

Telecommunications (Interception and Access) Act 1979

Annual Report for the year ending 30 June 2008



# Telecommunications (Interception and Access) Act 1979 Report for the year ending 30 June 2008

ISBN: 1 921241 73 X

#### © Commonwealth of Australia 2009

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at http://www.ag.gov.au/cca

# **CONTENTS**

LICT OF TABLEC	٠.
LIST OF TABLES ABBREVIATIONS	i\ ۷
CHAPTER 1—INTRODUCTION	1
CHAPTER 2—OVERVIEW OF THE ACT	2
Objectives of the legislation	2
Provisions relevant to this report	2
Telecommunications interception warrants Offences for which telecommunications interception warrants may be obtained Applying for telecommunications interception warrants Eligible Judges and nominated AAT members Form of applications Matters to be considered by an issuing authority	3 4 5 6
Safeguards and controls contained in the Act Inspections Destruction of records General Register of telecommunications interception warrants Special Register of telecommunications interception warrants Attorney-General to be given copies of telecommunications interception warrants and revocations and reports on outcomes	6 7 7 7
Reports by carrier Annual Report tabled by Attorney-General	8
Stored communications warrants Relevant offences Issuing authorities Form of application	8 8
Safeguards and controls relating to the stored communications regime Recordkeeping and inspections Destruction of records Annual report tabled by Attorney-General	9 9 10 10
Telecommunications data authorisations Telecommunications data Historical and prospective data Forms of application	10 10 11 11
Safeguards and controls relating to the telecommunications data regime Recordkeeping and inspections Annual report tabled by Attorney-General	12 12 12
CHAPTER 3—DEVELOPMENTS IN THE REPORTING PERIOD	13
Recent legislative and policy developments  The Telecommunications (Interception and Access) Amendment Act 2007  The Telecommunications (Interception and Access) Amendment Act 2008	13 13 14
Judicial decisions	15
Previous Annual Report	15
Effectiveness of interception	15

CHAPTER 4—TELECOMMUNICATIONS INTERCEPTION INFORMATION REQUIRED UNDER THE ACT	16
The information required	10
Which agencies may seek telecommunications interception warrants	1
Applications for telecommunications interception warrants Renewal applications for telecommunications interception warrants Applications for telecommunications interception warrants authorising entry onto premises Telecommunications interception warrants issued with specific conditions or restrictions Named person warrants Interpretative note B-Party warrants Interpretative note relating to B-Party warrants Categories of serious offences specified in telecommunications interception warrants Categories of serious offences specified in telecommunications interception warrants – all agencies	1 1 2 2 2 2 2 2 3 3 3 3 3 3 3
Duration of telecommunications interception warrants  Duration of original telecommunications interception warrants  Duration of renewal telecommunications interception warrants  Interpretative note relating to average duration of warrants across all agencies  Duration of original B-Party warrants  Duration of renewal B-Party warrants  Number of final renewals of telecommunications interception warrants	3° 4° 4° 4° 4°
Effectiveness of telecommunications interception warrants Arrests on the basis of lawfully intercepted information Prosecutions in which lawfully intercepted information was given in evidence Interpretative note relating to prosecutions and convictions statistics Percentage of 'eligible warrants'	40 40 50 50
Emergency interception	5!
Other information  Total expenditure incurred by agencies Average expenditure per telecommunications interception warrant Availability of eligible judges and nominated AAT members Interceptions on behalf of other agencies Resources devoted to telecommunications interception Emergency services facility declarations Reports by Commonwealth Ombudsman The ACC The AFP Other information	56 56 56 66 66 66
CHAPTER 5—STORED COMMUNICATIONS INFORMATION REQUIRED UNDER THE ACT	63
The information required	6
Which agencies may seek stored communications warrants?	6
Applications for stored communications warrants	6
Effectiveness of stored communications warrants Interpretative note relating to prosecutions and convictions statistics	6

CHAPTER 6—TELECOMMUNICATIONS DATA - INFORMATION REQUACT	JIRED UNDER THE 68
The information required	68
Authorisations granted	68

# **LIST OF TABLES**

Table 1	Applications for telecommunications interception warrants	18
Table 2	Telephone applications for telecommunications interception	19
Table 3	Renewal applications for telecommunications interception	20
Table 4	Applications for telecommunications interception warrants	21
Table 5	Telecommunications warrants issued with specific conditions or restrictions	22
Table 6	Original applications for named person warrants	24
Table 7	Telephone applications for named person warrants	25
Table 8	Renewal applications for named person warrants	25
Table 9	Named person warrants issued with conditions or restrictions	26
Table 10	Number of services intercepted under named person warrants	26
Table 11	Total number of services intercepted under named person warrants issued during the reporting period	28
Table 12	Applications for B-Party warrants	29
Table 13	Telephone applications for B-Party warrants	30
Table 14	Renewal applications for B-Party warrants	30
Table 15	Categories of serious offences specified in telecommunications interception warrants issued to the Australian Crime Commission	31
Table 16	Categories of serious offences specified in telecommunications interception warrants issued to the Australian Federal Police	32
Table 17	Categories of serious offences specified in telecommunications interception warrants issued to the Corruption and Crime Commission of Western Australia	32
Table 18	Categories of serious offences specified in telecommunications interception warrants issued to the Independent Commission Against Corruption	33
Table 19	Categories of serious offences specified in telecommunications interception warrants issued to the New South Wales Crime Commission	33
Table 20	Categories of serious offences specified in telecommunications interception warrants issued to the New South Wales Police	34
Table 21	Categories of serious offences specified in telecommunications interception warrants issued to the Northern Territory Police	34
Table 22	Categories of serious offences specified in telecommunications interception warrants issued to the Office of Police Integrity	34
Table 23	Categories of serious offences specified in telecommunications interception warrants issued to the Police Integrity Commission	35
Table 24	Categories of serious offences specified in telecommunications interception warrants issued to the South Australia Police	35
Table 25	Categories of serious offences specified in telecommunications interception warrants issued to the Tasmania Police	36
Table 26	Categories of serious offences specified in telecommunications interception warrants issued to the Victoria Police	36
Table 27	Categories of serious offences specified in telecommunications interception warrants issued to the Western Australia Police	37
Table 28	Categories of serious offences specified in telecommunications interception warrants issued in relation to all agencies	38
Table 29	Duration of original telecommunications interception warrants	40

Table 30	Duration of renewal of telecommunications interception warrants	41
Table 31	Duration of original B-Party warrants	43
Table 32	Duration of renewal of B-Party warrants	44
Table 33	Number of 'final renewals'	45
Table 34	Arrests on the basis of lawfully intercepted information	48
Table 35	Prosecutions in which lawfully intercepted information used in evidence	50
Table 36	Convictions in which lawfully interception information given in evidence	51
Table 37	Prosecutions and convictions in which lawfully intercepted information given in evidence	52
Table 38	Percentage of 'eligible warrants'	54
Table 39	Interceptions made in reliance on subsection 7(5) of the TIA Act	55
Table 40	Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants	56
Table 41	Average expenditure per telecommunications interception warrant	57
Table 42	Availability of Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT Members to issue telecommunications interception warrants	58
Table 43	Number of telecommunications interception warrants issued by Federal Court Judges, Family Court Judges, Federal magistrates and nominated AAT Members	58
Table 44	Number of interceptions carried out on behalf of other agencies	59
Table 45	Recurrent costs of interceptions per agency	59
Table 46	Emergency service facility declarations	60
Table 47	Applications for stored communications warrants	64
Table 48	Number of arrests, proceedings and convictions made on the basis of lawfully accessed information	67
Table 49	Number of authorisations made for access to existing information or documents in the enforcement of the criminal law	69
Table 50	Number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty	70
Table 51	Prospective authorisations	72
Table 52	Average specified and actual time in force	73

#### **ABBREVIATIONS**

AAT Administrative Appeals Tribunal

ACC Australian Crime Commission

ACLEI Australian Commission for Law Enforcement Integrity

AFP Australian Federal Police

ASIO Australian Security Intelligence Organisation

Blunn Report Report of the Review of the Regulation of Access to

**Communications** 

CAC Communications Access Co-ordinator

CCC WA Corruption and Crime Commission of Western

Australian

CMC Queensland Crime and Misconduct Commission

ICAC Independent Commission Against Corruption

(New South Wales)

NSW CC New South Wales Crime Commission

NSW Police New South Wales Police Force

NT Police Northern Territory Police

OPI Office of Police Integrity (Victoria)

PIC Police Integrity Commission (New South Wales)

SA Police South Australia Police

Tas Police Tasmania Police
Vic Police Victoria Police

WA Police Western Australia Police

2007 Amendment Act Telecommunications (Interception and Access)

Amendment Act 2007

2008 Amendment Act Telecommunications (Interception and Access)

Amendment Act 2008

The TIA Act Telecommunications (Interception and Access) Act

1979

Telecommunications Act Telecommunications Act 1997

## **CHAPTER 1—INTRODUCTION**

- 1.1 This is the twentieth Annual Report on the *Telecommunications* (*Interception and Access*) *Act 1979* (the TIA Act). This report relates to the period from 1 July 2007 to 30 June 2008.
- 1.2 Chapter 2 outlines the objectives and the structure of the TIA Act.
- 1.3 Chapter 3 records relevant developments that have occurred during the reporting period.
- 1.4 Chapter 4 presents the information collected in accordance with the statutory requirements of Part 2-8 of the TIA Act, relating to the interception of telecommunications.
- 1.5 Chapter 5 presents the information collected in accordance with the statutory requirements of Part 3-6 of the TIA Act, relating to accessing stored communications.
- 1.6 Chapter 6 presents the information collected in accordance with the statutory requirements of Part 4-2 of the TIA Act, relating to accessing telecommunications data.

#### CHAPTER 2—OVERVIEW OF THE ACT

2.1 This chapter provides an overview of the TIA Act, including an outline of its objects and a description of the provisions that are most relevant to the contents of this report. In addition, this chapter includes an outline of the accountability provisions of the TIA Act.

# Objectives of the legislation

- 2.2 The TIA Act has two key purposes. Its primary object is to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act makes it an offence to intercept communications, or access stored communications, other than in accordance with the provisions of the TIA Act. The second purpose of the TIA Act is to specify the circumstances in which it is lawful to intercept, access communications or authorise the disclosure of telecommunications data.
- 2.3 A telecommunications service may be intercepted under the authority of a telecommunications interception warrant by an *interception agency* for the investigation of a serious offence, or by the Australian Security Intelligence Organisation (ASIO) for national security purposes. A stored communication may be accessed under the authority of a stored communications warrant by a *law enforcement agency* for the investigation of a serious contravention or by ASIO for national security purposes. Telecommunications data may be disclosed by a telecommunications service provider under the authorisation of an officer holding a management office or position of an *enforcement agency*.

## Provisions relevant to this report

- 2.4 The foundations of the TIA Act are contained in subsections 7(1) and 108(1) which prohibit the interception of a communication passing over the telecommunications system or access to stored communications. Chapter 4 of the TIA Act allows the disclosure of telecommunications data which is ordinarily prohibited by the *Telecommunications Act 1997*.
- 2.5 Subsection 6(1) of the TIA Act defines interception as listening to or recording, by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication.
- 2.6 The effect of section 6AA and paragraph 108(1)(b) of the TIA Act is that accessing a stored communication comprises listening to, reading or recording a stored communication where that action is done with the assistance of a carrier. The access must be without the knowledge of either the sender or the intended recipient of the communication for it to fall within the parameters of the TIA Act.
- 2.7 Telecommunications data is not defined in the TIA Act. Section 172 excludes the content or substance of a call from being 'telecommunications data'. Accordingly, telecommunications data could include the date, time, subscriber and location of a call.

- 2.8 There are exceptions to these prohibitions, the most relevant of which relate to the interception of communications, access to stored communications under a warrant or the disclosure of telecommunications data under an authorisation.
- 2.9 The TIA Act regulates the issue and revocation of warrants and authorisations, the scope of the authority conferred by warrants or authorisations, the execution of warrants and the use of information obtained under warrants or authorisations.

# **Telecommunications interception warrants**

Offences for which telecommunications interception warrants may be obtained

- 2.10 Part 2-5 of the TIA Act provides for the issue of telecommunications interception warrants to interception agencies. This Part of the TIA Act provides that a telecommunications interception warrant can be sought to assist with the investigation of a serious offence.
- 2.11 A serious offence is exhaustively defined in section 5D which includes the following types of offences:
  - murder, kidnapping and equivalent offences
  - an offence against Division 307 of the *Criminal Code*, being serious drug import and export offences
  - an offence constituted by conduct involving an act or acts of terrorism
  - an offence against Subdivision A of Divisions 72, 101, 102 and 103 of the Criminal Code
  - offences in relation to which the Australian Crime Commission (ACC) is conducting a special investigation within the meaning of the Australian Crime Commission Act 2002<sup>1</sup>
  - offences relating to child pornography
  - specified offences involving particular conduct such as loss of a person's life, serious personal injury or trafficking in prescribed substances where the offence is punishable by at least seven years imprisonment
  - specified offences involving planning and organisation which involve conduct such as theft, handling of stolen goods, bribery or corruption where the offence is punishable by at least seven years imprisonment
  - money laundering offences
  - offences relating to people smuggling with exploitation, slavery, sexual servitude and deceptive recruiting
  - serious drug offences
  - computer-related offences, and
  - ancillary offences, such as aiding, abetting and conspiring to commit serious offences.

3

<sup>&</sup>lt;sup>1</sup> This section applies only to warrants sought by the ACC.

2.12 It is a general requirement that the offence be punishable by imprisonment for life or for a maximum period of at least seven years. However, there are exceptions to this rule. These exceptions generally apply to offences that by their nature require interception as an investigative tool or where the conduct is serious enough to warrant the use of interception regardless of the offence threshold. Examples of these types of offences include child pornography and cybercrime offences.

Applying for telecommunications interception warrants

- 2.13 Applications for telecommunications interception warrants may only be made by an interception agency. An interception agency is the ACC, the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Federal Police (AFP) or an 'eligible authority' of a State or the Northern Territory which is the subject of a declaration under section 34 of the TIA Act.
- 2.14 In effect, a section 34 declaration, which is made by the Attorney-General at the request of the Premier of a State or the Chief Minister of the Northern Territory, grants interception agency status to an eligible authority. This means that the agency can then apply for telecommunications interception warrants to assist in the investigation of a serious offence. An eligible authority which is *not* the subject of a declaration is *not* able to apply for such a warrant but is able to receive intercepted information for permitted purposes from an interception agency.
- 2.15 The TIA Act defines eligible authorities to be the police force of each of the States and of the Northern Territory. During the reporting period, 'eligible authority' also included:
  - in New South Wales the NSW Crime Commission, the Independent Commission Against Corruption (ICAC), the Inspector of the ICAC, the Police Integrity Commission (PIC) and the Inspector of the PIC
  - in Victoria the Office of Police Integrity (OPI)
  - in Queensland the Crime and Misconduct Commission (CMC)
  - in Western Australia the Corruption and Crime Commission of Western Australia (CCC WA) and the Parliamentary Inspector of the CCC WA.
- 2.16 During the reporting period, the following eligible authorities were the subject of a declaration pursuant to section 34 of the TIA Act and therefore were able to apply for telecommunications interception warrants:

AGENCY	DATE OF SECTION 34 DECLARATION
Victoria Police	28 October 1988
New South Wales Crime Commission	30 January 1989
New South Wales Police Force	30 January 1989
Independent Commission Against Corruption	6 June 1990
South Australia Police	10 July 1991
Western Australia Police	15 July 1997
Police Integrity Commission	14 July 1998
Corruption and Crime Commission of Western Australia	24 March 2004
Tasmania Police	5 February 2005
Northern Territory Police	25 October 2006
Office of Police Integrity Victoria	18 December 2006

#### Eligible Judges and nominated AAT members

- 2.17 Part 2-5 of the TIA Act provides that an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member may issue a telecommunications interception warrant on application by an agency.
- 2.18 An 'eligible Judge' refers to a Judge of a court created by the Parliament who has consented in writing and been declared by the Attorney-General to be an eligible Judge. In the reporting period, eligible Judges were members of the Federal Court of Australia, the Family Court of Australia and the Federal Magistrates Court.
- 2.19 A 'nominated AAT member' refers to a Deputy President, senior member or a member of the AAT who has been nominated by the Attorney-General to issue warrants. In the case of part-time senior members and members of the AAT, the member must have been enrolled as a legal practitioner of the High Court, the Federal Court or the Supreme Court of a State or Territory for no less than five years to be eligible for nomination to issue warrants.

## Form of applications

- 2.20 The TIA Act requires that an application for a telecommunications interception warrant be in writing and be accompanied by a supporting affidavit. However, in urgent circumstances, applications may be made by telephone. In either case, the warrant takes effect only when completed and signed by the Judge or nominated AAT member.
- 2.21 The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.
- 2.22 The TIA Act requires that an application contain the name of the agency and person making the application. The supporting affidavit must contain the facts on

which the application is based, the period for which the warrant is sought to be in force and information regarding any previous warrants obtained in relation to the same matter.

Matters to be considered by an issuing authority

- 2.23 There are a number of matters that an issuing authority must consider before issuing a telecommunications interception warrant, including the availability of alternative methods of investigation, the gravity of the conduct being investigated and the degree of interference with the privacy of any person.
- 2.24 Where an application for a warrant includes a request that the warrant authorise entry onto premises, section 48 requires that the Judge or nominated AAT member also be satisfied that it would be impracticable or inappropriate to intercept communications by less intrusive means.

# Safeguards and controls contained in the Act

2.25 The TIA Act contains a number of safeguards and controls in relation to interception as well as a number of reporting requirements. These requirements are designed to ensure that appropriate levels of accountability exist. The most significant of these requirements are outlined below.

#### **Inspections**

- 2.26 The ACC, ACLEI and the AFP are required to maintain records relating to interceptions and the use and dissemination of intercepted information. These records must be inspected by the Commonwealth Ombudsman on a regular basis.
- 2.27 The TIA Act requires the Commonwealth Ombudsman to report to the Attorney-General regarding these inspections and to include in his or her report a summary of any deficiencies identified and any remedial action taken.
- 2.28 Parallel requirements are imposed by State and Territory legislation on State and Territory interception agencies. The imposition of parallel record keeping and reporting requirements with the Commonwealth legislation is a precondition to the State or Territory eligible authority being granted interception agency status. If the Attorney-General is satisfied that the State or Territory legislation is no longer parallel to the Commonwealth legislation, he or she may revoke their interception agency status.
- 2.29 While the Commonwealth Ombudsman is responsible for inspecting the records of the ACC, ACLEI and the AFP, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies.<sup>2</sup> The reports of the inspections of the declared State and Territory agencies are given to the responsible State or Territory Minister who must provide a copy to the Commonwealth Attorney-General.

6

<sup>&</sup>lt;sup>2</sup> Instead of the State Ombudsman, inspection of the South Australian Police is undertaken by the Police Complaints Authority (South Australia), while inspections of the Victoria Police and the Office of Police Integrity are undertaken by the Special Investigations Monitor (Victoria).

- 2.30 Accordingly, all law enforcement agencies capable of applying for telecommunications interception warrants operate under equivalent supervisory and accountability provisions. This means that the TIA Act imposes a national scheme in relation to telecommunications interception and ensures that the Attorney-General is kept informed of the agencies' activities by means of reports from the agencies and the Ombudsman.
- 2.31 The reports of the inspecting authorities to date indicate a high level of compliance with the relevant statutory requirements.

#### Destruction of records

2.32 Section 79 of the TIA Act provides that agencies must destroy restricted records, being original records gained from interception, once the agency is satisfied that the records are not likely to be needed for a permitted purpose and they have been informed that the Attorney-General has inspected the relevant entry in the General Register.

General Register of telecommunications interception warrants

- 2.33 Section 81A of the TIA Act provides that the Secretary of the Attorney-General's Department must maintain a General Register which includes particulars of all telecommunications interception warrants. The particulars required to be recorded in the General Register are:
  - the date of issue and period for which the warrant was to be in force
  - the agency to which the warrant was issued and the Judge or nominated AAT member who issued the warrant
  - the telecommunications service to which the warrant relates
  - the name of the person specified in the warrant as the person using or likely to use the telecommunications service
  - each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied on the application for the warrant, and
  - for named person warrants, the name of the person to whom the warrant relates and each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred.
- 2.34 Section 81B of the TIA Act provides that the Secretary of the Attorney-General's Department must deliver the General Register to the Attorney-General for inspection every three months. Interception agencies are notified once the Attorney-General has inspected the General Register to enable the destruction of restricted records.

Special Register of telecommunications interception warrants

2.35 Section 81C of the TIA Act provides that the Secretary of the Attorney-General's Department must maintain a Special Register recording the details of telecommunications interception warrants which did not lead, directly or indirectly, to a prosecution within three months of the expiry of the warrant. The Secretary must

deliver the Special Register to the Attorney-General for inspection every three months together with the General Register.

Attorney-General to be given copies of telecommunications interception warrants and revocations and reports on outcomes

- 2.36 Section 59A of the TIA Act provides that the chief officer of each interception agency must give to the Attorney-General:
  - a copy of each telecommunications interception warrant issued to that agency,
  - each instrument revoking such a warrant, and
  - within three months of a warrant ceasing to be in force, a written report about the use made of information obtained by interception under the warrant.

#### Reports by carrier

2.37 Section 97 of the TIA Act provides that the Managing Director of a carrier who enables interception to occur under a warrant must report to the Attorney-General within three months of the warrant ceasing to be in force. The report must include details of the acts done by employees of the carrier to effect interception under the warrant and to discontinue interception when the warrant expires or is revoked.

Annual Report tabled by Attorney-General

2.38 Sections 99 and 104 of the TIA Act provide that the Attorney-General must prepare and table in Parliament each year a report setting out the information specified in Part 2-8 of the TIA Act. Chapter 4 of this report presents the required information.

#### Stored communications warrants

#### Relevant offences

- 2.39 Part 3-3 of the TIA Act enables an issuing authority to issue a stored communications warrant to an enforcement agency. The definition of enforcement agency includes listed criminal law enforcement agencies as well as agencies responsible for administering a law imposing a pecuniary penalty or relating to the protection of the public revenue.
- 2.40 A stored communications warrant authorises covert access to stored communications in connection with the investigation of a serious contravention. A 'serious contravention' is defined by the TIA Act as a serious offence (being an offence for which a telecommunications interception warrant may be obtained), an offence punishable by a maximum period of imprisonment of at least three years imprisonment or an offence with an equivalent monetary penalty.

#### Issuing authorities

2.41 Part 3-3 of the TIA Act provides that an enforcement agency may apply to an issuing authority for a stored communications warrant to access stored communications.

Section 6DB of the TIA Act provides that the Attorney-General may appoint issuing authorities to issue stored communications warrants.

- 2.42 Paragraph 6DB(1)(a) defines an issuing authority as a Judge of a court created by the Parliament, a Federal Magistrate or a State magistrate, who has consented in writing to being appointed by the Attorney-General and who has been so appointed by the Attorney-General. In the reporting period, issuing authorities included members of the Federal Court of Australia, the Family Court of Australia, the Federal Magistrates Court and State magistrates.
- 2.43 Paragraph 6DB(1)(b) further defines an issuing authority as including a person who is a Deputy President, senior member or a member of the AAT and has been appointed as an issuing authority by the Attorney-General. The member must have been enrolled as a legal practitioner of a Federal court or of the Supreme Court of a State or a Territory for at least five years before they are eligible to be appointed as an issuing authority.

#### Form of application

- 2.44 In the normal course of events, the TIA Act requires that an application for a stored communications warrant be in writing and accompanied by a supporting affidavit. However, in urgent circumstances, applications may be made by telephone. In either case, the warrant takes effect only when completed and signed by the issuing authority.
- 2.45 The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.
- 2.46 The TIA Act requires that an application contain the name of the agency and person making the application. The supporting affidavit must contain the facts on which the application is based.

# Safeguards and controls relating to the stored communications regime

2.47 The TIA Act contains a number of safeguards and controls in relation to stored communications warrants as well as a number of reporting requirements. These requirements are designed to ensure that appropriate levels of accountability exist.

#### Recordkeeping and inspections

- 2.48 Section 151 of the TIA Act provides that the chief officer of an enforcement agency must cause to be kept:
  - each stored communications warrant issued
  - each instrument of revocation

- copies of authorisations which authorise persons to receive stored communications and
- particulars of the destruction of information.
- 2.49 The TIA Act provides that the Commonwealth Ombudsman may conduct regular inspections of those records and must report to the Attorney-General on the results of those inspections.

#### Destruction of records

2.50 Section 150 of the TIA Act provides that if the chief officer of an agency is satisfied that the information or record obtained by accessing a stored communication is not likely to be required for the purposes for which it can be used under the TIA Act, that information or record must be destroyed.

Annual report tabled by Attorney-General

2.51 Sections 161 and 164 of the TIA Act provide that the Attorney-General must prepare and table in Parliament each year a report setting out the information specified in Part 3-6 of the TIA Act. Chapter 5 of this report presents the required information.

#### Telecommunications data authorisations

Telecommunications data

- 2.53 Part 4-1 of the TIA Act enables enforcement agencies to authorise the disclosure of telecommunications data.
- 2.54 Section 172 prohibits the disclosure of any content or substance of a communication. While telecommunications data is not defined in the TIA Act, it is taken to mean anything that is not the content or substance of a communication. It can include:
  - 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.
- 2.55 Sections 174 180 allow for the authorisation of the release of telecommunications data under certain circumstances.

#### Historical and prospective data

- 2.56 The disclosure of historical or existing data may be authorised when it is considered reasonably necessary, by an authorising officer, that it is reasonably necessary for the enforcement of a criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue. Historical or existing data is data which came into existence before the time the person from whom the disclosure is sought received notification of the authorisation. It does not include information which came into existence after notification was received but before the authorisation was executed.
- 2.57 The disclosure of prospective data may be authorised by an authorised officer of a criminal law-enforcement agency if it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years. An authorisation for the disclosure of prospective data comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation, and must end at a specified time no longer than 45 days from the day the authorisation is made, unless it is revoked earlier.

#### Forms of application

- 2.58 Section 183 of the TIA Act provides that an authorisation under Division 3 or 4 of Part 4-1, a notification, revocation or notification of revocation must be in written or electronic form and must comply with any requirements put in place by the Communications Access Co-ordinator (CAC). The requirements for an authorisation include:
  - the identity of the agency
  - the basis on which the agency is an enforcement agency or criminal lawenforcement agency
  - the identity of the authorised officer who is making the authorisation
  - the basis on which the authorised officer is an authorised officer
  - the relevant provisions of the TIA Act
  - the name of the person from whom the disclosure is sought
  - details of the information or documents to be disclosed
  - for access to existing information or documents, a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or the protection of the public revenue
  - for access to prospective information or documents, a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years

- for access to prospective information or documents, a statement that the
  authorised officer has had regard to how much the privacy of any person or
  persons would be likely to be interfered with and that the authorised officer is
  satisfied that the impact on privacy is outweighed by the seriousness of the
  conduct being investigated
- the date on which the authorisation is made, and for access to prospective information or documents, the date on which the authorisation is to end.
- 2.59 Section 184 requires a relevant staff member from an agency making an authorisation to notify the person from whom the disclosure is sought.

# Safeguards and controls relating to the telecommunications data regime

Recordkeeping and inspections

2.60 Section 185 of the TIA Act provides that the head of an enforcement agency must retain an authorisation made for three years beginning on the day the authorisation is made.

Annual report tabled by Attorney-General

2.61 Section 186 of the TIA Act provides that the agencies must provide the Attorney-General statistics about the number of authorisations made under sections 178,179 and 180. Section 186 also provides that the Attorney-General must prepare and table in Parliament each year a report setting out this information, which is presented in Chapter 6.

#### CHAPTER 3—DEVELOPMENTS IN THE REPORTING PERIOD

3.1 This chapter sets out the principal legislative developments and judicial decisions affecting the TIA Act during the reporting period 1 July 2007 to 30 June 2008. It also outlines comments made by intercepting agencies in relation to the value and importance of interception under telecommunications interception warrants.

# Recent legislative and policy developments

The Telecommunications (Interception and Access) Amendment Act 2007

- 3.2 The *Telecommunications (Interception and Access) Amendment Act 2007* (the 2007 Amendment Act) was introduced to Parliament on 14 June 2007 and became law on 28 September 2007. The majority of amendments commenced operation on 1 November 2007.
- 3.3 The main purpose of the 2007 Amendment Act was to implement two of the central recommendations of the Blunn Report. The first of these recommendations was to make the TIA Act the single piece of legislation regulating access by law enforcement and security agencies to telecommunications information. The *Telecommunications Act 1997* contained some provisions relating to access prior to the commencement of the 2007 Amendment Act. The second recommendation was to allow access to the content of communications for the protection of data systems and the development or testing of new technologies.
- 3.4 Chapter 4 of the TIA Act was introduced by the 2007 Amendment Act. It creates a regime for enforcement agencies to authorise the disclosure of telecommunications data, being information about communications or subscribers to communications services, but not including the content of communications.
- 3.5 This regime, which replaces provisions previously in the Telecommunications Act, permits occupiers of authorised management positions of enforcement agencies to authorise the disclosure of telecommunications data. Such authorisations can be made where it is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue.
- 3.6 The regime distinguishes between the disclosure of information that is already in existence when the authorisation is made and the disclosure of information that comes into existence while the authorisation is in force. The latter type of disclosure may only be authorised by criminal law-enforcement agencies, to investigate offences punishable by a maximum term of imprisonment of at least three years and only after the privacy impact on any persons of such a disclosure has been considered.

- 3.7 The *Telecommunications (Interception and Access) Amendment Act 2008* (the 2008 Amendment Act) received royal assent on 26 May 2008. Certain amendments commenced on 27 May 2008, while others commenced on 1 July 2008.
- 3.8 Previously the TIA Act required that interception agencies provide a copy of each warrant or instrument revoking a warrant to the responsible State Minister, who in turn was required to provide a copy to the Commonwealth Attorney-General. This resulted in duplication as agencies are also required to provide copies of warrants and revocations to the Attorney-General's Department directly. The 2008 Amendment Act removed the mandatory requirements for state interception agencies to provide copies of warrants and instrument of revocation to the responsible State Minister.
- 3.9 The 2008 Amendment Act also removed the requirement for the Attorney-General's Department to be informed of an intention to revoke a warrant. This requirement is unnecessary as the Attorney-General's Department plays no role in the actioning of warrants. These two amendments came into effect on 27 May 2008.
- 3.10 The 2008 Amendment Act extended the exemption provided for in section 5F(2) of the TIA Act that allows network administrators to access and copy any communication from the network boundary for network protection purposes by 18 months (until 12 December 2009). This exemption is essential for the protection of networks from attacks including viruses and Trojans. The extension was required to enable consultation and development of a solution which enables protection of networks and privacy of users without causing a technical breach of the TIA Act.
- 3.11 The 2008 Amendment Act clarified that section 46A of the TIA Act permits an application for a device-based named person warrant to identify one or more telecommunications devices on the face of the warrant.
- 3.12 Paragraph 100(1)(ec) of the TIA Act was amended requiring each interception agency to provide the total number of telecommunications services intercepted under service-based and device-based named person warrants and the total number of telecommunications devices by means of which communications were intercepted under device-based named person warrants.
- 3.13 The amendments to section 46A and paragraph 100(1)(ec) of the TIA Act did not take effect until 1 July 2008. As these amendments commenced outside of the reporting period, more detail on these amendments will be included in the next annual report.

#### Other amendments

3.14 The *Telecommunications* (*Interception and Access*) *Amendment Regulations* 2008 were registered on the Federal Register of Legislative Instruments on 23 June 2008. The regulations prescribe that from 25 June 2008, the Australian Customs Service (Customs) is a criminal law-enforcement agency. This means that

Customs may authorise the release of prospective telecommunications data in accordance with the TIA Act.

#### **Judicial decisions**

3.15 No major judicial decisions in relation to the TIA Act were handed down during the reporting period.

# **Previous Annual Report**

3.16 The Annual Report for the year ending 30 June 2007 was tabled in the Senate and in the House of Representatives on 13 February 2008.

# **Effectiveness of interception**

3.17 There remains a consistent view among agencies that telecommunications interception continues to be an extremely valuable investigative tool. Agencies have again noted that evidence gathered through the execution of a telecommunications interception warrant can lead to the successful conclusion of an investigation in circumstances where alternative evidence is uncorroborated, unavailable or insubstantial.

# CHAPTER 4—TELECOMMUNICATIONS INTERCEPTION INFORMATION REQUIRED UNDER THE ACT

### The information required

- 4.1 Part 2-8 of the TIA Act provides that this report must include the following information:
  - the number of applications for warrants made and the number of warrants issued (section 100)
  - the duration for which warrants were specified to be in force when issued and the period for which the warrants were actually in force (section 101)
  - the number of arrests, prosecutions and convictions during the reporting period based on intercepted information (section 102)
  - the number of times an agency intercepted a communication without a warrant in an emergency situation such as a siege, kidnapping or extortion (section 102A)
  - the total expenditure and the average expenditure per warrant incurred by relevant agencies in connection with the execution of warrants during the reporting period (paragraph 103(a))
  - information about the availability of Judges to issue warrants and the extent to which nominated AAT members have been used for that purpose (paragraph 103(ab))
  - the number of interceptions carried out on behalf of other agencies (paragraph 103(ac))
  - the number and type of emergency service facilities that were declared by the Attorney-General for each State and Territory during the reporting period (paragraph 103(ad))
  - a summary of the information required under subsection 84(1A) to be included in the report by the Ombudsman (paragraph 103(ae)), and
  - additional matters (if any) as have been prescribed under the TIA Act (paragraph 103(b)). No additional matters have been prescribed for the purpose of this paragraph.
- 4.2 The TIA Act provides that the information must be set out in relation to each interception agency and, where relevant, each eligible authority. In addition, the information must be combined for all agencies to indicate the overall use and effectiveness of telecommunications interception under the TIA Act.

# Which agencies may seek telecommunications interception warrants

- 4.3 During the reporting period, the following agencies were entitled to apply for telecommunications interception warrants for law enforcement purposes:
  - Australian Commission for Law Enforcement Integrity
  - Australian Crime Commission
  - Australian Federal Police
  - Corruption and Crime Commission (Western Australia)
  - Independent Commission Against Corruption (New South Wales)
  - New South Wales Crime Commission
  - New South Wales Police Force
  - Northern Territory Police
  - Office of Police Integrity (Victoria)
  - Police Integrity Commission (New South Wales)
  - South Australia Police
  - Tasmania Police
  - Victoria Police, and
  - Western Australia Police.

## **Applications for telecommunications interception warrants**

- 4.4 Paragraphs 100(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for telecommunications interception warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and for all agencies in total.
- 4.5 The Australian Commission for Law Enforcement Integrity was the only interception agency that did not apply for a warrant during the reporting period.
- 4.6 During the reporting period, 3246 warrants were issued to law enforcement agencies under Part 2-5 of the TIA Act. The total number of warrants issued decreased by approximately 1% on the total number of warrants issued during the previous reporting period. The Office of Police Integrity and the Police Integrity Commission had substantial increases in the number of warrants issued, due to increases in their operational requirements. Other agencies reported similar numbers as in the previous reporting period. This information is presented in Table 1.

Table 1 – Applications for telecommunications interception warrants

Made	
AUSTRALIAN CRIME COMMISSION   Refused/withdrawn   0   0   0   1   1   1   1   1   1   1	/08
Issued   202   211	79
AUSTRALIAN FEDERAL POLICE  Refused/withdrawn   Saued   S12   S34   S5   S54   S5   S54   S5   S54   S5   S5	0
AUSTRALIAN FEDERAL POLICE	79
Issued   512   534   55	33
Made	3
CORRUPTION AND CRIME COMMISSION OF WESTERN AUSTRALIA         Refused/withdrawn Issued         0         0         0         122         1           INDEPENDENT COMMISSION AGAINST CORRUPTION         Made         17         33         3           NEW SOUTH WALES CRIME COMMISSION         Made         835         790         6           NEW SOUTH WALES CRIME COMMISSION         Refused/withdrawn 2         2         2           Issued         833         788         6           NEW SOUTH WALES POLICE         Refused/withdrawn 0         1         1           Issued         543         866         8           NORTHERN TERRITORY POLICE         Refused/withdrawn 0         0         27         3           Made         0         27         3         3           OFFICE OF POLICE INTEGRITY         Made         0         14         3           Refused/withdrawn 1         0         0         14         3           POLICE INTEGRITY COMMISSION 2         Refused/withdrawn 1         0         0         1           Issued         51         40         0         0         0           BOUTH AUSTRALIA POLICE         Refused/withdrawn 1         0         0         0         0 </th <td>30</td>	30
Sed	02
AUSTRALIA	0
NEW SOUTH WALES   CRIME COMMISSION   Refused/withdrawn   Sued   Sued	02
NEW SOUTH WALES CRIME COMMISSION   Refused/withdrawn   Susued   Susued	33
NEW SOUTH WALES   CRIME COMMISSION   Issued   17   33   33   33   33   33   33   33	0
NEW SOUTH WALES   Refused/withdrawn   2   2   2   2   2   2   2   2   3   3	33
NEW SOUTH WALES CRIME COMMISSION         Refused/withdrawn Issued         2         2         2         2         333         788         6           NEW SOUTH WALES POLICE         Refused/withdrawn Issued         0         1         2         2         2         2         2         2         2         4         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         8         6         8         6         8         8         6         8         8         6         8         6<	72
NEW SOUTH WALES POLICE   Refused/withdrawn   0	0
NEW SOUTH WALES POLICE         Made         543         866         8           Refused/withdrawn         0         1         1           Issued         543         865         8           Made         0         27         3           Refused/withdrawn         0         0         27         3           Made         0         14         3           Refused/withdrawn         0         0         14         3           POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0         6           Issued         51         40         95         1           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0         0	72
NEW SOUTH WALES POLICE         Refused/withdrawn         0         1           Issued         543         865         8           NORTHERN TERRITORY POLICE         Made         0         27         3           Refused/withdrawn         0         0         27         3           OFFICE OF POLICE INTEGRITY         Made         0         14         3           Refused/withdrawn         0         0         14         3           Made         52         40         9           POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0         0           Issued         51         40         0           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0	14
Issued   543   865   88	3
NORTHERN TERRITORY POLICE         Made Refused/withdrawn   0   0   0   0   0   0   0   0   0	11
NORTHERN TERRITORY POLICE         Refused/withdrawn         0         0           Issued         0         27         3           OFFICE OF POLICE INTEGRITY         Made         0         14           Refused/withdrawn         0         0         14           Issued         0         14         3           POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0           Issued         51         40         0           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0	39
Issued   0   27   3   3   3   3   3   3   3   3   3	2
OFFICE OF POLICE INTEGRITY         Made         0         14         1           Refused/withdrawn         0         0         14         1           Issued         0         14         1           POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0           Issued         51         40         0           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0	- 37
OFFICE OF POLICE INTEGRITY         Refused/withdrawn         0         0           Issued         0         14         3           Made         52         40         3           POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0           Issued         51         40         3           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0	78
Issued   0	0
POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0           Issued         51         40         9           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0	78
POLICE INTEGRITY COMMISSION         Refused/withdrawn         1         0           Issued         51         40         9           Made         140         95         1           SOUTH AUSTRALIA POLICE         Refused/withdrawn         0         0	91
Issued   51   40   0   0   0   0   0   0   0   0	0
SOUTH AUSTRALIA POLICE Refused/withdrawn 0 0	91
SOUTH AUSTRALIA POLICE Refused/withdrawn 0 0	24
	0
	24
Made 1 13	 17
TASMANIA POLICE	0
	17
	73
	0
	73
	99
	0
	99
	<u>//</u> 254
	8
	246

Telephone applications for telecommunications interception warrants

- 4.7 Section 40 of the TIA Act provides that an application for a telecommunications interception warrant may be made by telephone in urgent circumstances. Paragraphs 100(1)(b) and (2)(b) of the TIA Act provide that the report must set out the number of telephone applications for warrants, the number of warrants issued to each agency and the total number of warrants issued on the basis of telephone applications. The information required under paragraphs 100(1)(b) and (2)(b) is presented in Table 2.
- 4.8 The total number of telephone applications made in the reporting period is consistent with previous reporting periods.

Table 2—Telephone applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	TELEPHONE APPLICATIONS FOR WARRANTS		
		05/06	06/07	07/08
	Made	1	2	2
AUSTRALIAN FEDERAL POLICE	Refused/withdrawn	0	0	0
	Issued	1	2	2
	Made	0	2	0
NEW SOUTH WALES CRIME	Refused/withdrawn	0	0	0
COMMISSION	Issued	0	2	0
	Made	11	29	22
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0	0
	Issued	11	29	22
	Made	1	0	0
SOUTH AUSTRALIA POLICE	Refused/withdrawn	0	0	0
	Issued	1	0	0
	Made	22	21	27
VICTORIA POLICE	Refused/withdrawn	0	0	0
	Issued	22	21	27
	Made	5	3	0
WESTERN AUSTRALIA POLICE	Refused/withdrawn	0	0	0
	Issued	5	3	0
TASMANIA POLICE	Made	0	0	6
	Refused/withdrawn	0	0	0
	Issued	0	0	6
	Made	40	57	57
TOTAL [paragraph 100(2)(b)]	Refused/withdrawn	0	0	0
	Issued	40	57	57

Renewal applications for telecommunications interception warrants

4.9 Agencies may apply for the renewal of telecommunications interception warrants that are still in force. Paragraphs 100(1)(c) and (2)(c) of the TIA Act provide that the report must set out the number of renewal applications made in relation to each agency and in total for all agencies. This information is presented in Table 3.

4.10 The number of renewal applications increased by 1.28% in comparison with the number of renewal applications made in the previous reporting period.

Table 3— Renewal applications for telecommunications interception warrants

AGENCY	RELEVANT	RENEWAL APPLICATIONS			
STATISTICS		05/06	06/07	07/08	
	Made	49	56	46	
AUSTRALIAN CRIME	Refused/withdrawn	0	0	0	
COMMISSION	Issued	49	56	46	
	Made	101	74	103	
AUSTRALIAN FEDERAL POLICE	Refused/withdrawn	0	0	0	
	Issued	101	74	103	
	Made	12	70	50	
CORRUPTION AND CRIME	Refused/withdrawn	0	0	0	
COMMISSION OF WESTERN AUSTRALIA	Issued	12	70	50	
	Made	4	5	6	
INDEPENDENT COMMISSION	Refused/withdrawn	0	0	0	
AGAINST CORRUPTION	Issued	4	5	6	
	Made	137	128	111	
NEW SOUTH WALES	Refused/withdrawn	0	0	0	
CRIME COMMISSION	Issued	137	128	111	
	Made	84	102	116	
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0	0	
	Issued	84	102	116	
NORTHERN TERRITORY POLICE	Made	0	3	0	
	Refused/withdrawn	0	0	0	
	Issued	0	3	0	
	Made	0	2	23	
OFFICE OF POLICE INTEGRITY	Refused/withdrawn	0	0	0	
	Issued	0	2	23	
	Made	13	22	10	
POLICE INTEGRITY	Refused/withdrawn	0	0	0	
COMMISSION	Issued	13	22	10	
	Made	12	0	1	
SOUTH AUSTRALIA POLICE	Refused/withdrawn	0	0	0	
	Issued	12	0	1	
	Made	0	1	0	
TASMANIA POLICE	Refused/withdrawn	0	0	0	
	Issued	0	1	0	
VICTORIA POLICE	Made	37	56	56	
	Refused/withdrawn	0	0	0	
	Issued	37	56	56	
	Made	13	25	29	
WESTERN AUSTRALIA POLICE	Refused/withdrawn	0	0	0	
	Issued	13	25	29	
	Made	462	544	551	
TOTAL [paragraph 100(2)(c)]	Refused/withdrawn	0	0	0	
	Issued	462	544	551	

Applications for telecommunications interception warrants authorising entry onto premises

- 4.11 Subsection 48(1) of the TIA Act provides that an application for a telecommunications interception warrant may include a request that the warrant authorise entry onto premises. Paragraphs 100(1)(d) and (2)(d) of the TIA Act provide that the report must set out the number of applications for warrants that include requests for authorisation of entry onto premises. This information is set out in Table 4.
- 4.12 Agencies sought and were issued with a very small number of such warrants, which is consistent with the last three reporting periods.

Table 4—Applications for telecommunications interception warrants authorising entry on premises

AGENCY	RELEVANT STATISTICS	WARRANTS AUTHORISING ENTRY ON PREMISES		-
		05/06	06/07	07/08
	Made	1	3	7
AUSTRALIAN FEDERAL POLICE	Refused/withdrawn	0	0	0
	Issued	1	3	7
	Made	0	1	0
NEW SOUTH WALES CRIME	Refused/withdrawn	0	0	0
COMMISSION	Issued	0	1	0
	Made	1	0	0
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0	0
	Issued	1	0	0
POLICE INTEGRITY	Made	0	3	0
COMMISSION	Refused/withdrawn	0	0	0
	Issued	0	3	0
	Made	0	3	0
VICTORIA POLICE	Refused/withdrawn	0	0	0
	Issued	0	3	0
	Made	3	1	0
INDEPENDENT COMMISSION AGAINST CORRUPTION	Refused/withdrawn	0	0	0
	Issued	3	1	0
	Made	0	0	1
CORRUPTION AND CRIME COMMISSION OF WESTERN	Refused/withdrawn	0	0	0
AUSTRALIA	Issued	0	0	1
	Made	5	11	8
TOTAL [paragraph 100(2)(d)]	Refused/withdrawn	0	0	0
	Issued	5	11	8

Telecommunications interception warrants issued with specific conditions or restrictions

- 4.13 Subsection 49(1) of the TIA Act provides that a telecommunications interception warrant may specify conditions and restrictions regarding the interception of communications under that warrant. Paragraphs 100(1)(e) and (2)(e) of the TIA Act provide that the number of warrants issued with conditions and restrictions must be set out in the report. This information is set out in Table 5.
- 4.14 There was a decrease of 48.3% in the number of warrants issued with conditions or restrictions when compared to the previous reporting period. The ability to impose conditions or restrictions is at the discretion of the issuing authority.

Table 5—Telecommunications interception warrants issued with specific conditions or restrictions

AGENCY	WARRANTS ISSUED WITH CONDITIONS OR RESTRICTIONS			
	05/06	06/07	07/08	
AUSTRALIAN FEDERAL POLICE	1	11	1	
AUSTRALIAN CRIME COMMISSION	1	1	2	
INDEPENDENT COMMISSION AGAINST CORRUPTION	0	1	0	
NEW SOUTH WALES CRIME COMMISSION	47	61	26	
NEW SOUTH WALES POLICE	10	12	13	
POLICE INTEGRITY COMMISSION	0	1	3	
WESTERN AUSTRALIA POLICE	0	0	0	
TOTAL [paragraph 100(2)(e)]	59	87	45	

#### Named person warrants

- 4.15 Paragraph 100(1)(ea) of the TIA Act provides that the report include the same statistics outlined above in relation to named person warrants. This means that the following statistics must be provided:
  - the number of named person warrants applied for, refused and issued
  - the number of telephone applications for named person warrants, made, refused and issued
  - the number of renewal applications for named person warrants, made, refused and issued
  - the number of named person warrants which authorise entry onto premises, and

- the number of named person warrants issued with conditions or restrictions attached.
- 4.16 Paragraph 100(2)(ea) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 6 to 9 set out the information supplied by intercepting agencies regarding named person warrants. The number of named person warrants issued to agencies increased by 25.2% from the number of warrants issued in the previous reporting period. The number of renewal applications for named person warrants increased by 71% from the previous reporting period. No named person warrants authorised entry onto premises during the reporting period.

#### Interpretative note

4.17 The increase in named person warrants is attributable to operational priorities and the increase in the easy availability for multiple services for individuals. Such services are easily obtained. For example, an individual is able to obtain any number of pre-paid mobile phones in attempts to avoid detection. The named person warrant regime provides an efficient and effective method for interception agencies to be able to intercept communications by an individual as new services become known.

Table 6—Original applications for named person warrants

AGENCY	RELEVANT APPLICATIONS FOR NAMED PERSON W			ON WARRANTS
	STATISTICS	05/06	06/07	07/08
	Made	81	84	131
AUSTRALIAN FEDERAL	Refused/withdrawn	0	0	1
POLICE	Issued	81	84	130
	Made	118	115	99
AUSTRALIAN CRIME	Refused/withdrawn	0	0	0
COMMISSION	Issued	118	115	99
	Made	12	19	41
NEW SOUTH WALES	Refused/withdrawn	0	0	1
POLICE	Issued	12	19	40
	Made	41	33	57
NEW SOUTH WALES CRIME COMMISSION	Refused/withdrawn	0	0	0
GRANIE GOMMINGOTOR	Issued	41	33	57
DOLLOS 15:7505::	Made	0	0	0
POLICE INTEGRITY COMMISSION	Refused/withdrawn	0	0	0
	Issued	0	0	0
INDEDENIE	Made	0	2	0
INDEPENDENT COMMISSION AGAINST	Refused/withdrawn	0	0	0
CORRUPTION	Issued	0	2	0
	Made	9	8	10
SOUTH AUSTRALIA	Refused/withdrawn	0	0	0
POLICE	Issued	9	8	10
	Made	67	82	90
VICTORIA POLICE	Refused/withdrawn	0	0	0
	Issued	67	82	90
	Made	31	27	30
WESTERN AUSTRALIAN	Refused/withdrawn	0	0	0
POLICE	Issued	31	27	30
CORRUPTION AND	Made	4	0	3
CRIME COMMISSION OF WESTERN AUSTRALIA	Refused/withdrawn	0	0	0
WESTERN AUSTRALIA	Issued	4	0	3
	Made	0	2	0
TASMANIA POLICE	Refused/withdrawn	0	0	0
	Issued	0	2	0
NORTHERN TERRITORY	Made	0	5	7
POLICE	Refused/withdrawn	0	0	0
	Issued	0	5	7
	Made	0	3	10
OFFICE OF POLICE	Refused/withdrawn	0	0	0
INTEGRITY	Issued	0	3	10
	Made	363	380	478
TOTAL [paragraph	Refused/withdrawn	0	0	2
100(ea)]	Issued	363	380	476

Table 7—Telephone applications for named person warrants

AGENCY	RELEVANT	APPLICATIONS FOR WARRANTS			
AGENCY	STATISTICS	05/06	06/07	07/08	
	Made	0	1	0	
TASMANIA POLICE	Refused/withdrawn	0	0	0	
	Issued	0	1	0	
VICTORIA POLICE	Made	1	5	5	
	Refused/withdrawn	0	0	0	
	Issued	1	5	5	
TOTAL [paragraph 100(ed)]	Made	1	6	5	
	Refused/withdrawn	0	0	0	
100(ed)]	Issued	1	6	5	

Table 8—Renewal applications for named person warrants

AGENCY	RELEVANT	APPLICATIONS FOR WARRANTS			
AGENCY	STATISTICS	05/06	06/07	07/08	
AUSTRALIAN FEDERAL POLICE	Made	23	17	43	
	Refused/withdrawn	0	0	0	
	Issued	23	17	43	
AUSTRALIAN CRIME	Made	34	39	40	
COMMISSION	Refused/withdrawn	0	0	0	
	Issued	34	39	40	
CONNECT THE ONLINE	Made	1	0	0	
COMMISSION OF WESTERN	Refused/withdrawn	0	0	0	
AUSTRALIA	Issued	1	0	0	
NEW SOUTH WALES CRIME	Made	9	5	13	
COMMISSION	Refused/withdrawn	0	0	0	
	Issued	9	5	13	
	Made	2	5	14	
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0	0	
	Issued	2	5	14	
OFFICE OF DOLLOR	Made	-	-	6	
OFFICE OF POLICE INTEGRITY	Refused/withdrawn	-	-	0	
zemii	Issued	-	-	6	
	Made	14	13	24	
VICTORIA POLICE	Refused/withdrawn	0	0	0	
	Issued	14	13	24	
MECTEDNI ALICTRALIA	Made	2	5	4	
WESTERN AUSTRALIA POLICE	Refused/withdrawn	0	0	0	
FOLICE	Issued	2	5	4	
	Made	85	84	144	
TOTAL [paragraph 100(ed)]	Refused/withdrawn	0	0	0	
	Issued	85	84	144	

Table 9—Named person warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS WITH CONDITIONS		
		05/06	06/07	07/08
AUSTRALIAN CRIME COMMISSION	Made	1	1	1
	Refused/withdrawn	0	0	0
	Issued	1	1	1
	Made	1	1	1
TOTAL [paragraph 100(2)(ea)]	Refused/withdrawn	0	0	0
	Issued	1	1	1

- 4.18 Paragraphs 100(1)(eb) and (2)(eb) of the TIA Act provide that the report must include, for each agency and in total, the number of named person warrants issued which involved the interception of services in the following ranges:
  - the number of warrants involving interception of a single telecommunications service
  - the number of warrants involving interception of between two and five telecommunications services
  - the number of warrants involving interception of between six and ten telecommunications services, and
  - the number of warrants involving interception of more than ten telecommunications services.
- 4.19 This information is included in Table 10.

Table 10—Number of services intercepted under named person warrants

AGENCY	RELEVANT	NUMBER OF SERVICES		
	STATISTICS	05/06	06/07	07/08
	1 service only	37	28	31
AUSTRALIAN CRIME COMMISSION	2 – 5 services	55	76	59
COMMISSION	6 – 10 services	16	8	6
	10+ services	5	3	1
	1 service only	11	17	27
AUSTRALIAN FEDERAL POLICE	2 – 5 services	62	48	73
	6 – 10 services	8	9	18
	10+ services	0	2	8
	1 service only	0	0	0
CORRUPTION AND CRIME COMMISSION	2 – 5 services	3	0	2
COMMISSION	6 – 10 services	1	0	1
	10+ services	1	0	0
INDEPENDENT COMMISSION AGAINST CORRUPTION	1 service only	0	0	0
	2 – 5 services	0	0	2
	6 – 10 services	0	0	0
	10+ services	0	0	0

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES			
		05/06	06/07	07/08	
	1 service only	14	5	12	
NEW SOUTH WALES CRIME COMMISSION	2 – 5 services	22	17	34	
CRIME GOIVINI GOION	6 – 10 services	5	11	10	
	10+ services	0	0	1	
	1 service only	3	5	11	
NEW SOUTH WALES POLICE	2 – 5 services	6	17	29	
	6 – 10 services	2	2	0	
	10+ services	1	0	0	
	1 service only	0	0	1	
NORTHERN TERRITORY POLICE	2 – 5 services	0	3	5	
	6 – 10 services	0	2	1	
	10+ services	0	0	0	
	1 service only	0	0	1	
OFFICE OF POLICE INTEGRITY	2 – 5 services	0	3	8	
	6 – 10 services	0	0	1	
	10+ services	0	0	0	
	1 service only	0	0	0	
POLICE INTEGRITY COMMISSION	2 – 5 services	0	0	0	
COMMISSION	6 – 10 services	0	0	0	
	10+ services	0	0	0	
	1 service only	0	1	5	
SOUTH AUSTRALIA POLICE	2 – 5 services	5	6	4	
	6 – 10 services	4	1	1	
	10+ services	0	0	0	
	1 service only	0	0	0	
TASMANIA POLICE	2 – 5 services	0	2	0	
	6 – 10 services	0	0	0	
	10+ services	0	0	0	
	1 service only	17	15	24	
VICTORIA POLICE	2 – 5 services	45	70	60	
	6 – 10 services	3	7	6	
	10+ services	2	0	0	
	1 service only	1	5	5	
WESTERN AUSTRALIA POLICE	2 – 5 services	24	18	17	
	6 – 10 services	5	4	8	
	10+ services	1	0	0	
	1 service only	83	76	117	
TOTAL [paragraph 100(2)(eb)]	2 – 5 services	222	260	293	
	6 – 10 services	44	44	52	
	10+ services	10	5	10	

4.20 Paragraphs 100(1)(ec) and (2)(ec) of the TIA Act provide that the report must include, for each agency and in total, the total number of services intercepted under named person warrants. There was a 30% increase in the total number of services intercepted from the previous reporting period. This information is included in Table 11.

Table 11—Total number of services intercepted under named person warrants

AGENCY	TOTAL NUMBER OF SERVICES INTERCEPTED		
	05/06	06/07	07/08
AUSTRALIAN FEDERAL POLICE	173	248	619
AUSTRALIAN CRIME COMMISSION	214	374	249
CORRUPTION AND CRIME COMMISSION OF WESTERN AUSTRALIA	23	0	18
INDEPENDENT COMMISSION AGAINST CORRUPTION	0	0	6
NEW SOUTH WALES CRIME COMMISSION	88	131	205
NEW SOUTH WALES POLICE	40	88	92
NORTHERN TERRITORY POLICE	0	28	26
OFFICE OF POLICE INTEGRITY	0	9	38
POLICE INTEGRITY COMMISSION	0	0	0
SOUTH AUSTRALIA POLICE	49	31	24
TASMANIA POLICE	0	9	0
VICTORIA POLICE	160	246	231
WESTERN AUSTRALIAN POLICE	121	87	119
TOTAL	868	1251	1627

## **B-Party warrants**

- 4.21 Paragraphs 100(1)(ed), (ee) and (ef) of the TIA Act provide that the report must include the same statistics outlined above in relation to warrants where subparagraph 46(1)(d)(ii) applied, being B-Party warrants. This means that the following statistics must be provided:
  - the number of B-Party warrants applied for, refused and issued
  - the number of telephone applications for B-Party warrants made, refused and issued
  - the number of renewal applications for B-Party warrants made, refused and issued
  - the number of B-Party warrants which authorise entry onto premises, and
  - the number of B-Party warrants issued with conditions or restrictions attached.
- 4.22 Paragraphs 100(2)(ed), (ee) and (ef) of the TIA Act provide that the report must also include these statistics in total across all agencies. Tables 12 to 14 set out the information supplied by intercepting agencies regarding B-Party warrants. As this is the second reporting period in which B-Party warrants have been obtained, only the 2006-07 figures are available for comparison. There has been a 35% increase since the

last reporting period. This increase can be attributed to agencies being more familiar with the B-Party regime and when such warrants are effective.

4.23 No B-Party warrants authorised entry onto premises during the reporting period and no B-Party warrants were issued subject to any specific conditions or restrictions.

**Table 12—Applications for B-Party warrants** 

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRAN	
		06/07	07/08
	Made	7	15
AUSTRALIAN FEDERAL POLICE	Refused/withdrawn	0	0
	Issued	7	15
	Made	1	3
INDEPENDENT COMMISSION AGAINST CORRUPTION	Refused/withdrawn	0	0
AUAINST CORROL TION	Issued	1	3
	Made	18	22
NEW SOUTH WALES CRIME COMMISSION	Refused/withdrawn	0	0
CKTIME COMMISSION	Issued	18	22
	Made	39	26
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0
	Issued	39	26
	Made	5	15
VICTORIA POLICE	Refused/withdrawn	0	0
	Issued	5	15
	Made	1	0
WESTERN AUSTRALIA POLICE	Refused/withdrawn	0	0
	Issued	1	0
	Made	-	3
CORRUPTION AND CRIME COMMISSION OF WESTERN	Refused/withdrawn	-	0
AUSTRALIA	Issued	-	3
	Made	-	10
OFFICE OF POLICE INTEGRITY	Refused/withdrawn	-	0
	Issued	-	10
	Made	-	2
AUSTRALIAN CRIME	Refused/withdrawn	-	0
COMMISSION	Issued	-	2
	Made	71	96
TOTAL [paragraph 100(2)(ed)]	Refused/withdrawn	0	0
	Issued	71	96

Table 13—Telephone applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS	
		06/07	07/08
	Made	7	7
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0
	Issued	7	7
	Made	2	2
VICTORIA POLICE	Refused/withdrawn	0	0
	Issued	2	2
	Made	9	9
TOTAL [paragraph 100(2)(ed)]	Refused/withdrawn	0	0
	Issued	9	9

Table 14—Renewal applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS	
		06/07	07/08
	Made	2	1
AUSTRALIAN FEDERAL POLICE	Refused/withdrawn	0	0
	Issued	2	1
	Made	4	0
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0
	Issued	4	0
	Made	-	8
VICTORIA POLICE	Refused/withdrawn	-	0
	Issued	-	8
	Made	-	2
NEW SOUTH WALES CRIME COMMISSION	Refused/withdrawn	-	0
CRIVIL COMMISSION	Issued	-	2
	Made	6	11
TOTAL [paragraph 100(2)(ed)]	Refused/withdrawn	0	0
	Issued	6	11

Interpretative note relating to B-Party warrants

- 4.24 These statistics demonstrate that B-Party warrants are only used sparingly. Of the thirteen agencies that were issued telecommunications interception warrants during the reporting period, only eight applied for and were issued B-Party warrants, with B-Party warrants representing only 3% of the total number of warrants issued.
- 4.25 It is important to note that only 11 of the 96 B-Party warrants were renewed, meaning that agencies recognise the primary purpose of B-Party warrants, which is a mechanism for identifying the telecommunications services, identity or location of the suspect.

Categories of serious offences specified in telecommunications interception warrants

- 4.26 Paragraph 100(1)(f) of the TIA Act provides that the report must set out the categories of serious offences specified in telecommunications interception warrants issued to each agency during the reporting period. Paragraph 100(1)(g) of the TIA Act provides that the report must set out the number of serious offences in each category that were so specified.
- 4.27 The information required by paragraphs 100(1)(f) and (g) is set out in Tables 15 to 27. As in previous years, agencies obtained the majority of warrants to assist with investigations into drug-related offences.
- 4.28 Care should be taken in interpreting the following table as warrants may have been issued in the investigation of more than one serious offence. The data for each serious offence includes figures for any related ancillary offences, such as assisting in the commission of, or conspiring to commit, a principal offence.

Table 15—Categories of serious offences specified in telecommunications interception warrants issued to the Australian Crime Commission

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
ACC special investigations	152	208	160
Bribery or corruption	4	0	0
Money laundering	0	0	0
Serious drug offences	44	3	16
Serious fraud or loss of revenue	2	0	3
Serious personal injury or loss of life	0	0	0

Table 16—Categories of serious offences specified in telecommunications interception warrants issued to the Australian Federal Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Bribery or corruption	6	9	0
Child pornography	5	31 <sup>3</sup>	0
Cybercrime	2	4	1
Kidnapping	3	5	4
Loss of life	2	4	2
Money laundering	19	48	106
Murder	10	1	2
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the <i>Criminal Code</i>	-	-	3
Organised crime	32	11	16
People smuggling or sexual servitude	23	5	5
Serious drug offences	372	387	361
Serious fraud or loss of revenue	12	20	13
Serious personal injury or loss of life	4	21	14
Serious damage to property	0	3	5
Terrorism	46	28	10
Telecommunications offences	-	31 <sup>4</sup>	3

Table 17—Categories of serious offences specified in telecommunications interception warrants issued to the Corruption and Crime Commission of Western Australia

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Bribery or corruption	79	122	102
Cybercrime	-	-	3

32

<sup>&</sup>lt;sup>3</sup> There was an error in the information provided in the 2006-2007 Annual Report. The category of child pornography was recorded as 31, when it should have read zero.

<sup>&</sup>lt;sup>4</sup> The category of telecommunications offences was entered as zero, when it should have read 31.

Table 18—Categories of serious offences specified in telecommunications interception warrants issued to the Independent Commission Against Corruption

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Bribery or corruption	11	33	30
Serious fraud or loss of revenue	6	0	3

Table 19—Categories of serious offences specified in telecommunications interception warrants issued to the New South Wales Crime Commission

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Bribery or corruption	6	0	0
Cybercrime	8	15	0
Kidnapping	2	0	0
Money laundering	80	123	142
Murder	142	57	64
Offences relating to the administration of justice	0	14	0
Organised crime	72	130	40
Serious damage to property	39	17	13
Serious drug offences	707	555	474
Serious fraud or loss of revenue	28	0	27
Serious personal injury or loss of life	60	25	16

Table 20—Categories of serious offences specified in telecommunications interception warrants issued to the New South Wales Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Bribery or corruption	18	26	33
Child pornography	-	-	5
Kidnapping	10	40	27
Murder	178	216	231
Organised crime	153	106	120
Serious damage to property	25	38	57
Serious drug offences	128	180	145
Serious fraud or loss of revenue	4	14	7
Serious personal injury or loss of life	119	265	208
Terrorism	-	-	19

Table 21—Categories of serious offences specified in telecommunications interception warrants issued to Northern Territory Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Murder	-	8	4
Organised crime	-	-	1
Serious drug offences	-	19	32
Serious personal injury or loss of life	-	-	2

Table 22—Categories of serious offences specified in telecommunications interception warrants issued to the Office of Police Integrity

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	05/06	06/07	07/08
Bribery or corruption	-	3	68
Murder	-	10	11
Serious drug offences	-	3	1

Table 23—Categories of serious offences specified in telecommunications interception warrants issued to the Police Integrity Commission

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY				
	05/06	07/08			
Bribery or corruption	30	36	65		
Money laundering	-	-	11		
Murder	18	3	0		
Organised crime	2	2	3		
Serious drug offences	5	3	1		
Serious personal injury or loss of life	-	-	12		

Table 24—Categories of serious offences specified in telecommunications interception warrants issued to the South Australia Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY				
	05/06	06/07	07/08		
Bribery or corruption	1	5	4		
Kidnapping	0	0	1		
Murder	23	12	37		
Organised crime	4	0	0		
Serious damage to property	10	3	3		
Serious drug offences	73	57	71		
Serious fraud or loss of revenue	0	7	0		
Serious personal injury or loss of life	16	11	8		
Terrorism	13	0	0		

Table 25—Categories of serious offences specified in telecommunications interception warrants issued to Tasmania Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY				
	05/06	07/08			
Bribery or corruption	-	-	3		
Murder	-	-	3		
Organised crime	1	0	0		
Serious drug offences	0	13	5		
Serious fraud or loss of revenue	-	-	3		
Serious personal injury of loss of life	-	-	3		

Table 26—Categories of serious offences specified in telecommunications interception warrants issued to the Victoria Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY				
	05/06	06/07	07/08		
Bribery or corruption	7	3	0		
Kidnapping	14	5	1		
Murder	70	99	118		
Organised crime	0	4	4		
Serious damage to property	8	4	6		
Serious drug offences	192	163	180		
Serious fraud or loss of revenue	-	-	3		
Serious personal injury or loss of life	61	88	61		

Table 27—Categories of serious offences specified in telecommunications interception warrants issued to the Western Australia Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY				
	05/06	06/07	07/08		
Bribery or corruption	0	3	5		
Child pornography	4	1	0		
Kidnapping	4	1	0		
Money laundering	14	21	5		
Murder	15	13	29		
Organised crime	-	-	2		
Serious damage to property	5	2	2		
Serious drug offences	123	111	134		
Serious fraud or loss of revenue	3	0	7		
Serious personal injury or loss of life	19	15	15		
Terrorism	12	5	0		

Categories of serious offences specified in telecommunications interception warrants – all agencies

4.29 Paragraphs 100(2)(f) and (g) of the TIA Act provide that the categories of serious offences specified in telecommunications interception warrants for all agencies must be set out in combined form. This information is set out in Table 28.

Table 28—Categories of serious offences specified in telecommunications interception warrants in relation to all agencies

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY				
	05/06	06/07	07/08		
ACC special investigations <sup>5</sup>	152	208	160		
Bribery or corruption	162	240	310		
Child pornography	9	32	5		
Cybercrime	10	19	4		
Kidnapping	33	51	33		
Money laundering	113	192	264		
Murder	456	419	499		
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the <i>Criminal Code</i>	-	-	3		
Offences relating to the administration of justice	0	14	0		
Organised crime	264	253	186		
People smuggling or sexual servitude	23	5	5		
Serious damage to property	87	67	86		
Serious drug offences	1644	1494	1420		
Serious fraud or loss of revenue	55	34	66		
Serious personal injury or loss of life	279	425	339		
Telecommunications offences	-	-	3		
Terrorism	71	33	29		

-

<sup>&</sup>lt;sup>5</sup> Applies only to the ACC.

# **Duration of telecommunications interception warrants**

4.30 Section 49 of the TIA Act provides that a telecommunications interception warrant must specify the period for which it is to be in force. Warrants may be revoked before the specified period lapses. Section 57 of the Act provides that the chief officer of an agency must revoke a warrant where he or she is satisfied that the grounds on which the warrant was issued have ceased to exist.

Duration of original telecommunications interception warrants

- 4.31 Paragraph 101(1)(a) of the TIA Act provides that the report must set out the average period specified in original telecommunications interception warrants in relation to each agency. Paragraph 101(1)(b) provides that the report must set out the average of the periods for which those warrants were actually in force. Paragraphs 101(2)(a) and (b) provide that the same information must be averaged across all agencies. This information is set out in Table 29.
- 4.32 The average duration of warrants, both specified and actual, has remained reasonably consistent over the previous reporting periods. The average duration has increased for some agencies while it has decreased for others, with all variations being minor, meaning that there is no general trend relating to the duration of warrants.
- 4.33 However, as in previous reporting periods, the average actual duration of warrants is again significantly less than the average specified duration of warrants, meaning that agencies continue to regularly review warrants and revoke those that are no longer required prior to their expiration. This demonstrates that agencies do not intercept telecommunications services longer than they need to for their investigations.

Table 29—Duration of original telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	05/06	06/07	07/08	05/06	06/07	07/08
AUSTRALIAN CRIME COMMISSION	88.44	88.66	86.72	48.19	58.43	56.94
AUSTRALIAN FEDERAL POLICE	78.90	75.82	77.06	35.84	45.72	40.82
CORRUPTION AND CRIME COMMISSION	90	85.38	76.92	73.73	62.36	49.10
INDEPENDENT COMMISSION AGAINST CORRUPTION	77.85	88.39	79.44	58.46	55.43	60.56
NEW SOUTH WALES CRIME COMMISSION	83.31	79.05	82.34	49.81	48.41	53.08
NEW SOUTH WALES POLICE	42.52	49.01	46.46	30.63	29.11	37.29
NORTHERN TERRITORY POLICE	-	67.50	83.27	-	50.50	68.97
OFFICE OF POLICE INTEGRITY	-	89.33	76.23	-	63.60	66.78
POLICE INTEGRITY COMMISSION	80.34	86.67	87.78	62.37	69	77.49
SOUTH AUSTRALIA POLICE	74.64	78.11	82.04	46.96	48.04	55.36
TASMANIA POLICE	90	74.85	54.18	12	59	18.20
VICTORIA POLICE	53.92	58.28	51.59	37.53	45.45	37.35
WESTERN AUSTRALIA POLICE	53.97	57.38	63.92	32.90	38.78	41.38
AVERAGE [paragraphs 101(2)(a)-(b)]	68.10	67.32	67.56	41.11	47.62	45.92

Duration of renewal telecommunications interception warrants

4.34 Paragraphs 101(1)(c), (1)(d), (2)(c) and (2)(d) of the TIA Act provide that the report set out corresponding information in relation to telecommunications interception warrants that have been renewed. This information is set out in Table 30. As with original warrants, there is no substantial variation in the average specified or actual durations of renewal warrants from previous reporting periods.

Table 30—Duration of renewal of telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			RAGE PER RANTS IN F (DAYS)	-	
	05/06	06/07	07/08	05/06	06/07	07/08
AUSTRALIAN CRIME COMMISSION	89.27	41.64	89.61	73.07	60.29	71.20
AUSTRALIAN FEDERAL POLICE	85.92	88.23	88.97	44.05	69.82	73.31
CORRUPTION AND CRIME COMMISSION	75	90	90	53.33	83.66	71.22
INDEPENDENT COMMISSION AGAINST CORRUPTION	60	90	74	59	32.33	51.33
NEW SOUTH WALES CRIME COMMISSION	78.61	71.47	76.14	56.83	45.88	53.63
NEW SOUTH WALES POLICE	45.55	49.75	52.18	40.97	47.88	58.66
NORTHERN TERRITORY POLICE	-	60	0	-	60	0
OFFICE OF POLICE INTEGRITY	-	90	85	-	06	83.86
POLICE INTEGRITY COMMISSION	62.31	88.45	89.80	54.20	78.86	82.78
SOUTH AUSTRALIA POLICE	87.08	-	90	53.33	-	42.00
TASMANIA POLICE	-	90	0	-	47	0
VICTORIA POLICE	59.81	66.95	54.52	38.90	51.21	47.92
WESTERN AUSTRALIA POLICE	55.38	52.80	68.28	35.75	47	60.69
AVERAGE [paragraphs 101(2)(a)-(b)]	72.68	65.93	73.89	50.76	51.16	62.23

41

<sup>&</sup>lt;sup>6</sup> An average period was not recorded as the warrant was still in force at the end of the reporting period.

Interpretative note relating to average duration of warrants across all agencies

- 4.35 The figures in Tables 29 and 30 reflect the average durations, both specified and actual, for all original and renewal warrants issued to all agencies.
- 4.36 These figures illustrate that the duration of warrants is generally consistent from year to year, and that the actual duration of warrants is typically one to two weeks shorter than the specified duration.

### Duration of original B-Party warrants

- 4.37 As with all telecommunications interception warrants, a B-Party warrant must specify the period for which it is to be in force and may be revoked before the specified period lapses. The obligation on the chief officer of an agency to revoke a B-Party warrant where he or she is satisfied that the grounds on which the warrant was issued have ceased to exist is particularly important in the case of B-Party warrants. For example, if a B-Party warrant was issued because the telecommunications service of the target was not able to be identified, once the service is identified, the warrant must be revoked.
- 4.38 Paragraph 101(1)(da) of the TIA Act provides that the report must set out the average period specified in original B-Party warrants in relation to each agency and the average of the periods for which those warrants were actually in force. Paragraph 101(2)(da) provides that the same information must be averaged across all agencies. This information is set out in Table 31.
- 4.39 As this is the second year in which B-Party warrants have been issued, only the 2006-07 information is available as comparative information.

Table 31—Duration of original B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)
	06/07	07/08	06/07	07/08
AUSTRALIAN CRIME COMMISSION	-	26.33	-	3.83
AUSTRALIAN FEDERAL POLICE	45.00	35.93	21.00	19.4
CORRUPTION AND CRIME COMMISSION	-	45	-	15.0
INDEPENDENT COMMISSION AGAINST CORRUPTION	45.00	15	0 <sup>7</sup>	15
NEW SOUTH WALES CRIME COMMISSION	44.5	42.15	21.31	27.75
NEW SOUTH WALES POLICE	32.43	21.96	22.08	18.0
OFFICE OF POLICE INTEGRITY	-	45	-	16.13
VICTORIA POLICE	34.40	34	27.76	25.29
WESTERN AUSTRALIA POLICE	30.00	0	26.00	0
AVERAGE [paragraph 101(2)(da)]	37.63	33.10	24.82	22.82

\_

<sup>&</sup>lt;sup>7</sup> No actual duration is known as the warrant was still in force at the end of the reporting period.

## Duration of renewal B-Party warrants

4.40 Paragraphs 101(1)(da) and (2)(da) of the TIA Act also provide that the report must set out corresponding information in relation to B-Party warrants that have been renewed. This information is set out in Table 32.

Table 32—Duration of renewal of B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)
	06/07	07/08	06/07	07/08
AUSTRALIAN FEDERAL POLICE	45.00	45	45.00	40
NEW SOUTH WALES POLICE	35.00	0	34.8	0
NEW SOUTH WALES CRIME COMMISSION	43.00	43.5	43.00	31.5
VICTORIA POLICE	-	45	-	45
AVERAGE [paragraphs 101(2)(da)]	39.40	44.72	39.30	42.09

Number of final renewals of telecommunications interception warrants

- 4.41 Paragraph 101(1)(e) of the TIA Act provides that the report must record the number of final renewals that ceased to be in force during the reporting period. A final renewal refers to a telecommunications interception warrant that is the last renewal of an original warrant, and is recorded in terms of the number of days after the date of issue of the original warrant that the final renewal ceases to be in force. The categories of final renewals are as follows:
  - 90 day final renewal—a last renewal that ceases to be in force more than 90 days but not more than 150 days after the date of issue of the original warrant
  - 150 day final renewal—a last renewal that ceases to be in force more than 150 days but not more than 180 days after the date of issue of the original warrant, and
  - 180 day final renewal—a last renewal that ceases to be in force more than 180 days after the date of issue of the original warrant.
- 4.42 This information gives some indication of the overall duration of warrants that have been renewed. Paragraph 101(2)(e) of the Act provides that the same information must be set out in total across all agencies. This information is set out in Table 33.
- 4.43 The figures in Table 33 show an increase in 90 day renewals, and slight decreases in 150 and 180 day renewals.

Table 33—Number of 'final renewals'

AGENCY	(	90 DAYS		150 DAYS			180 DAYS		
	05/06	06/07	07/08	05/06	06/07	07/08	05/06	06/07	07/08
AUSTRALIAN CRIME COMMISSION	8	1	7	15	5	14	9	23	10
AUSTRALIAN FEDERAL POLICE	5	7	10	34	30	30	18	9	31
CORRUPTION AND CRIME COMMISSION	-	-	5	3	-	1	-	27	10
INDEPENDENT COMMISSION AGAINST CORRUPTION	1	3	4	1	-	2	1	-	0
NEW SOUTH WALES CRIME COMMISSION	5	7	4	9	3	3	4	-	3
NEW SOUTH WALES POLICE	508	32	41	14	8	7	5	2	2
NORTHERN TERRITORY POLICE	-	-	0	-	3	0	-	-	0
OFFICE OF POLICE INTEGRITY	-	-	3	-	-	3	-	-	7
POLICE INTEGRITY COMMISSION	3	-	2	3	5	0	-	10	1
SOUTH AUSTRALIA POLICE	2	-	3	3	-	0	2	-	0
TASMANIA POLICE	-	1	0	-	-	0	-	-	0
VICTORIA POLICE	10	22	18	1	12	9	5	7	1
WESTERN AUSTRALIA POLICE	5	8	7	-	13	1	ı	1	10
TOTAL [paragraph 101(2)(e)]	547	81	104	83	79	70	44	79	75

## **Effectiveness of telecommunications interception warrants**

- 4.44 Section 102 of the TIA Act provides that the report must include information about the effectiveness of telecommunications interception warrants. Specifically, the report must state how many arrests were made on the basis of information obtained by intercepting a communication under a telecommunications interception warrant.
- 4.45 The report must also include information about prosecutions for 'prescribed offences' in which lawfully intercepted information was given in evidence and the number of those in respect of which convictions were recorded. The term 'prescribed offence' is defined in subsection 5(1) of the TIA Act to mean:
  - a serious offence
  - an offence against subsection 7(1) of the TIA Act, which prohibits the interception of telecommunications
  - an offence against section 63 of the TIA Act, which prohibits the communication, recording or use of intercepted information
  - an offence against subsection 108(1) of the TIA Act, which prohibits the accessing of stored communications
  - an offence against section 133 of the TIA Act, which prohibits the communication, recording or use of lawfully accessed information
  - an offence against a provision of Part 10.6 of the *Criminal Code*, which deals with the protection of telecommunications networks and installations
  - any other offence punishable by imprisonment for life or for a period, or maximum period, of at least 3 years, or
  - an ancillary offence relating to an offence of a kind referred to above.
- 4.46 Figures for the number of arrests for prescribed offences in which lawfully intercepted information was given in evidence are provided in respect of all eligible authorities and eligible Commonwealth authorities. While only eligible authorities that are interception agencies for the purposes of the TIA Act may obtain warrants, information obtained under such warrants may in some circumstances be communicated to another eligible authority that is not an interception agency.
- 4.47 The communication of that information may result in further investigation and possibly arrests and prosecution by an eligible authority on the basis of lawfully intercepted information. That is notwithstanding that the authority is itself unable to obtain a warrant. An example of such a situation might be the interception under warrant by a Commonwealth agency of information pointing to the commission of a State offence where the police force of that State has not been declared to be an interception agency for the purposes of the TIA Act but is an eligible authority. In these circumstances, it may be possible for the Commonwealth agency to communicate the information to the State police service in accordance with Part 2-6 of the TIA Act.

- 4.48 Eligible authorities that are not interception agencies for the purposes of the TIA Act are:
  - the Queensland Police
  - the Queensland Crime and Misconduct Commission
  - the Inspector of the Police Integrity Commission
  - the Inspector of the Independent Commission against Corruption, and
  - the Parliamentary Inspector of the Corruption and Crime Commission of Western Australia.

Arrests on the basis of lawfully intercepted information

- 4.49 Paragraph 102(1)(a) of the TIA Act provides that the report must set out, for each agency and eligible authority, how many arrests were made in connection with the performance by the agency or authority of its functions and on the basis of information that was or included lawfully intercepted information during the reporting period.
- 4.50 Paragraph 102(2)(a) provides that the total number of arrests across agencies and eligible authorities must be reported. This information is set out in Table 34. The number of arrests made during the reporting period represents an 18.1% increase on the figures reported during 2006-07. On a per warrant basis, there were 63 arrests for every 100 warrants issued. This represents an increase from the previous reporting period, in which agencies reported 53 arrests for every 100 warrants issued.<sup>8</sup>

47

<sup>&</sup>lt;sup>8</sup> This figure was incorrectly reported as 51 arrests for every 100 warrants issued in the last annual report.

Table 34—Arrests on the basis of lawfully intercepted information

AGENCY	NUMBER OF ARRESTS				
	05/06	06/07	07/08		
AUSTRALIAN CRIME COMMISSION	148	116	166		
AUSTRALIAN FEDERAL POLICE	111	99	165		
CORRUPTION AND CRIME COMMISSION	0	5	3		
CRIME AND MISCONDUCT COMMISSION	27	66	231 <sup>9</sup>		
INDEPENDENT COMMISSION AGAINST CORRUPTION	2	0	0		
NEW SOUTH WALES CRIME COMMISSION	307	438	306		
NEW SOUTH WALES POLICE	761	345	321		
NORTHERN TERRITORY POLICE	0	18	27		
POLICE INTEGRITY COMMISSION	27	2	85		
QUEENSLAND POLICE	0	0	18		
SOUTH AUSTRALIA POLICE	124	76	67		
TASMANIA POLICE	6	6	7		
VICTORIA POLICE	388	439	493		
WESTERN AUSTRALIA POLICE	123	131	167		
TOTAL [paragraph 102(2)(a)]	2024	1741	2056		

-

<sup>&</sup>lt;sup>9</sup> As the CMC is not entitled to apply for warrants under the TIA Act and obtains access to TI material through joint operations with other law enforcement agencies, the statistics supplied by the CMC may duplicate or be included in the totals supplied by those agencies.

Prosecutions in which lawfully intercepted information was given in evidence

- 4.51 Paragraphs 102(1)(b) and (c) of the TIA Act provide that the report must set out, for each agency and each eligible authority, the categories of prescribed offences prosecuted, and the number of offences in each category, in which lawfully intercepted information was given in evidence, and the number of offences in each category in respect of which convictions were recorded. Paragraphs 102(2)(b) and (c) provide that this information must be set out in total across all agencies and eligible authorities. The information required is set out in Tables 35 to 37.
- 4.52 During the reporting period, there was a 46.6% increase in the number of prosecutions commenced and a 12.7% increase in the number of convictions obtained on the basis of lawfully intercepted information.
- 4.53 On a per warrant basis, there were 120 prosecutions and 78 convictions secured on the basis of intercepted information for every 100 warrants issued. In the previous reporting period, agencies reported 81 prosecutions and 69 convictions based on lawfully intercepted information for every 100 warrants issued. It should be noted that the statistics do not necessarily relate to lawfully intercepted information obtained under telecommunications interception warrants issued in the current reporting period.
- 4.54 In these tables, the category 'other offences' refers to any other offence punishable by imprisonment for life or for a period of at least 3 years, or to any related ancillary offences. It should also be noted that, to assist readability, the categories of offences in the tables are grouped more thematically than has been the case in previous reports.

Table 35—Prosecutions in which lawfully intercepted information used in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC	СМС	ICAC	NSW	NSW POL	NT	PIC	OLD	SA POL	TAS	VIC	WA	TOTAL
Bribery or corruption			3	2			94		1				11		111
Child pornography		2												3	2
Conspiring	10								-						1
Cybercrime						-									-
Kidnapping						2	3						-		6
Money laundering	l	24				48								20	93
Murder						2	62			2		1	11	1	66
Organised crime						239	329						3	34	909
Serious damage to property						30	8						3	4	45
Serious drug offences	44	102		228		395	655	21	12	18	57	3	230	578	2343
Serious fraud or loss of revenue				1		1	63		4						89
Serious personal injury/ loss of life						8	197		2		3		36	26	272
Terrorism		7													7
Other offences	2	7	2	26		4			8		8		167	19	246
TOTAL	09	142	2	257	0	736	1428	21	28	20	89	4	462	685	3916

Table 36—Convictions in which lawfully intercepted information given in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC	СМС	ICAC	NSW	NSW	NT	PIC	OLD	SA POL	TAS	VIC	WA	TOTAL
Bribery or corruption			3				34		-				<u></u>		49
Child pornography		1												3	4
Conspiring	10								-						7
Cybercrime						_									-
Kidnapping						2	8								œ
Money laundering	-					48									49
Murder						2	46						7		28
Organised crime						239	149						3	27	418
Serious damage to property						30	-						-		32
Serious drug offences	41	13		49		393	274	6	12	2	45		226	461	1525
Serious fraud or loss of revenue						1	23		4						28
Serious personal injury/ loss of life						8	66		2				32	12	153
Terrorism															0
Other offences	5		2	12		4			8		8		162	2	206
TOTAL	57	14	5	61	0	734	629	6	28	2	53	0	442	208	2542

Table 37—Prosecutions and convictions in which lawfully intercepted information given in evidence

AGENCY	CATEGORIES OF OFFENCES PROSECUTED	PROSE	ER OF OFF CUTED FO CATEGOR	R EACH	CC RECOI	IUMBER O ONVICTIO RDED FOR CATEGOR	NS EACH
		05/06	06/07	07/08	05/06	06/07	07/08
	Serious Offence	42	41	55	38	44	52
AUSTRALIAN CRIME COMMISSION	Other <sup>10</sup>	10	24	5	9	18	5
COMMISSION	Agency Total	52	65	60	47	62	57
	Serious Offence	69	99	136	2	19	14
AUSTRALIAN FEDERAL	Other	0	17	6	0	0	0
POLICE	Agency Total	69	116	142	2	19	14
	Serious Offence	3	0	3	1	0	3
CORRUPTION AND CRIME	Other	0	18	2	0	18	2
COMMISSION	Agency Total	3	18	5	1	18	5
	Serious Offence	216	216	231	13	37	49
CRIME AND MISCONDUCT COMMISSION	Other	6	11	26	0	5	12
COMMISSION	Agency Total	222	227	257	13	42	61
	Serious Offence	3	21	0	3	21	0
INDEPENDENT COMMISSION AGAINST	Other	0	37	0	0	37	0
CORRUPTION	Agency Total	3	58	0	3	58	0
	Serious Offence	1139	414	736	440	414	734
NEW SOUTH WALES CRIME COMMISSION	Other	2	3	0	2	3	0
CRIME COMMISSION	Agency Total	1141	417	736	442	417	734
	Serious Offence	271	1000	1428	172	480	629
NEW SOUTH WALES POLICE	Other	2	2	0	1	2	0
POLICE	Agency Total	273	1002	1428	173	482	629
	Serious Offence	-	-	21	-	-	9
NORTHERN TERRITORY POLICE	Other	-	-	0	-	-	0
POLICE	Agency Total	-	-	21	-	-	9
	Serious Offence	13	15	20	13	15	20
POLICE INTEGRITY COMMISSION	Other	0	9	8	0	9	8
COMMISSION	Agency Total	13	24	28	13	24	28
	Serious Offence	25	0	20	5	0	2
QUEENSLAND POLICE	Other	0	0	0	0	0	0
	Agency Total	25	0	20	5	0	2
0011711 411077	Serious Offence	31	86	60	29	54	45
SOUTH AUSTRALIA POLICE	Other	5	1	8	4	1	8
	Agency Total	36	87	68	33	55	53
	Serious Offence	0	3	4	0	0	0
TASMANIA POLICE	Other	0	13	0	0	0	0
	Agency Total	0	16	4	0	0	0

<sup>&</sup>lt;sup>10</sup> The 'Other' offences here refer to those offences that are not 'serious offences' (ie offences for which a telecommunications interception warrant can be obtained) but whose investigation is able to be furthered through the use of lawfully intercepted information. It also includes offences of dishonesty such as theft and offences against the administration of justice.

AGENCY	CATEGORIES OF OFFENCES PROSECUTED	PROSE	ER OF OFF CUTED FO CATEGORY	R EACH	CC RECOI	IUMBER O DNVICTIO RDED FOR CATEGOR	NS EACH
		05/06	06/07	07/08	05/06	06/07	07/08
	Serious Offence	329	220	295	320	216	280
VICTORIA POLICE	Other	117	81	167	107	78	162
	Agency Total	446	301	462	427	294	442
	Serious Offence	695	301	666	313	702	503
WESTERN AUSTRALIA POLICE	Other	29	39	19	14	82	5
POLICE	Agency Total	724	340	685	327	784	508
	Serious Offence	2836	2445	3675	1349	2008	2340
TOTAL	Other	171	228	241	137	247	202
	Grand Total	3007	2671	3916	1486	2255	2542

Interpretative note relating to prosecutions and convictions statistics

- 4.55 The statistics presented in Tables 35 to 37 should be interpreted with some caution, particularly in presuming a relationship between the number of arrests, prosecutions (which include committal proceedings) and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution/committal (if at all) until a later reporting period and any resulting conviction may be recorded in that or an even later reporting period. Additionally, the number of arrests may not equate to the number of charges laid as an arrested person may be prosecuted and convicted for a number of offences, some or all of which may be prosecuted at a later time.
- 4.56 Further, the tables may understate the effectiveness of interception in so far as, in some cases, prosecutions may be initiated, and convictions recorded, without the need to give intercepted information in evidence. In particular, agencies report that telecommunications interception effectively enables investigators to identify persons involved in, and the infrastructure of, organised criminal activities, particularly drug trafficking syndicates. In many cases, the weight of evidence obtained through telecommunications interception results in defendants entering guilty pleas, thereby obviating the need for the information to be introduced into evidence.
- 4.57 Finally, it should also be noted that some intercepting agencies that are not police forces do not have prosecutions and convictions as a primary aim. The anti-corruption and integrity bodies have a range of statutory powers available to them, with the result that an investigation does not necessarily require a prosecution and conviction to be considered successful.

Percentage of 'eligible warrants'

4.58 Subsections 102(3) and (4) of the TIA Act provide that the report must include information that provides a general indication of the proportion of telecommunications interception warrants that provide information which is used in the prosecution of an offence.

- 4.59 Subsection 102(3) of the TIA Act provides that the report must set out the number of eligible warrants issued to each agency during the reporting period and the percentage of warrants issued to that agency that were eligible warrants. An 'eligible warrant' is defined in subsection 102(3) as a warrant that was in force during the reporting period (not necessarily a warrant that was issued during the reporting period) where a prosecution was instituted or was likely to be instituted on the basis of information obtained by interceptions under the warrant.<sup>11</sup>
- 4.60 Subsection 102(4) of the TIA Act provides that the report must set out the percentage of each agency's total warrants in force during the reporting period, that were eligible warrants. These figures are set out in Table 38, and indicate a 1.2% decrease in eligible warrants when compared to the previous reporting period.

Table 38—Percentage of 'eligible warrants'

AGENCY	NUMBER OF ELIGIBLE WARRANTS	TOTAL NUMBER OF WARRANTS	%
AUSTRALIAN FEDERAL POLICE	379	642	59.03
AUSTRALIAN CRIME COMMISSION	151	217	69.58
CORRUPTION AND CRIME COMISSION	97	134	72.38
INDEPENDENT COMMISSION AGAINST CORRUPTION	32	49	65.31
NEW SOUTH WALES CRIME COMMISSION	553	632	87.50
NEW SOUTH WALES POLICE	727	934	77.83
NORTHERN TERRITORY POLICE	30	37	81.08
OFFICE OF POLICE INTEGRITY	12	79	15.19
POLICE INTEGRITY COMMISSION	39	101	38.61
SOUTH AUSTRALIA POLICE	71	141	50.35
TASMANIA POLICE	14	17	82.35
VICTORIA POLICE	343	417	82.25
WESTERN AUSTRALIA POLICE	192	220	87.27
TOTAL [subsection 102(4)]	2640	3619	72.95

\_

<sup>&</sup>lt;sup>11</sup> If the warrant was a renewal, this includes information obtained under the original or any renewal of the original warrant; if the warrant was an original warrant, this includes information obtained under any renewal of that original warrant.

# **Emergency interception**

- 4.61 Section 102A of the TIA Act provides that the report must set out the number of occasions on which an officer or staff member of the agency intercepted a communication in reliance on subsection 7(4) or (5) of the TIA Act. These provisions permit the Australian Federal Police or a police force of a State or the Northern Territory to intercept calls in emergencies such as sieges and, with appropriate consent, in kidnapping and extortion cases.
- 4.62 An interception in reliance on subsection 7(4) of the TIA Act may be carried out by an officer of one of the above agencies where the officer is a party to the communication and, because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a telecommunications interception warrant to be made and there are reasonable grounds for suspecting that the other party to the communication has:
  - done an act that has resulted or may result in loss of life or the infliction of serious personal injury, or
  - threatened to kill or seriously injure another person or to cause serious damage to property, or
  - threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety.
- 4.63 In the reporting period no interceptions were carried out in reliance on subsection 7(4).
- 4.64 Interception of communications carried out pursuant to subsection 7(5) of the TIA Act must have been consented to by the person to whom the communication is directed, and must satisfy the same conditions specified for subsection 7(4).
- 4.65 The information required by section 102A is set out in Table 39.

Table 39—Interceptions made in reliance on subsection 7(5) of the TIA Act

SUSPICION OF	AUSTRA	LIAN FEDER	AL POLICE	NEW S	OUTH WALES	POLICE
OI	05/06	06/07	07/08	05/06	06/07	07/08
An act that may result in loss of life or serious injury	0	0	0	0	0	2
Threat to kill or seriously injure	0	0	2	0	0	0
Threat to take own life	0	0	0	0	0	0
TOTAL	0	0	2	0	0	2

## Other information

Total expenditure incurred by agencies

- 4.66 Paragraph 103(a) of the TIA Act provides that the report include details of the total expenditure (including expenditure of a capital nature) incurred by agencies in connection with the execution of telecommunications interception warrants for law enforcement purposes. The information required by this subsection is set out in Table 40.
- 4.67 Total expenditure incurred by agencies in connection with telecommunications interception increased by only 0.27% from the previous reporting period.

Table 40—Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants

AGENCY	то	TAL EXPENDITURE	(\$)
	05/06	06/07	07/08
AUSTRALIAN CRIME COMMISSION	5,126,736	5,452,586	5,078,973
AUSTRALIAN FEDERAL POLICE	5,999,850	6,128,468	8,256,034
CORRUPTION AND CRIME COMMISSION	1,813,310	1,649,035	1,638,018
INDEPENDENT COMMISSION AGAINST CORRUPTION	80,484	180,861	236,021
NEW SOUTH WALES CRIME COMMISSION	4,229,692	4,043,947	4,274,442
NEW SOUTH WALES POLICE	3,959,048	4,331,722	4,268,907
NORTHERN TERRITORY POLICE	0	1,545,000	886,000
OFFICE OF POLICE INTEGRITY	0	1,358,331	1,914,644
POLICE INTEGRITY COMMISSION	695,096	1,887,274	1,189,530
SOUTH AUSTRALIA POLICE	2,225,126	2,041,918	2,492,495
TASMANIA POLICE	259,863	442,000	548,000
VICTORIA POLICE	3,774,450	4,298,337	4,145,055
WESTERN AUSTRALIA POLICE	2,229,651	3,209,047	1,810,687
TOTAL	30,393,306	36,568,526	36,738,806

Average expenditure per telecommunications interception warrant

4.68 Paragraph 103(aa) of the TIA Act provides that the report must set out for each agency the average amount spent on each telecommunications interception warrant worked out using the formula:

Total warrant expenditure

Number of warrants

#### where:

'Total warrant expenditure' is the total expenditure incurred by the agency in connection with the execution of warrants during the period to which the report relates; and

'Number of warrants' means the number of warrants to which the total warrant expenditure relates.

4.69 The average expenditure incurred by agencies per warrant over the reporting period is presented in Table 41.

Table 41—Average expenditure per telecommunications interception warrant

AGENCY	AVE	RAGE EXPENDITUR	E (\$)
	05/06	06/07	07/08
AUSTRALIAN CRIME COMMISSION	25,380	25,842	28,374
AUSTRALIAN FEDERAL POLICE	11,718	11,477	15,577
CORRUPTION AND CRIME COMMISSION	22,953	13,517	16,059
INDEPENDENT COMMISSION AGAINST CORRUPTION	4,734	5,481	7,152
NEW SOUTH WALES CRIME COMMISSION	5,078	5,132	6,361
NEW SOUTH WALES POLICE	7,291	5,008	5,264
NORTHERN TERRITORY POLICE	0	57,222	23,946
OFFICE OF POLICE INTEGRITY	0	97,024	24,547
POLICE INTEGRITY COMMISSION	13,629	47,182	13,072
SOUTH AUSTRALIA POLICE	16,108	21,494	20,101
TASMANIA POLICE	259,863	34,000	32,235
VICTORIA POLICE	10,723	11,744	11,113
WESTERN AUSTRALIA POLICE	11,204	18,657	9,099

Availability of eligible judges and nominated AAT members

4.70 Paragraph 103(ab) of the TIA Act provides that the report must set out information about the availability of Judges to issue telecommunications interception warrants and the extent to which nominated AAT members have been used for that purpose. This information is set out in Tables 42 and 43.

Table 42—Availability of Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT Members to issue telecommunications interception warrants

ISSUING AUTHORITY	NUMBER ELIGIBLE
FEDERAL COURT JUDGES	9
FAMILY COURT JUDGES	12
FEDERAL MAGISTRATES	34
NOMINATED AAT MEMBERS	37

4.71 During the reporting period, approximately 90.72% of telecommunications interception warrants were issued by AAT members, 5.85% by Family Court Judges, 3.14% by Federal Magistrates and 0.22% by Federal Court Judges.

Table 43—Number of telecommunications interception warrants issued by Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT members

AGENCY		ISSUING A	UTHORITY	
	FEDERAL COURT JUDGES	FAMILY COURT JUDGES	FEDERAL MAGISTRATES	NOMINATED AAT MEMBERS
AUSTRALIAN CRIME COMMISSION	2	1	0	176
AUSTRALIAN FEDERAL POLICE	0	2	35	491
CORRUPTION AND CRIME COMMISSION	0	1	0	101
INDEPENDENT COMMISSION AGAINST CORRUPTION	0	0	0	33
NEW SOUTH WALES CRIME COMMISSION	3	0	25	644
NEW SOUTH WALES POLICE	0	0	31	780
NORTHERN TERRITORY POLICE	2	0	11	24
OFFICE OF POLICE INTEGRITY	0	0	0	78
POLICE INTEGRITY COMMISSION	0	0	0	91
SOUTH AUSTRALIA POLICE	0	0	0	124
TASMANIA POLICE	0	0	0	17
VICTORIA POLICE	0	0	0	373
WESTERN AUSTRALIA POLICE	0	186	0	13
TOTAL	7	190	102	2945

Interceptions on behalf of other agencies

- 4.72 Paragraph 103(ac) of the TIA Act provides that the report must set out the number (if any) of interceptions carried out by each agency on behalf of other agencies. Table 44 sets out the number of interceptions executed by agencies on behalf of other agencies during the reporting period.
- 4.73 The main circumstances in which this type of interception occurs is where a larger agency assists a smaller agency to intercept to reduce the costs of the smaller agency, or where, due to a higher than usual number of warrants or a system failure, an agency is required to utilise another agency's facilities.

Table 44—Number of interceptions carried out on behalf of other agencies

INTERCEPTION	INTERC	EPTION CARRIED OUT ON BEHALF (	OF
CARRIED OUT BY	TASMANIA POLICE	AUSTRALIAN CRIME COMMISSION	TOTAL
VIC POLICE	26	0	26
SA POLICE	0	2	2

Resources devoted to telecommunications interception

4.74 In addition to the total expenditure figures provided in Table 40, the figures in Table 45 below were supplied by each agency and provide a breakdown of the total recurrent costs of interception over the reporting period. However, as agencies do not necessarily treat particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

Table 45—Recurrent costs of interceptions per agency

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL (\$)
ACC	4,163,707	24,232	0	891,034	5,078,973
AFP	5,278,524	197,055	1,000,362	1,780,093	8,256,034
CCC WA	1,295,329	0	105,251	237,438	1,638,018
ICAC	67,453	28,712	13,536	126,320	236,021
NSW CC	2,155,173	65,333	626,066	1,427,870	4,274,442
NSW POLICE	3,286,369	402,072	48,900	531,566	4,268,907
NT POLICE	443,000	151,000	241,000	26,000	861,000
OPI	1,520,169	61,084	46,282	287,109	1,914,644
PIC	1,091,232	0	26,290	72,008	1,189,530
SA POLICE	2,086,577	234,384	109,807	61,727	2,492,495
TAS POLICE	344,000	2,000	40,000	162,000	548,000
VIC POLICE	3,427,276	296,004	108,512	313,263	4,145,055
WA POLICE	1,580,180	93,528	0	136,979	1,810,687

## Emergency services facility declarations

4.75 Paragraph 103(ad) of the TIA Act provides that the report must include the number and type of premises for each State and Territory that have been declared by the Attorney-General to be emergency services facilities pursuant to subsection 6(2A) of the TIA Act during the reporting period. The declarations enable such facilities to record incoming and outgoing calls without a telecommunications interception warrant. Table 46 provides the required information.

Table 46—Emergency service facility declarations

STATE/TERRITORY	POLICE	FIRE BRIGADE	AMBULANCE	DESPATCHING
AUSTRALIAN CAPITAL TERRITORY	3	0	0	1
NEW SOUTH WALES	8	4	6	1
VICTORIA	6	1	10	4
SOUTH AUSTRALIA	1	2	1	0
WESTERN AUSTRALIA	1	2	1	0
TASMANIA	1	2	1	0
QUEENSLAND	21	12	9	0
NORTHERN TERRITORY	3	1	2	1
TOTAL	43	24	30	7

## Reports by Commonwealth Ombudsman

- 4.76 The Commonwealth Ombudsman has the function of inspecting the records of Commonwealth interception agencies and reporting to the Attorney-General regarding the outcome of those inspections. Paragraph 103(ae) of the TIA Act provides that a summary of the information included in the Ombudsman's report must be included in this report, including:
  - a summary of the inspections conducted during the financial year under section
     83 of the Act
  - particulars of any deficiencies identified that impact on the integrity of the telecommunications interception regime, and
  - particulars of any remedial action taken or proposed to be taken to address those deficiencies.
- 4.77 The Ombudsman completed two inspections each of the ACC's and AFP's records during the reporting period. The reports concluded that there was generally a high degree of compliance with the detailed record keeping requirements of the TIA Act, although a number of recommendations were made after each inspection. Both agencies implemented a range of measures to improve compliance with the TIA Act.

#### The ACC

- 4.78 In relation to the ACC, the Ombudsman identified a deficiency in relation to the requirement to record each occasion where lawfully intercepted information was given in evidence. The ACC is seeking advice from the Attorney-General's Department in order to clarify the scope of these requirements.
- 4.79 The Ombudsman reported delays in relation to the sending of certified true copies of warrants (interception warrants and stored communications warrants) and instruments of revocation to carriers. The ACC advised that the Ombudsman's notional standard of five working days is difficult to meet for a number of practical reasons. The Ombudsman will consult further with agencies to determine whether a five day timeframe remains reasonable.
- 4.80 The Ombudsman also noted that copies of certified true copies of warrants (interception warrants and stored communications warrants) were not being retained on file, making it difficult to ascertain that a certified true copy of each warrant had been sent to the carrier as soon as practicable. The ACC implemented a new procedure whereby a photocopy of the certified copy of each warrant is retained on file.
- 4.81 The Ombudsman was unable to verify whether reports to be provided to the Attorney-General under sections 94(2) and 94B of the TIA Act were provided within the statutory timeframe. The ACC undertook to ensure that a copy of the final signed letter of transmission is kept on file to provide an appropriate audit trail.
- 4.82 The Ombudsman also made a recommendation that the ACC obtain more information from the carrier upon execution of a stored communications warrant to demonstrate that the accessed information was obtained in compliance with the TIA Act. The ACC advised that it will modify the template printed on blank discs sent to carriers to include the access date and access time, and that it will continue to liaise with the Attorney-General's Department and other agencies to establish a consistent approach to dealing with carriers in connection with stored communications warrants.

### The AFP

- 4.83 In relation to the AFP, the Ombudsman identified a deficiency in relation to the requirement to record each occasion where lawfully intercepted information was given in evidence. The AFP undertook to review how this information can be documented and reported in compliance with the TIA Act.
- 4.84 The Ombudsman also identified a deficiency in relation to delays in notifying the Secretary of the Attorney-General's Department of the issue and revocation of interception warrants. The AFP advised that it would focus on ensuring that the Secretary was informed within one working day of the issue or revocation of warrants, and a distinct improvement in this area was observed by the Ombudsman during the second inspection.
- 4.85 A similar deficiency was identified in relation to delays in notifying carriers of the revocation of warrants and in sending certified true copies of warrants and instruments of revocation to them. The AFP undertook to focus on providing notifications to carriers within one working day, but advised that it would be difficult to

forward certified true copies of warrants within five working days due to the time it takes to forward original copies from regional offices and arrange for an authorised officer to certify the copies. The Ombudsman will consult further with agencies to determine whether a five day timeframe remains reasonable.

- 4.86 The Ombudsman made a recommendation that more information be obtained from the carrier upon execution of a warrant to demonstrate that information accessed under the stored communications provisions was obtained in compliance with the TIA Act. The AFP advised that it would amend its procedures when requesting stored communications from carriers.
- 4.87 The Ombudsman made a recommendation that the AFP have appropriate systems in place to screen material to determine that information received from a carrier has been lawfully accessed. The AFP reviewed its procedures to ensure that a robust quality checking process is applied to all stored communications received from carriers.

#### Other information

4.88 Paragraph 103(b) of the TIA Act provides that the report must set out such other information (if any) as is prescribed. There was no other information prescribed during the reporting period.

# CHAPTER 5—STORED COMMUNICATIONS INFORMATION REQUIRED UNDER THE ACT

## The information required

- 5.1 The reporting requirements of the TIA Act in relation to accessing stored communications are contained in Part 3-6 of the Act, which provides that this report must include information on:
  - the relevant statistics relating to applications for stored communication warrants that were made by the agency during the reporting period (paragraph 162(2)(a))
  - the relevant statistics relating to telephone applications for stored communication warrants made by the agency during the reporting period (paragraph 162(2)(b))
  - the relevant statistics relating to renewal warrants that were made by the agency during the reporting period (paragraph 162(2)(c))
  - the number of warrants which were issued with specified conditions or restrictions (paragraph 162(2)(d))
  - the number of arrests made during the reporting period based on lawfully intercepted information (paragraph 163(a)), and
  - the number of proceedings which ended in the reporting period in which information collected by means of a warrant was given in evidence (paragraph 163(b)).
- 5.2 The TIA Act provides that the information must be set out in relation to each agency that is entitled to be issued with warrants authorising access to stored communications. In addition, the information must be combined for all agencies to indicate the overall extent and effectiveness of access to stored communications under the TIA Act.
- 5.3 It is possible for an enforcement agency to record arrests, proceedings in which lawfully accessed information was given in evidence or convictions based on lawfully accessed information where the agency has not applied for stored communications warrants. This can arise where an agency has received stored communications for purposes provided for by section 139 of the TIA Act but was not the agency that applied for the warrant.

## Which agencies may seek stored communications warrants?

5.4 Any enforcement agency may apply for a stored communications warrant. The definition of enforcement agency includes criminal law enforcement agencies, civil penalty enforcement agencies or public revenue agencies. This includes all the bodies mentioned as interception agencies and eligible authorities for the purposes of telecommunications interception warrants, as well as other regulatory bodies such as the Australian Customs Service, the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, the Australian Taxation Office and Centrelink.

# **Applications for stored communications warrants**

- 5.5 Paragraphs 162(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting year for each agency and in total. This information is presented in Table 47. Only those enforcement agencies that applied for stored communications warrants during the reporting period are included in the table.
- 5.6 The stored communications warrant regime commenced on 13 June 2006, however, no stored communications were applied for or issued during the 18 days that the regime was in force prior to 1 July 2006. Accordingly, comparative information is only available from the previous reporting period.
- 5.7 There was a 108.9% increase in the use of stored communications warrants in the reporting period which was anticipated as more agencies utilised the provisions in the second year.

Table 47—Applications for stored communications warrants

AGENCY	RELEVANT	APPLICATIONS FOR WARRANTS		
	STATISTICS	06/07	07/08	
	Made	12	13	
AUSTRALIAN FEDERAL POLICE	Refused/withdrawn	0	0	
	Issued	12	13	
	Made	4	12	
AUSTRALIAN CRIME COMMISSION	Refused/withdrawn	0	0	
COMMISSION	Issued	4	12	
	Made	1	1	
AUSTRALIAN CUSTOMS SERVICE	Refused/withdrawn	0	0	
	Issued	1	1	
	Made	-	1	
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	Refused/withdrawn	-	0	
TITVESTIVIENTS COMMISSION	Issued	-	1	
	Made	1	0	
CORRUPTION AND CRIME COMMISSION	Refused/withdrawn	0	0	
00	Issued	1	0	

AGENCY	RELEVANT	APPLICATIONS FOR WARRANTS		
	STATISTICS	06/07	07/08	
	Made	4	1	
NEW SOUTH WALES CRIME COMMISSION	Refused/withdrawn	0	0	
COMMISSION	Issued	4	1	
	Made	24 <sup>12</sup>	27	
NEW SOUTH WALES POLICE	Refused/withdrawn	0	0	
	Issued	24 <sup>13</sup>	27	
	Made	-	6	
NORTHERN TERRITORY POLICE	Refused/withdrawn	-	0	
	Issued	-	6	
	Made	-	3	
POLICE INTEGRITY COMMISSION	Refused/withdrawn	-	0	
COMMISSION	Issued	-	3	
	Made	1	27	
QUEENSLAND POLICE	Refused/withdrawn	1	0	
	Issued	0	27	
	Made	3	1	
SOUTH AUSTRALIA POLICE	Refused/withdrawn	0	0	
	Issued	3	1	
	Made	1	8	
TASMANIA POLICE	Refused/withdrawn	0	0	
	Issued	1	8	
	Made	6	5	
VICTORIA POLICE	Refused/withdrawn	0	0	
	Issued	6	5	
	Made	-	12	
WESTERN AUSTRALIA POLICE	Refused/withdrawn	-	0	
	Issued	-	12	
	Made	57	117	
TOTAL [paragraph 162(2)(a)]	Refused/withdrawn	1	0	
	Issued	56	117	

Telephone applications for stored communications warrants

5.8 Paragraphs 162(1)(b) and (2)(b) of the TIA Act provide that the report must set out how many telephone applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and in total. There were no telephone applications for stored communications warrants applied for during the reporting period.

<sup>&</sup>lt;sup>12</sup> The number of applications for stored communications warrants made by the NSW Police Force in 2006-07 was incorrectly recorded as 24 in the last annual report. The correct number should be 23.

Renewal applications for stored communications warrants

5.9 Paragraph 162(2)(c) of the TIA Act provides that the report must set out how many renewal applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and in total. There were no renewal warrants issued for stored communications.

Stored communications warrants subject to conditions or restrictions

5.10 Paragraph 162(2)(d) of the TIA Act provides that the report must set out how many stored communications warrants issued on application made during the reporting period specified conditions or restrictions, for each agency and in total. No stored communications warrants specified conditions or restrictions during the reporting period.

## **Effectiveness of stored communications warrants**

The number of arrests, proceedings and convictions made during the reporting period based on lawfully accessed information

5.11 Section 163 of the TIA Act provides that the report must set out the number of arrests made on the basis of lawfully accessed information and the number of proceedings in which lawfully accessed information was given in evidence. This information is set out in Table 48. The table also includes the number of convictions recorded based on lawfully accessed information.

Table 48—Number of arrests, proceedings and convictions made on the basis of lawfully accessed information

AGENCY	ARRESTS		PROCEEDINGS		CONVICTIONS	
	06/07	07/08	06/07	07/08	06/07	07/08
NEW SOUTH WALES CRIME COMMISSION	6	0	0	0	0	0
NEW SOUTH WALES POLICE	13	7	1	1	1	1
QUEENSLAND POLICE	-	36	-	0	-	0
SOUTH AUSTRALIA POLICE	2	0	0	0	0	0
TASMANIA POLICE	2	0	0	0	0	0
VICTORIA POLICE	0	3	1	0	1	0
TOTAL	23	45	2	1	2	1

Interpretative note relating to prosecutions and convictions statistics

5.12 Many enforcement agencies do not have prosecutions and convictions as a primary aim. The anti-corruption and integrity bodies and the non-police regulatory agencies have a range of statutory powers available to them, with the result that an investigation does not necessarily require a prosecution and conviction to be considered successful. It should also be noted that stored communications warrants will usually authorise access to less information than can be obtained under a telecommunications interception warrant, meaning that multiple stored communications warrants may often be obtained as part of a single investigation.

# CHAPTER 6—TELECOMMUNICATIONS DATA - INFORMATION REQUIRED UNDER THE ACT

## The information required

- 6.1 The reporting requirements of the TIA Act in relation to authorising the disclosure of telecommunications data are contained in Part 4-2 of the Act. Part 4-2 provides that this report must include information on:
  - the number of authorisations made under section 178
     (paragraph 186(1)(a))
  - the number of authorisations made under section 179 (paragraph 186(1)(b))
  - for criminal law-enforcement agencies the number of authorisations made under section 180 (paragraph 186(1)(c)), and
  - any other matter requested by the Minister in relation to those authorisations (paragraph 186(1)(d)).

# Which agencies may authorise the disclosure of telecommunications data?

- 6.2 Agencies whose legislation enables them to enforce a criminal law, impose pecuniary penalties or protect the public revenue are deemed to be enforcement agencies.
- 6.3 Enforcement agencies notify the Communications Access Coordinator of the positions which can authorise the disclosure of telecommunications data.

## **Authorisations granted**

- 6.4 The telecommunications data regime was transferred to the TIA Act on 1 November 2007. Therefore, statistics were sought from agencies for authorisations made from that date.
- 6.5 The number of authorisations made for access to existing information or documents in the enforcement of the criminal law is given at Table 49. The number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue is given in Table 50.

Table 49—Number of authorisations made for access to existing information or documents in the enforcement of the criminal law

AGENCY	AUTHORISATIONS
	07/08
AUSTRALIAN FEDERAL POLICE	12996
AUSTRALIAN CRIME COMMISSION	5639
AUSTRALIAN CUSTOMS SERVICE	2022
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	1076
AUSTRALIAN TAX OFFICE	17
AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY	5
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	2
CORRUPTION AND CRIME COMMISSION	265
INDEPENDENT COMMISSION AGAINST CORRUPTION	199
NEW SOUTH WALES CRIME COMMISSION	3011
NEW SOUTH WALES POLICE	88368
NORTHERN TERRITORY POLICE	979
OFFICE OF POLICE INTEGRITY	1001
POLICE INTEGRITY COMMISSION	2048
QUEENSLAND POLICE	4529
QUEENSLAND CRIME AND MISCONDUCT COMMISSION	5716
SOUTH AUSTRALIA POLICE	7852
VICTORIA POLICE	46643
WESTERN AUSTRALIA POLICE	275
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	3
DEPARTMENT OF CONSUMER AND EMPLOYMENT PROTECTION WA	217
DEPARTMENT OF DEFENCE	13

AGENCY	AUTHORISATIONS
	07/08
DEPARTMENT OF ENVIRONMENT AND CLIMATE CHANGE NSW	19
DEPARTMENT OF PRIMARY INDUSTRIES VIC	191
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS VIC	8
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS QLD	2
TRANSPORT ACCIDENT COMMISSION	3
TOTAL	183,099

Table 50 – Number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue

AGENCY	AUTHORISATIONS 07/08
AUSTRALIAN FEDERAL POLICE	481
AUSTRALIAN CUSTOMS SERVICE	1526
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	111
AUSTRALIAN TAX OFFICE	1407
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	29
CENTRELINK	2
INDEPENDENT COMMISSION AGAINST CORRUPTION	82
NORTHERN TERRITORY POLICE	14
QUEENSLAND POLICE	1
ACT REVENUE OFFICE	7
AUSTRALIAN BUILDING AND CONSTRUCTION COMMISSIONER	13
AUSTRALIAN POSTAL CORPORATION	229
CHILD SUPPORT AGENCY	532

CONSUMER AFFAIRS VICTORIA	328
CONSUMER AFFAIRS AND FAIR TRADING TASMANIA	3
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	22
DEPARTMENT OF CONSUMER AND EMPLOYMENT PROTECTION WA	10
DEPARTMENT OF DEFENCE	44
DEPARTMENT OF SUSTAINABILITY AND ENVIRONMENT VIC	105
HEALTH CARE COMPLAINTS COMMISSION NSW	1
NSW DEPARTMENT OF PRIMARY INDUSTRIES	33
OFFICE OF FAIR TRADING – DEPARTMENT OF COMMERCE NSW	439
OFFICE OF STATE REVENUE QLD	1
OFFICE OF CONSUMER AND BUSINESS AFFAIRS SA	51
QLD ENVIRONMENTAL PROTECTION AGENCY	15
REVENUE SA	53
STATE REVENUE OFFICE VIC	68
TERRITORY REVENUE OFFICE	1
WORKCOVER QLD	41
TOTAL	5649

The number of authorisations made by a criminal law-enforcement agency for access to specified information or documents that come into existence during the period for which the authorisations is in force is given in Table 51. The table also outlines the number of days the authorisations were specified in force, and for how many days they were in force. The number of authorisations still in force at the end of the reporting period is also given.

**Table 51 – Prospective authorisations** 

AGENCY	NUMBER OF AUTHORISATIONS MADE	DAYS SPECIFIED IN FORCE	ACTUAL DAYS IN FORCE	AUTHORISATIONS DISCOUNTED
AUSTRALIAN FEDERAL POLICE	68	2164	927	8
AUSTRALIAN CRIME COMMISSION	37	1481	1019	2
NEW SOUTH WALES CRIME COMMISSION	330	6590	4959	29
NEW SOUTH WALES POLICE	196	5452	3220	11
NORTHERN TERRITORY POLICE	81	3577	2955	26
POLICE INTEGRITY COMMISSION	79	2994	1966	20
SOUTH AUSTRALIA POLICE	45	1290	723	1
TASMANIA POLICE	26	985	455	0
VICTORIA POLICE	214	4896	2500	11
WESTERN AUSTRALIA POLICE	113	4747	1778	4
OFFICE OF POLICE INTEGRITY	54	2147	1824	1
QUEENSLAND CRIME AND MISCONDUCT COMMISSION	11	44	44	0
QUEENSLAND POLICE	61	1326	867	10
TOTAL	1315	37,693	23,237	123

<sup>6.7</sup> Information is also given about the average number of days the authorisations were specified in force, and the average actual number of days they remained in force. This information is presented at Table 52.

Table 52 – Average specified and actual time in force

AGENCY	AVERAGE PERIOD SPECIFIED	AVERAGE PERIOD ACTUAL
AUSTRALIAN FEDERAL POLICE	31.82	15.45
AUSTRALIAN CRIME COMMISSION	40.03	29.11
NEW SOUTH WALES CRIME COMMISSION	19.97	16.47
NEW SOUTH WALES POLICE	27.82	17.40
NORTHERN TERRITORY POLICE	44.16	53.73
POLICE INTEGRITY COMMISSION	37.89	33.32
SOUTH AUSTRALIA POLICE	28.66	16.43
TASMANIA POLICE	37.88	17.5
VICTORIA POLICE	22.87	12.31
WESTERN AUSTRALIA POLICE	42.00	16.31
OFFICE OF POLICE INTEGRITY	39.75	34.41
QUEENSLAND CRIME AND MISCONDUCT COMMISSION	4	4
QUEENSLAND POLICE	21.73	17
TOTAL	28.66	19.49