

---

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>
<b>Background to the inquiry.....</b>	<b>1</b>
<b>Conduct of the inquiry.....</b>	<b>2</b>
<b>Structure of the report.....</b>	<b>3</b>
Chapter Two.....	4
Chapter Three.....	4
Chapter Four.....	5
Chapter Five.....	6
Appendices .....	7
<b>2 Telecommunications Interception.....</b>	<b>9</b>
<b>Strengthening the safeguards and privacy protections .....</b>	<b>10</b>
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
<b>Reforming the lawful access regime for agencies .....</b>	<b>22</b>
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
<b>Revision of the interception regime .....</b>	<b>66</b>
<b>3 Telecommunications security .....</b>	<b>69</b>
<b>Issues raised in evidence .....</b>	<b>72</b>
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
<b>Committee comment.....</b>	<b>82</b>
<b>4 Australian Intelligence Community Legislation Reform.....</b>	<b>85</b>
<b>Proposals the Government wishes to progress.....</b>	<b>86</b>
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>
<b>Introduction .....</b>	<b>139</b>
The current regime.....	141
The international experience .....	142
<b>Responses to data retention.....</b>	<b>147</b>
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.