interception to be available, such as child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks

### **Smartphone Technology**

Mobile phones built with mobile computing capabilities.

### **Stored communications**

Communications which are no longer passing over the telecommunications system, held on carrier equipment and cannot be accessed on the equipment by a person who is not a party to the communication without the assistance of an employee of the carrier.

### **Stored communications Warrant**

A warrant authorising access to stored communications.

### **Suborning**

Bribery or procurement of a person to commit some unlawful or wrongful act.

### **Subscriber data**

Information about a subscriber to a communications service, such as name or billing address.

### **Telecommunications System**

A system over which telecommunications are transmitted. It comprises of three primary units, a transmitter, a transmission medium and a receiver.

### **Terabytes**

For digital information or computer storage a gigabyte represents 1 trillion bytes.

### **Terminal device**

A device which the end user interacts with that terminates one end of a communication, such as a phone or computer.

**TI** – telecommunications interception

**TIA Act** – *Telecommunications (Interception and Access) Act 1979*

**Traffic data** – information relating to how a communication passes across a network, such as the time, duration or location from which the communication was made.

### **Transactional data**

Data describing an event, including when it occurred.

### **TSSR – Telecommunications Sector Security Reform**

TSSR refers to the proposed regulatory framework being explored by Australian Government, which aims to manage and mitigate national security risks associated with telecommunications infrastructure.

### **VoIP – Voice over Internet Protocol**

A technology that allows real-time voice conversations over the Internet.



**Appendix F – Letter from Attorney-General  
the Hon Nicola Roxon MP to the  
Hon Anthony Byrne MP**



**THE HON NICOLA ROXON MP  
ATTORNEY-GENERAL  
MINISTER FOR EMERGENCY MANAGEMENT**

12/7195

Anthony Byrne MP  
Chair  
Parliamentary Joint Committee on Intelligence and Security  
Parliament House  
CANBERRA ACT 2600  
AUSTRALIA

Dear Mr Byrne

*Anthony,*

I refer to our meeting of 13 September 2012 and to the data retention proposal contained in my Department's discussion paper entitled "Equipping Australia Against Emerging and Evolving Threats". The Terms of Reference of my referral to the Committee state that the Government is expressly seeking the views of the Committee on a "tailored data retention scheme for periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts".

I appreciate the Committee's desire to receive further details on what this proposal may entail. I do not have a specific data retention model in mind but I can provide the following further information to clarify the parameters of this proposal.

"Telecommunications data" is information about the process of a communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the telecommunications carrier or internet service provider to establish the account, and information such as the time and date of the communication, its duration, location and type of communication.

The Government does not propose that a data retention scheme would apply to the content of communications. The content of communications may include the text or substance of emails, SMS messages, phone calls or photos and documents sent over the internet. Access to the content of communication is only ever carried out under warrants issued in accordance with the *Telecommunications (Interception and Access) Act 1979*. There is no intention to alter the requirement for warranted access to the contents of communications.

The need to consider a data retention scheme has come about because of changes in technology that have affected the behaviour of criminal and national security suspects. Targets of interest now utilise the wide range of telecommunications services available to them to communicate, coordinate, manage and carry out their activities. The ability to



lawfully access telecommunications data held by the telecommunications industry enables investigators to identify and build a picture of a suspect, provides vital leads of inquiry and creates evidence for alibis and prosecutions.

Two examples that have been provided to my Department by State agencies serve to illustrate the importance of maintaining access to telecommunications data:

- a) During a recent murder investigation there were a number of open lines of inquiry. When a human source provided information implicating a particular, previously unknown, person as responsible for the murder, telephone billing records were used to link the person nominated by the human source to another key suspect. The billing records also ultimately resulted in other lines of enquiry being discounted. The link between two of the principal offenders could not have been easily made without access to reliable telecommunications data. All the persons involved in that matter have been charged with the murder and associated offences and are currently before the courts.
- b) A corruption investigation revealed evidence of SMS communications between a police member and a member of an organised criminal network. Despite knowledge of the communications occurring recently, no data relating to the communications was available. The inability to obtain relevant information about the communications led to the loss of evidence which could have supported the investigation into the corrupt links.

In the past the telecommunications industry retained most types of telecommunications data. However, due to rapid changes in the technology and business environment Australian agencies are finding the much of the information they seek is not being kept. The main drivers are the increased use of internet protocol technology and the trend to charge customers based on volume of data sent or received rather than by transaction (such as call by call or message by message).

Australia is not alone in being forced to consider answers to these challenges. In recognition of the impact the lack of access and retention of telecommunications data is having on investigations, the European Union adopted the EU Directive 2006/24/EC on data retention on 15 March 2006. The Directive has been implemented by the majority of the 25 Member States of the EU with the remaining Member states at various stages of implementation.

The EU Directive imposes an obligation for providers of publicly available electronic communications services and public communication networks to retain communications data for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in national law. The Directive only requires the retention of subscriber and traffic data. No data revealing the content of the communication may be retained under the Directive. The data set is at **Attachment A**.

The Directive applies to fixed network telephony (landline), mobile telephony, internet access, internet email and internet telephony. The Directive specifies that certain categories of data must be retained, namely data necessary for identifying:

- a) the source of a communication;
- b) the destination of a communication
- c) the date, time and duration of a communication;

- d) the type of a communication;
- e) users' communication equipment or what purports to be their equipment; and
- f) the location of mobile communication equipment.

The Directive requires Member States to ensure that data is retained for periods of between six and 24 months. Because there is flexibility in the Directive's requirement the EU members have picked varying retention periods appropriate for their own local needs. There is also variability in the retention period for different types of information, for example, requiring telephony data to be held for 12 months but internet data for six months.

To protect the integrity of retained data, the Directive requires Member States to ensure that operators respect four data security principles, specifically, that the retained data shall be:

- a) of the same quality and subject to the same security and protection as those data on the public communications network;
- b) subject to appropriate technical and organisation measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
- c) subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and
- d) destroyed at the end of the period of retention, except those that have been accessed and preserved for the purposes set down in the Directive.

The reasons for the implementation of the EU Directive are explained in the preamble to the Directive as a response to terrorist attacks in Europe (particularly, the Madrid and London bombings), the maintenance of ability to fight crime and terrorism and for the consistency and completeness of regulation across the EU.

For Australia, the principal argument in favour of a data retention scheme is to maintain our agencies' access to a critically important source of intelligence and evidence. Agencies have indicated that the need to access this information is immediate and that the eroding of such access is already seriously affecting agency investigations.

I understand that the AFP will be appearing before the Committee and they will be in a position to provide details of the operational requirements for a potential data retention scheme in Australia.

I thank the Committee for its work on this and the other matters that I have referred for your consideration and I look forward to obtaining your advice on what you would consider to be an appropriate data retention scheme in Australia.

Given the high level of public interest in this inquiry I intend to make this further correspondence to the committee, public.

Yours in friendship



**NICOLA ROXON**

Encl : Attachment A – EU Directive on Data Retention data set



**Article 5 of the EU Data Retention Directive**

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.**



**Appendix G – Letter from Mr Roger Wilkins  
AO, Secretary of the Attorney-General's  
Department, to the Hon Anthony Byrne MP**



**Australian Government**  
**Attorney-General's Department**

Secretary

12/7195-04

17 October 2012

The Hon Anthony Byrne MP  
Chair  
Parliamentary Joint Committee on Intelligence and Security  
Parliament House  
CANBERRA ACT 2600

Dear Mr Byrne

**Telecommunications Data – Departmental View**

During the Parliamentary Joint Committee on Intelligence and Security's inquiry into potential national security reforms a large number of submissions raised concerns regarding the proposed establishment of a data retention regime, specifically in relation to what information may be being considered for inclusion in such a regime.

While the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) does not contain a definition of telecommunications data (also referred to as metadata, communications data and communications associated data), the Department has prepared a document which outlines what types of data the Department considers to fall within the term telecommunications data.

This document was prepared for the Committee to assist in the Committee's consideration of the issues before the inquiry; however I note that this document was tabled on 16 October 2012 as part of the Department's evidence to the Senate Legal and Constitutional Affairs Committee Supplementary Budget estimates hearing.

I have attached the document for the Committee's consideration and note that the contents of this document have not been endorsed by the Government.

The action officer for this matter is Catherine Smith who can be contacted on 6141 2900.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'RW', with a long horizontal flourish extending to the right.

Roger Wilkins AO



## **Definition of Telecommunications Data**

**Also known as Metadata, Communications Data and Communications Associated Data**

This data falls into 2 categories:

- 1. Information that allows a communication to occur**
- 2. Information about the parties to the communications**

Relates to communications for:

1. telephones – both fixed and mobile
2. 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, ie cell tower.
- 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
- Same information on recipient party if known by the service provider.





## **Appendix H – Telecommunications data provided to law enforcement and national security agencies by Telstra**

Data disclosed to law enforcement and national security agencies

Type of Data Disclosure	Data Classification	Authority for Release
<p>Any telecommunications data or meta data but not the content or substance of a communication. . It may include:</p> <ul style="list-style-type: none"> <li>• subscriber information (including name, address, date of birth, method of payment and related account transaction details)</li> <li>• telephone numbers of the parties involved in the communication</li> <li>• the date and time of a communication</li> <li>• the duration of a communication</li> <li>• Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication, and</li> <li>• location-based information</li> </ul>	<p>Historic data - telecommunications data that is already in existence at the time of the request for access to that data</p>	<p><b>TIA Act Section 175(2)</b> Allows ASIO to access existing information or documents.</p>
		<p><b>TIA Act Section 177</b> Disclosures by Telstra to an enforcement agency if the disclosure is reasonably necessary for the enforcement of:</p> <ul style="list-style-type: none"> <li>• criminal law; or</li> <li>• law imposing a pecuniary penalty or for the protection of public revenue.</li> </ul>
		<p><b>TIA Act Section 178</b> Allows an authorised officer of an enforcement agency to authorise a telecommunications service provider to disclose historical data if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.</p>
		<p><b>TIA Act Section 178(A)</b> Allows access to existing information or documents for locating missing persons</p>
		<p><b>TIA Act Section 179</b> Allows an authorised officer of an enforcement agency to authorise a telecommunications service provider to disclose historical data if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of a pecuniary penalty or protection of the public revenue.</p>
		<p><b>Telco Act Section 280</b> Authorises disclosure by or under law.</p>
		<p><b>Telco Act Section 284</b> Disclosure of information or document to assist ACMA, ACCC, TIO, or TUSMA to help them carry out their functions.</p>
		<p><b>Telco Act Section 286</b> Allows access to law enforcement agencies of information or documents because of a call to an emergency service number (000).</p>
		<p><b>Telco Act Section 289</b> Allows for access and disclosure of information or document relating to the affairs or personal particulars of another person and the person is aware of the usual use or disclosure of such or where they have consented in circumstances concerned.</p>



Answers to additional questions on notice from the Parliamentary Joint Committee on Intelligence and Security – Telstra Corporation – December 2012

	Historic <i>and</i> prospective data	<p><b>Telco Act Section 287</b> Allows for access to existing information or documents where reasonable grounds exist or it is reasonably necessary to prevent or lessen a serious threat to the life or health a person</p> <p><b>Telco Act Section 288</b> Allows for access to information or document if reasonably necessary for the preservation of human life at sea or if in relation to the location of a vessel at sea and is made for maritime communications purposes.</p>
Anything relating to, but not the content or substance of, a communication. It can include: <ul style="list-style-type: none"> <li>• telephone numbers of the parties involved in the communication</li> <li>• the date and time of a communication</li> <li>• the duration of a communication</li> <li>• Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication, and</li> <li>• location-based information</li> </ul>	Prospective data - telecommunications data that is collected as it is created and forwarded to the law enforcement agency in near real time as a result of the request for access to that data	<p><b>TIA Act Section 176(2)</b> Allows telecommunications service providers to disclose information or documents that come into existence during the period for which the authorisation is in force (prospective telecommunications data). The authorisation period is 90 days.</p> <p><b>TIA Act Section 180</b> Allows an authorised officer of a 'criminal law-enforcement agency' to authorise the disclosure of prospective telecommunications data. In making the authorisation, the officer must be satisfied that the disclosure is reasonably necessary for the investigation of a Commonwealth, state or territory offence punishable by more than 3 years. The authorisation period is 90 days.</p>
Communications and information being carried over a telecommunications network	Prospective (real time) communications and interception information	<p><b>Interception Warrants</b> under authority of the TIA Act, received by Telstra, authorising the <i>Organisation</i> (ASIO) to intercept telecommunications.</p> <p><b>Interception Warrants</b> under authority of the TIA Act, received by Telstra, authorising <i>Agencies</i> to intercept telecommunications.</p>
Stored communications not passing over Telstra's telecommunications network, held on equipment operated by, and in the possession of, Telstra that cannot be accessed on that equipment by a person who is not a party to the communication, without the assistance of Telstra along with some communications data embedded within said communications.	Historic communications and information	<p><b>Stored Communications Warrants</b> under authority of the TIA Act, received by Telstra, authorising access to communications.</p> <p><b>Telco Act Section 290</b> Allows for the use and disclosure of information or document or substance of a communication if in regard to all relevant circumstances, it might reasonably expected that the sender and the recipient of the communication would have consented to the disclosure if they had been made aware of it.</p>