Telecommunications (Interception and Access) Act 1979

Report for the year ending 30 June 2011

ISBN: 978-1-921725-95-1

Contact us

Inquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Telephone: (02) 6141 6666
copyright@ag.gov.au

CONTENTS

LIST OF TABLES

ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
ASIC	Australian Securities and Investments Commission
Blunn Report	Report of the *Review of the Regulation of Access to Communications*
CAC	Communications Access Co-ordinator
CCC	Corruption and Crime Commission (Western Australia)
CMC	Crime and Misconduct Commission (Queensland)
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)
Qld Police	Queensland Police Service
SA Police	South Australia Police
Tas Police	Tasmania Police
Vic Police	Victoria Police
WA Police	Western Australia Police
2008 Amendment Act	*Telecommunications Interception Legislation 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 twenty-third Annual Report on the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This report relates to the period from 1 July 2010 to 30 June 2011.

1.2 In this report:

- Chapter 2 outlines of the objectives and structure of the TIA Act
- Chapter 3 outlines relevant developments to the legislation and cases impacting on its interpretation
- Chapter 4 provides information about the use of interception powers
- Chapter 5 provides information about the use of powers enabling access to stored communications, and
- Chapter 6 provides information about the of use powers enabling access to 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
- a description of the provisions that are most relevant to the contents of this report, and
- an outline of the accountability provisions.

Objectives of the legislation

2.2 The TIA Act has two key purposes:

(i) to protect the privacy of individuals who use the Australian telecommunications system, and

(ii) to specify the circumstances in which it is lawful to intercept, and access communications or authorise the disclosure of telecommunications data.

2.3 The TIA Act achieves these outcomes by:

- prohibiting the listening to or recording of communications
- prohibiting access to stored communications
- establishing a warrant scheme to enable access to communications to assist in the investigation of serious offences and serious contraventions, and
- establishing processes to enable access to telecommunications data to assist in the enforcement of the criminal law, laws imposing criminal penalties and laws aimed at protecting public revenue.

Provisions relevant to this report

2.4 Section 7 of the TIA Act prohibits the interception of a communication in its passage over the Australian telecommunications network.

2.5 Section 6 defines an 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 Section 108 of the TIA Act prohibits access to stored communications. Stored communications are:

(a) communications which have passed over the telecommunications system, and

(b) are accessed with the assistance of a telecommunications carrier without the knowledge of one of the parties to the communication.

Examples of stored communications include voice mail, e-mails and SMS messages.

2.7 Access to telecommunications data is prohibited under the *Telecommunications Act 1997*. Telecommunications data is not defined but can include information such as subscriber details and the date, time, and location of a communication. Telecommunications data does not include the content or substance of the communication.

2.8 The main exceptions to these prohibitions are the interception or access of communications under a warrant or the disclosure of telecommunications data under an authorisation in accordance with the TIA Act.

2.9 Accordingly, the TIA Act also 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 provides that a telecommunications interception warrant may be sought by an interception agency 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
- serious drug offences
- terrorism offences
- offences punishable by at least 7 years imprisonment that involve conduct such as:
  - risk of loss of a person life, serious personal injury, serious property damage endangering personal safety
  - serious arson
  - bribery or corruption, and
  - tax evasion, fraud, loss of revenue to the Commonwealth.
- offences relating to people smuggling, slavery sexual servitude, deceptive recruiting and trafficking in persons
- sexual offences against children and offences involving child pornography

- money laundering offences, cybercrime offences, serious cartel offences
- offences involving organised crime, and
- ancillary offences, such as aiding, abetting and conspiring to commit serious offences.

Applying for telecommunications interception warrants

2.12 Applications for telecommunications interception warrants may only be made by an interception agency.

2.13 During the reporting period, the term 'interception agency' included:

- the ACC
- the ACLEI
- the AFP, and
- an 'eligible authority' of a State or the Northern Territory which was the subject of a declaration under section 34 of the TIA Act.

2.14 During the reporting period, the following eligible authorities were the subject of a declaration pursuant to section 34 of the TIA Act and 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	24 March 2004
Tasmania Police	5 February 2005
Northern Territory Police	25 October 2006
Office of Police Integrity Victoria	18 December 2006
Queensland Police Service	8 July 2009
Queensland Crime and Misconduct Commission	8 July 2009

Eligible Judges and nominated AAT members

2.15 The TIA Act provides that an eligible Judge or nominated AAT member may issue a telecommunications interception warrant on application by an agency.

2.16 An ‘eligible Judge’ is a Judge who has consented in writing and been declared by the Attorney-General to be an eligible Judge. In the reporting period, eligible Judges included members of:

- the Federal Court of Australia
- the Family Court of Australia, and
- the Federal Magistrates Court.

2.17 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.

2.18 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

2.19 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.

2.20 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.

2.21 The TIA Act requires that an application contain the name of the agency and person making the application. An application must be supported by an affidavit which contains 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

2.22 An issuing authority must consider the following matters before issuing a telecommunications interception warrant:

- privacy of any person or persons would be likely to be interfered with
- gravity of the offence
- how much the information likely to be obtained would assist the investigation
- the availability of alternative methods of investigation
- how much the use of the methods would assist the investigation, and
- how much the use of such methods would prejudice the investigation by the agency, whether because of delay or for any other reason.

2.23 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 relating to the telecommunications interception regime

2.24 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.

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

2.25 Sections 57, 59A and 94 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.

Reports by carrier

2.26 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.

General Register of telecommunications interception warrants

2.27 Section 81A of the TIA Act requires the Secretary of the Attorney-General's Department to maintain a General Register which includes particulars of all telecommunications interception warrants.

2.28 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.

2.29 Interception agencies are notified once the Attorney-General has inspected the General Register to enable the destruction of restricted records in accordance with section 79 of the TIA Act.

Special Register of telecommunications interception warrants

2.30 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 to a prosecution within three months of the expiry of the warrant. The Special Register is delivered to the Attorney-General for inspection together with the General Register.

Destruction of records

2.31 Section 79 of the TIA Act provides that agencies must destroy restricted records which are original records. Once the chief officer of the agency is satisfied that the record will not be needed for any permitted purpose and the Attorney-General has inspected the relevant Register, those records must be destroyed.

Independent oversight

2.32 The ACC, ACLEI and the AFP are required to maintain records relating to interceptions and the use, dissemination and destruction of intercepted information. These records must be inspected by the Commonwealth Ombudsman on a regular basis.

2.33 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.

2.34 Parallel requirements are imposed by State and Territory legislation on State and Territory interception agencies.

2.35 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.[1] 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.

2.36 Accordingly, all law enforcement agencies capable of applying for telecommunications interception warrants operate under equivalent provisions. This means that the TIA Act imposes a national scheme in relation to telecommunications interception.

Annual Report tabled by Attorney-General

2.37 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.

[1] Instead of the State Ombudsman, inspection of the SA Police is undertaken by the Police Complaints Authority (South Australia), while inspections of the Vic Police and the OPI are undertaken by the Special Investigations Monitor (Victoria).

Stored communications warrants

Offences for which stored communications warrants may be obtained

2.38 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.

Applying for a stored communications warrant

2.39 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

2.40 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.

2.41 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.

2.42 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 Section 6DB also defines an issuing authority as a person who is a Deputy President, senior member or a member of the AAT who has been appointed by the Attorney-General.

2.44 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 applications

2.45 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.

2.46 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.

2.47 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.

Matters to be considered by an issuing authority

2.48 Before issuing a stored communications warrant, an issuing authority must consider the following matters:

- privacy of any person or persons would be likely to be interfered with
- the gravity of the conduct constituting the serious contravention
- how much information would be likely to assist the investigation
- the availability of alternative investigative methods
- how much the use of such methods would assist the investigation, and
- how much the use of such methods would prejudice the investigation by the agency, whether because of delay or for any other reason.

Safeguards and controls relating to the stored communications regime

2.49 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

2.50 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.

Destruction of records

2.51 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.

Inspections

2.52 The TIA Act provides that the Commonwealth Ombudsman must conduct regular inspections of records and report to the Attorney-General on the results of those inspections.

Annual report tabled by Attorney-General

2.53 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

2.54 Part 4-1 of the TIA Act enables enforcement agencies to authorise the disclosure of telecommunications data.

2.55 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.

2.56 Sections 174 – 180 allow for the authorisation of the release of telecommunications data under certain circumstances.

Historical data

2.57 Historical data is information which existed before an authorisation for disclosure was received. It does not include information which comes into existence after the authorisation was received.

2.58 The disclosure of historical or existing data may be authorised by an enforcement agency when it is considered reasonably necessary:

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

Prospective data

2.59 Prospective data is data that comes into existence during the period the authorisation is in force.

2.60 The disclosure of prospective data may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years.

2.61 A criminal law enforcement agency is defined as meaning all interception agencies and any other agency prescribed by the Attorney-General. During the reporting period, the ACBPS was the only body prescribed.

2.62 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. The authorisation must end at a specified time no longer than 45 days from the day the authorisation is made, unless it is revoked earlier.

Who may authorise historical and prospective telecommunications data authorisations

2.63 The disclosure of telecommunications data may only be approved by an authorised officer of the relevant enforcement agency. An authorised officer includes:

- the head (however described) or a person acting as that head
- deputy head (however described) or a person acting as that deputy head, or
- a person who holds or is acting in an office or position covered by an authorisation in force under subsection 5AB(1) of the TIA Act.

Forms of application

2.64 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 CAC. The requirements for an authorisation include:

- the identity of the agency
- the basis on which the agency is an enforcement agency or criminal law-enforcement 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
- 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
- authorisations for prospective access must also include
  - 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
  - that the officer had regard the impact on privacy
  - that any impact on privacy was outweighed by the seriousness of the conduct being investigated, and
  - the date on which the authorisation is due to end.

Safeguards and controls relating to the telecommunications data regime

Recordkeeping and inspections

2.65 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

2.66 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.

Recent legislative and policy developments

Corporations Amendment (No. 1) Act 2010

3.2 Insider trading and market manipulation causes serious harm to the fair and efficient functioning of Australia's financial markets. These types of offences are difficult to investigate as they often involve complex networks of people, technological sophistication and avoidance of paper and traceable communications. In addition, telephone conversations are often the only evidence of the offence.

3.3 The *Corporations Amendment Act 2010* amended the TIA Act to enable an interception agency (such as the AFP) to apply for a telecommunications interception warrant to assist in the investigation of serious insider trading and market manipulation offences.

Crimes Legislation Amendment Act 2011

3.4 The TIA Act prohibits the use of information obtained under a telecommunications interception warrant. An exception to this prohibition is the ability to use intercepted information for defined permitted purposes.

3.5 A 'permitted purpose' for the ACC includes the ability to be able to use intercepted information in proceedings related to the alleged misbehaviour or alleged improper conduct of an ACC officer. However, that purpose does not extend to enable the use of information in internal investigations.

3.6 Accordingly, the *Crimes Legislation Amendment Act 2010* amended the definition of permitted purpose in the TIA Act to enable the ACC to use intercepted information in their investigations of serious misconduct. The provisions only enable the ACC to use information obtained under telecommunications interception warrants, they do not enable the ACC to apply for an interception warrant to assist in the investigation of misconduct unless that conduct is a serious offence.

3.7 These amendments ensure that the TIA Act applies to the ACC in the same was as it applies to the AFP officers.

Telecommunications Interception and Intelligence Services Legislation Amendment Act 2010

3.8 The *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2010* (TIISLA) amended the TIA Act to remove legislative barriers to interoperability between national security and law enforcement agencies and enhanced their ability to share information. These amendments enable the Australian Security Intelligence Organisation (the Organisation) to provide technical assistance in relation to telecommunications interception warrants which assists to ensure that interception remains an effective investigation tool.

3.9 The TIISLA amended the TIA Act to place obligations on the telecommunications industry to provide assistance to interception agencies. Carriers and carriage service providers are now required to provide notice of changes to business plans that may impact on their ability to meet their obligations under the TIA Act and the *Telecommunications Act 1997*.

3.10 The TIISLA enacted provisions enabling law enforcement agencies to access telecommunications data to assist in the location of missing persons. The amendments ensure that where police are performing functions in relation to protecting public safety, vital information can be obtained to assist them to locate a person. Any information obtained will not be able to be used further and the provisions limit the authority of police to disclose telecommunications data to the person making a missing person's report.

3.11 The TIISLA also enacted provisions enabling law enforcement agencies to apply for stored communications warrants in their investigations of serious contraventions. These amendments were necessary to enable law enforcement agencies to have access to vital information that may be stored on a victims account in circumstances where the victim was unable to consent to that access, for example, because they are missing, incapacitated or deceased.

Recent case law

Wainohu v New South Wales [2011] HCA 24 (23 June 2011)

3.12 In this case the High Court of Australia considered the validity of the *Crimes (Criminal Organisations Control) Act 2009 NSW* (the NSW Act). The NSW Act enabled an eligible judge of the Supreme Court to 'declare' an 'organisation' on the basis of its involvement in serious criminal activity. The effect of a declaration was to enabled a Supreme Court to make control orders against the organisation's members, for example prohibiting members from associating with another 'controlled member'. The High Court held (by a majority of 6 to 1) that the provisions establishing the process of declaring an organisation were invalid as it did not require the judge to provide reasons. The Court held that the lack of this requirement was incompatible with the exercise of judicial power. Given that the ability to declare an organisation was fundamental to the remaining provisions, the entire Act was held to be invalid.

3.13 The flow through effect of the case is that law enforcement will be unable to obtain a telecommunications interception warrant to assist in the investigation of declared criminal organisations until the NSW Act is amended to cure the invalidity or new legislation is enacted.

R v Mark William Standen 2009/8922 (21 March 2011)

3.14 In this case, the Supreme Court of New South Wales upheld an application by Fairfax Media to obtain recordings of conversations acquired under telecommunications interception warrants. The procedure adopted by the court was for the prosecution to provide the electronic or documentary copies of the intercept evidence to the Court's Information Officer after that evidence had been adduced in open court during the trial.

3.15 In coming to this decision, Justice James referred to cases establishing that section 74 impliedly authorised publication by the media of evidence given in accordance with section 74. Justice James also referred to *Fairfax Publications Pty Limited v District Court of New South Wales* (2004) 61 NSWLR 334 in which Spieglman CJ held:

> 'The entitlement of the media to report on court proceedings is a corollary right of access by the members of the public. Nothing should be done to discourage fair and accurate reporting of proceedings'.

3.16 Accordingly, this case supports the publication of evidence obtained under the TIA Act once it has been given in court.

Previous Annual Report

3.17 The Annual Report for the year ending 30 June 2010 was tabled in Parliament on 23 March 2011.

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)
- Crime and Misconduct Commission (Queensland)
- 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)
- Queensland Police Service
- 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 During the reporting period, 3,488 warrants were issued to law enforcement agencies under Part 2-5 of the TIA Act. The total number of warrants issued decreased by approximately 2.5% on the total number of warrants issued during the previous reporting period. Fluctuations in the number of warrants issued over the past three reporting periods are consistent with operational practices. This information is presented in Table 1.

Table 1 – Applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
ACC	Made Refused/withdrawn Issued	154 - 154	210 - 210	190 - 190
ACLEI	Made Refused/withdrawn Issued	- - -	1 - 1	4 - 4
AFP	Made Refused/withdrawn Issued	573 1 572	642 1 641	523 - 523
CCC	Made Refused/withdrawn Issued	49 - 49	40 - 40	35 - 35
CMC	Made Refused/withdrawn Issued	- - -	18 - 18	25 - 25
ICAC	Made Refused/withdrawn Issued	32 - 32	14 - 14	12 - 12
NSW CC	Made Refused/withdrawn Issued	622 3 619	368 1 367	410 3 407
NSW POLICE	Made Refused/withdrawn Issued	838 7 831	1,142 1 1,141	1,282 3 1,279
NT POLICE	Made Refused/withdrawn Issued	47 2 45	50 - 50	46 - 46
OPI	Made Refused/withdrawn Issued	65 - 65	36 - 36	45 - 45
PIC	Made Refused/withdrawn Issued	115 - 115	48 - 48	63 - 63
QLD POLICE	Made Refused/withdrawn Issued	- - -	173 1 172	177 - 177
SA POLICE	Made Refused/withdrawn Issued	105 - 105	113 - 113	107 - 107
TAS POLICE	Made Refused/withdrawn Issued	15 - 15	21 1 20	27 - 27
VIC POLICE	Made Refused/withdrawn Issued	331 - 331	388 - 388	317 - 317
WA POLICE	Made Refused/withdrawn Issued	287 - 287	325 - 325	232 1 231
TOTAL [paragraph 100(2)(a)]	**Made** **Refused/withdrawn** **Issued**	**3,233** **13** **3,220**	**3,589** **5** **3,584**	**3,495** **7** **3,488**

Telephone applications for telecommunications interception warrants

4.6 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.

4.7 The total number of telephone applications made in the reporting period has increased by approximately 9% on the total number of telephone applications made during the previous reporting period.

Table 2—Telephone applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	TELEPHONE APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
AFP	Made Refused/withdrawn Issued	2 - 2	5 - 5	- - -
NSW POLICE	Made Refused/withdrawn Issued	22 - 22	38 - 38	50 - 50
TAS POLICE	Made Refused/withdrawn Issued	1 - 1	- - -	- - -
VIC POLICE	Made Refused/withdrawn Issued	16 - 16	23 - 23	21 - 21
WA POLICE	Made Refused/withdrawn Issued	2 - 2	1 - 1	2 - 2
TOTAL [paragraph 100(2)(b)]	**Made** **Refused/withdrawn** **Issued**	**43** **-** **43**	**67** **-** **67**	**73** **-** **73**

Renewal applications for telecommunications interception warrants

4.8 Agencies may apply for a new warrant in respect of a service or person while an existing warrant is still in force – this is known as a renewal warrant. 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.

4.9 The number of renewal applications increased by approximately 5% in comparison with the number of renewal applications made in the previous reporting period.

Table 3— Renewal applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	RENEWAL APPLICATIONS		
		08/09	09/10	10/11
ACC	Made Refused/withdrawn Issued	37 - 37	50 - 50	44 - 44
AFP	Made Refused/withdrawn Issued	112 - 112	220 - 220	173 - 173
CCC	Made Refused/withdrawn Issued	12 - 12	7 - 7	6 - 6
CMC	Made Refused/withdrawn Issued	- - -	3 - 3	1 - 1
ICAC	Made Refused/withdrawn Issued	2 - 2	3 - 3	1 - 1
NSW CC	Made Refused/withdrawn Issued	70 - 70	42 - 42	85 - 85
NSW POLICE	Made Refused/withdrawn Issued	104 - 104	169 - 169	242 - 242
NT POLICE	Made Refused/withdrawn Issued	4 - 4	5 - 5	1 - 1
OPI	Made Refused/withdrawn Issued	2 - 2	11 - 11	4 - 4
PIC	Made Refused/withdrawn Issued	30 - 30	25 - 25	19 - 19
QLD POLICE	Made Refused/withdrawn Issued	- - -	14 - 14	16 - 16
SA POLICE	Made Refused/withdrawn Issued	3 - 3	1 - 1	3 - 3
TAS POLICE	Made Refused/withdrawn Issued	- - -	5 - 5	7 - 7
VIC POLICE	Made Refused/withdrawn Issued	43 - 43	56 - 56	49 - 49
WA POLICE	Made Refused/withdrawn Issued	51 - 51	45 - 45	37 - 37
TOTAL [paragraph 100(2)(c)]	**Made** **Refused/withdrawn** **Issued**	**470** **-** **470**	**656** **-** **656**	**688** **-** **688**

Applications for telecommunications interception warrants authorising entry onto premises

4.10 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.

4.11 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		
		08/09	09/10	10/11
AFP	Made	7	1	-
	Refused/withdrawn	-	-	-
	Issued	7	1	-
CCC	Made	2	2	-
	Refused/withdrawn	-	-	-
	Issued	2	2	-
NSW CC	Made	5	-	-
	Refused/withdrawn	-	-	-
	Issued	5	-	-
PIC	Made	3	1	2
	Refused/withdrawn	-	-	-
	Issued	3	1	2
TOTAL [paragraph 100(2)(d)]	**Made**	**17**	**4**	**2**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**17**	**4**	**2**

Telecommunications interception warrants issued with specific conditions or restrictions

4.12 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.

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

AGENCY	WARRANTS ISSUED WITH CONDITIONS OR RESTRICTIONS		
	08/09	09/10	10/11
ACC	-	-	3
AFP	5	2	2
ICAC	2	-	-
NSW CC	10	-	-
NSW POLICE	4	4	6
PIC	-	1	1
TAS POLICE	3	-	-
TOTAL [paragraph 100(2)(e)]	**24**	**7**	**12**

Named person warrants

4.13 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.

4.14 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 approximately 14% from the number of warrants issued in the previous reporting period. The number of renewal applications for named person warrants increased by approximately 14% from the previous reporting period. No named person warrants authorised entry onto premises during the reporting period.

Interpretative note relating to named person warrants

4.15 The increase in named person warrants is consistent with operational fluctuations. This demonstrates the high impact on privacy that named person warrants have, and that agencies only use them when necessary and other alternative methods are not available. 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 STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS		
		08/09	09/10	10/11
ACC	Made Refused/withdrawn Issued	103 - 103	103 - 103	115 - 115
AFP	Made Refused/withdrawn Issued	113 - 113	155 - 155	191 - 191
CCC	Made Refused/withdrawn Issued	2 - 2	3 - 3	1 - 1
CMC	Made Refused/withdrawn Issued	- - -	8 - 8	6 - 6
ICAC	Made Refused/withdrawn Issued	1 - 1	2 - 2	- - -
NSW POLICE	Made Refused/withdrawn Issued	28 - 28	25 - 25	41 - 41
NSW CC	Made Refused/withdrawn Issued	60 1 59	48 - 48	75 1 74
NT POLICE	Made Refused/withdrawn Issued	7 - 7	10 - 10	5 - 5
OPI	Made Refused/withdrawn Issued	10 - 10	- - -	8 - 8
PIC	Made Refused/withdrawn Issued	4 - 4	2 - 2	2 - 2
QLD POLICE	Made Refused/withdrawn Issued	- - -	26 - 26	29 - 29
SA POLICE	Made Refused/withdrawn Issued	6 - 6	27 - 27	21 - 21
TAS POLICE	Made Refused/withdrawn Issued	1 - 1	1 - 1	- - -
VIC POLICE	Made Refused/withdrawn Issued	66 - 66	87 - 87	81 - 81
WA POLICE	Made Refused/withdrawn Issued	33 - 33	53 - 53	54 - 54
TOTAL [paragraph 100(ea)]	**Made** **Refused/withdrawn** **Issued**	**434** **1** **433**	**550** **-** **550**	**629** **1** **628**

Table 7—Telephone applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
VIC POLICE	Made	4	2	1
	Refused/withdrawn	-	-	-
	Issued	4	2	1
TOTAL [paragraph 100(ed)]	**Made**	**4**	**2**	**1**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**4**	**2**	**1**

Table 8—Renewal applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
ACC	Made	30	36	35
	Refused/withdrawn	-	-	-
	Issued	30	36	35
AFP	Made	40	62	79
	Refused/withdrawn	-	-	-
	Issued	40	62	79
CCC	Made	-	1	-
	Refused/withdrawn	-	-	-
	Issued	-	1	-
CMC	Made	-	2	1
	Refused/withdrawn	-	-	-
	Issued	-	2	1
ICAC	Made	-	1	-
	Refused/withdrawn	-	-	-
	Issued	-	1	-
NSW CC	Made	14	8	11
	Refused/withdrawn	-	-	-
	Issued	14	8	11
NSW POLICE	Made	13	4	10
	Refused/withdrawn	-	-	-
	Issued	13	4	10
NT POLICE	Made	3	2	1
	Refused/withdrawn	-	-	-
	Issued	3	2	1
OPI	Made	-	1	-
	Refused/withdrawn	-	-	-
	Issued	-	1	-
PIC	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
QLD POLICE	Made	-	5	5
	Refused/withdrawn	-	-	-
	Issued	-	5	5
SA POLICE	Made	2	1	-
	Refused/withdrawn	-	-	-
	Issued	2	1	-
VIC POLICE	Made	9	17	22
	Refused/withdrawn	-	-	-
	Issued	9	17	22
WA POLICE	Made	11	12	9
	Refused/withdrawn	-	-	-
	Issued	11	12	9
TOTAL [paragraph 100(ed)]	**Made**	**122**	**152**	**174**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**122**	**152**	**174**

Table 9—Named person warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS WITH CONDITIONS		
		08/09	09/10	10/11
ACC	Issued	-	-	3
AFP	Issued	1	-	-
NSW CC	Issued	1	-	2
TOTAL [paragraph 100(2)(ea)]	**Issued**	**2**	**-**	**5**

4.16 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.

4.17 This information is included in Table 10.

Table 10—Number of services intercepted under named person warrants

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		08/09	09/10	10/11
ACC	1 service only	29	19	29
	2 – 5 services	66	76	66
	6 – 10 services	8	7	15
	10+ services	-	1	1
AFP	1 service only	13	31	22
	2 – 5 services	91	96	126
	6 – 10 services	10	13	17
	10+ services	2	1	4
CCC	1 service only	-	1	-
	2 – 5 services	2	2	-
	6 – 10 services	-	-	-
	10+ services	-	-	1
CMC	1 service only	-	3	2
	2 – 5 services	-	5	4
	6 – 10 services	-	1	-
	10+ services	-	-	-
ICAC	1 service only	-	-	-
	2 – 5 services	1	2	-
	6 – 10 services	-	-	-
	10+ services	-	-	-
NSW CC	1 service only	9	9	14
	2 – 5 services	42	27	52
	6 – 10 services	8	12	6
	10+ services	-	-	1

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		08/09	09/10	10/11
NSW POLICE	1 service only	6	3	8
	2 – 5 services	20	18	25
	6 – 10 services	1	2	5
	10+ services	-	-	-
NT POLICE	1 service only	1	1	2
	2 – 5 services	5	9	3
	6 – 10 services	1	-	-
	10+ services	-	-	-
OPI	1 service only	1	-	1
	2 – 5 services	8	2	5
	6 – 10 services	1	-	2
	10+ services	-	-	0
PIC	1 service only	-	-	-
	2 – 5 services	2	2	-
	6 – 10 services	2	2	2
	10+ services	-	-	-
QLD POLICE	1 service only	-	3	5
	2 – 5 services	-	23	22
	6 – 10 services	-	-	1
	10+ services	-	-	-
SA POLICE	1 service only	3	5	7
	2 – 5 services	3	19	13
	6 – 10 services	-	2	1
	10+ services	-	-	-
TAS POLICE	1 service only	-	-	-
	2 – 5 services	1	1	-
	6 – 10 services	-	-	-
	10+ services	-	-	-
VIC POLICE	1 service only	12	9	12
	2 – 5 services	46	67	56
	6 – 10 services	8	9	12
	10+ services	-	2	2
WA POLICE	1 service only	5	11	8
	2 – 5 services	19	34	44
	6 – 10 services	5	7	2
	10+ services	3	1	-
TOTAL [paragraph 100(2)(eb)]	**1 service only**	**79**	**95**	**110**
	2 – 5 services	**306**	**383**	**416**
	6 – 10 services	**44**	**55**	**63**
	10+ services	**5**	**5**	**9**

4.18 Paragraphs 100(1)(ec) and 100(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 service based named person warrants and the number of devices intercepted under a device based named person warrant. This information is presented in Tables 11 and 12.

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

AGENCY	TOTAL NUMBER OF SERVICES INTERCEPTED		
	08/09	09/10	10/11
ACC	285	311	337
AFP	416	459	586
CCC	8	6	11
CMC	-	22	12
ICAC	2	4	-
NSW CC	209	181	212
NSW POLICE	70	75	125
NT POLICE	25	28	12
OPI	37	2	8
PIC	22	6	14
QLD POLICE	-	68	68
SA POLICE	9	78	53
TAS POLICE	3	5	-
VIC POLICE	225	296	293
WA POLICE	150	175	169
TOTAL	**1,461**	**1,716**	**1,900**

Table 12—Total number of services and devices intercepted under *device* based named person warrants

AGENCY	SERVICES			DEVICES		
	08/09	09/10	10/11	08/09	09/10	10/11
ACC	-	-	-	-	-	9
AFP	-	-	-	16	12	21
NSW POLICE	-	2	2	1	7	4
QLD POLICE	-	-	-	-	2	-
VIC POLICE	-	-	-	1	-	-
NSW CC	-	1	-	-	5	-
TOTAL	**-**	**3**	**2**	**18**	**26**	**34**

B-Party warrants

4.19 Paragraphs 100(1)(ed) of the TIA Act provides 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.

4.20 Paragraph 100(2)(ed) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 13 to 16 set out the information supplied by intercepting agencies regarding B-Party warrants. There has been a 7.5% decrease of applications for B-Party warrants since the last reporting period. This decrease can be attributed to the operational needs of agencies.

4.21 No B-Party warrants authorised entry onto premises during the reporting period.

Table 13—Applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		08/09	09/10	10/11
ACC	Made Refused/withdrawn Issued	1 - 1	- - -	2 - 2
AFP	Made Refused/withdrawn Issued	8 - 8	43 - 43	42 - 42
CCC	Made Refused/withdrawn Issued	- - -	1 - 1	4 - 4
ICAC	Made Refused/withdrawn Issued	1 - 1	- - -	- - -
NSW CC	Made Refused/withdrawn Issued	13 - 13	4 - 4	10 - 10
NSW POLICE	Made Refused/withdrawn Issued	40 - 40	38 - 38	44 - 44
OPI	Made Refused/withdrawn Issued	3 - 3	- - -	3 - 3
QLD POLICE	Made Refused/withdrawn Issued	- - -	1 - 1	1 - 1
SA POLICE	Made Refused/withdrawn Issued	2 - 2	- - -	- - -
VIC POLICE	Made Refused/withdrawn Issued	5 - 5	32 - 32	5 - 5
WA POLICE	Made Refused/withdrawn Issued	- - -	1 - 1	- - -
TOTAL [paragraph 100(2)(ed)]	**Made** **Refused/withdrawn** **Issued**	**73** **-** **73**	**120** **-** **120**	**111** **-** **111**

Table 14—Telephone applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		08/09	09/10	10/11
AFP	Made Refused/withdrawn Issued	- - -	3 - 3	**-** **-** **-**
NSW POLICE	Made Refused/withdrawn Issued	5 - 5	8 - 8	9 - 9
VIC POLICE	Made Refused/withdrawn Issued	- - -	- - -	1 - 1
TOTAL [paragraph 100(2)(ed)]	**Made** **Refused/withdrawn** **Issued**	**5** **-** **5**	**11** **-** **11**	**10** **-** **10**

Table 15—Renewal applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		08/09	09/10	10/11
AFP	Made Refused/withdrawn Issued	4 - 4	26 - 26	24 - 24
NSW POLICE	Made Refused/withdrawn Issued	2 - 2	4 - 4	5 - 5
VIC POLICE	Made Refused/withdrawn Issued	- - -	15 - 15	- - -
TOTAL [paragraph 100(2)(ed)]	**Made** **Refused/withdrawn** **Issued**	**6** **-** **6**	**45** **-** **45**	**29** **-** **29**

Table 16— B-Party warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		08/09	09/10	10/11
ICAC	Issued	1	-	-
TOTAL [paragraph 100(2)(ed)]	**Issued**	**1**	**-**	**-**

Interpretative note relating to B-Party warrants

4.22 These statistics demonstrate that B-Party warrants are only used sparingly. Of the sixteen agencies that were issued telecommunications interception warrants during the reporting period, only eleven applied for and were issued B-Party warrants, with B-Party warrants representing approximately 3% of the total number of warrants issued.

4.23 It is important to note that only 29 of the 111 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

4.24 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.

4.25 The information required by paragraphs 100(1)(f) and (g) is set out in Tables 17 to 32. As in previous years, agencies obtained the majority of warrants to assist with investigations into drug-related offences.

4.26 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 17—Categories of serious offences specified in telecommunications interception warrants issued to the ACC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
ACC special investigations	153	210	171
Serious drug offences	1	-	19
Serious fraud or loss of revenue	-	-	-

Table 18—Categories of serious offences specified in telecommunications interception warrants issued to ACLEI

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	-	1	4

Table 19—Categories of serious offences specified in telecommunications interception warrants issued to the AFP

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	1
Bribery or corruption	1	1	-
Child pornography	-	3	-
Cybercrime	3	3	12
Kidnapping	4	-	-
Money laundering	104	136	137
Murder	21	16	2
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	-	2	3
Offences involving planning and organisation	26	13	23
People smuggling or sexual servitude	19	30	10
Serious damage to property	-	-	-
Serious drug offences	282	391	443
Serious fraud or loss of revenue	12	18	12
Serious personal injury or loss of life	27	73	16
Telecommunications offences	11	17	3
Terrorism	91	141	61

Table 20—Categories of serious offences specified in telecommunications interception warrants issued to the CCC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	19	39	28
Child pornography	10	-	-
Cybercrime	27	4	-
Offences involving planning and organisation	-	-	3
Serious drug offences	11	-	12
Serious personal injury or loss of life	-	-	1

Table 21—Categories of serious offences specified in telecommunications interception warrants issued to the CMC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	-	7	9
Serious drug offences	-	11	15
Serious personal injury or loss of life	-	-	1

Table 22—Categories of serious offences specified in telecommunications interception warrants issued to the ICAC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	32	14	9
Cybercrime offences	-	-	3

Table 23—Categories of serious offences specified in telecommunications interception warrants issued to the NSW CC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	22
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	27
Cybercrime	6	-	-
Kidnapping	9	-	3
Money laundering	26	61	36
Murder	47	61	65
Offences involving planning and organisation	33	24	5
Serious drug offences	478	228	257
Serious fraud or loss of revenue	24	10	16
Serious personal injury or loss of life	16	20	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	10	15	27
Conspiring to commit or aiding or abetting the commission of a serious offence	-	2	8
Kidnapping	14	22	-
Murder	237	293	296
Offences involving planning and organisation	165	152	155
People smuggling or sexual servitude	-	-	1
Serious arson	-	9	23
Serious damage to property	30	20	15
Serious drug offences	147	389	410
Serious fraud or loss of revenue	19	46	24
Serious personal injury or loss of life	194	164	293
Terrorism	10	29	35

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Murder	3	7	4
Serious arson	-	-	1
Serious drug offences	42	43	37
Serious personal injury or loss of life	-	-	4

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	58	36	40
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	2
Murder	-	-	1
Serious drug offences	-	-	2
Serious personal injury or loss of life	7	-	

Table 27—Categories of serious offences specified in telecommunications interception warrants issued to the PIC

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	98	41	56
Money laundering	7	-	-
Serious drug offences	10	3	7
Serious personal injury or loss of life	-	4	-

Table 28—Categories of serious offences specified in telecommunications interception warrants issued to the Qld Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	11	-
Murder	-	26	31
Offences involving planning and organisation	-	7	-
Serious arson	-	1	-
Serious drug offences	-	115	127
Serious fraud or loss of revenue	-	7	-
Serious personal injury or loss of life	-	9	19

Table 29—Categories of serious offences specified in telecommunications interception warrants issued to the SA Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Administration of justice[2]	4	-	-
Bribery or corruption	-	5	6
Child Pornography	-	6	-
Conspiring to commit or aiding or abetting the commission of a serious offence	-	16	10
Cybercrime	3	-	3
Kidnapping	-	-	1
Money Laundering	-	4	2
Murder	23	17	7
Offences involving planning and organisation	-	-	2
Serious arson	1	-	-
Serious drug offences	65	90	63
Serious fraud or loss of revenue	6	1	-
Serious personal injury or loss of life	3	14	15

Table 30—Categories of serious offences specified in telecommunications interception warrants issued to Tas Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Conspiring to commit or aiding or abetting the commission of a serious offence	-	1	-
Murder	2	17	10
Serious arson	-	-	1
Serious drug offences	8	8	26
Serious personal injury of loss of life	5	-	-

[2] This refers to offences against section 131.1, 135.1, 142.1 or 142.2, subsection 148.2(3), or section 268.112 of the *Criminal Code*; or section 35, 36, 36A, 37, 39, 41, 42, 43, 46 or 47 of the *Crimes Act 1914*, as outlined in Section 5D.

Table 31—Categories of serious offences specified in telecommunications interception warrants issued to the Vic Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	28	4	8
Child pornography offences	-	-	1
Kidnapping	3	11	12
Money Laundering	-	1	-
Murder	63	113	49
Offences involving planning and organisation	-	-	1
Serious arson	2	3	3
Serious damage to property	-	-	2
Serious drug offences	170	191	154
Serious fraud or loss of revenue	-	-	4
Serious personal injury or loss of life	65	65	71
Terrorism	-	-	8

Table 32—Categories of serious offences specified in telecommunications interception warrants issued to the WA Police

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	08/09	09/10	10/11
Bribery or corruption	9	-	-
Child pornography	9	-	2
Kidnapping	8	8	-
Money laundering	1	3	-
Murder	38	34	26
Offences involving planning and organisation	2	14	11
Serious arson	-	10	-
Serious damage to property	-	1	-
Serious drug offences	177	209	168
Serious fraud or loss of revenue	11	-	2
Serious personal injury or loss of life	32	46	22

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

4.27 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 33.

Table 33—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		
	08/09	09/10	10/11
ACC special investigations[3]	153	210	171
Administration of justice[4]	4	-	-
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	11	23
Bribery or corruption	255	162	183
Child pornography	19	9	3
Conspiring to commit or aiding or abetting the commission of a serious offence	-	19	47
Cybercrime	39	7	18
Kidnapping	38	41	16
Money laundering	138	205	175
Murder	434	584	491
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	-	3	7
Offences involving planning and organisation	226	210	200
People smuggling or sexual servitude	19	30	11
Serious arson	3	13	28
Serious damage to property	30	21	17
Serious drug offences	1,391	1,678	1,222
Serious fraud or loss of revenue	72	82	58
Serious personal injury or loss of life	349	395	442
Telecommunications offences	11	17	3
Terrorism	101	170	104

Duration of telecommunications interception warrants

4.28 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 TIA 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

4.29 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

[3] Applies only to the ACC.

[4] This refers to offences against sections 35, 36, 36A, 37, 39, 41, 42, 43, 46 or 47 of the *Crimes Act 1914*

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 34.

4.30 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 34—Duration of original telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	08/09	09/10	10/11	08/09	09/10	10/11
ACC	89	86	84	62	45	83
ACLEI	-	25	90	-	25	33
AFP	73	80	66	49	54	44
CCC	90	73	72	80	64	78
CMC	-	53	72	-	48	53
ICAC	83	90	52	55	84	30
NSW CC	85	84	88	52	71	89
NSW POLICE	49	61	48	46	52	39
NT POLICE	86	86	81	66	61	64
OPI	70	55	78	44	47	61
PIC	89	90	65	76	69	53
QLD POLICE	-	40	46	-	31	39
SA POLICE	74	83	72	61	64	54
TAS POLICE	74	84	81	46	68	74
VIC POLICE	52	55	55	43	41	41
WA POLICE	62	86	86	39	48	58
AVERAGE [paragraphs 101(2)(a)-(b)]	**69**	**71**	**71**	**55**	**52**	**56**

Duration of renewal telecommunications interception warrants

4.31 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 35. There is no substantial variation in the average specified or actual durations of renewal warrants from previous reporting periods.

Table 35—Duration of renewal of telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	08/09	09/10	10/11	08/09	09/10	10/11
ACC	83	76	78	68	79	76
AFP	87	83	65	73	66	35
CCC	83	73	90	85	60[5]	58
CMC	-	65	90	-	61	41
ICAC	90	90	90	22	17	26
NSW CC	86	89[6]	85	60	68	74
NSW POLICE	55	66	61	47	64	49
NT POLICE	90	81	60	90	45	9
OPI	45	-	90	41	-	88
PIC	90	90	86	71	88	75
QLD POLICE	-	42	51	-	32	44
SA POLICE	60	90	57	60	-	18
TAS POLICE	-	90	80	-	90	73
VIC POLICE	59	59	59	52	40	19
WA POLICE	64	74	85	49	53	67
AVERAGE [paragraphs 101(2)(a)-(b)]	**74**	**75**	**75**	**56**	**63**	**50**

Interpretative note relating to average duration of warrants across all agencies

4.32 The figures in Tables 34 and 35 reflect the average durations, both specified and actual, for all original and renewal warrants issued to all agencies.

4.33 These figures illustrate that the duration of warrants is generally consistent from year to year, and that the actual duration of warrants is typically shorter than the specified duration.

Duration of original B-Party warrants

4.34 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.

[5] CCC advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[6] NSW CC advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

4.35 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 36.

Table 36—Duration of original B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	08/09	09/10	10/11	08/09	09/10	10/11
ACC	45	-	45	13	-	45
AFP	45	45	43	44	33	36
CCC	-	45	45	-	38	42
ICAC	45	-	-	45	-	-
NSW CC	42	45	45	15	32	36
NSW POLICE	27	34	29	18	25	15
OPI	34	-	45	21	-	6
QLD POLICE	-	8	3	-	8	3
SA POLICE	30	-	-	30	-	-
VIC POLICE	45	45	41	16	45	43
WA POLICE	-	14	-	-	14	-
AVERAGE [paragraph 101(2)(da)]	**34**	**34**	**37**	**21**	**28**	**28**

Duration of renewal B-Party warrants

4.36 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 37.

Table 37—Duration of renewal of B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	08/09	09/10	10/11	08/09	09/10	10/11
AFP	45	46	45	42	47	45
NSW POLICE	30	29	28	29	29	21
VIC POLICE	-	45	-	-	29	-
AVERAGE [paragraphs 101(2)(da)]	**40**	**40**	**36**	**38**	**35**	**33**

Number of final renewals of telecommunications interception warrants

4.37 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.

4.38 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 38.

4.39 The figures in Table 38 show an increase in 90 day, 150 day and 180 day renewals. There has been a significant increase in the number of 180 day renewals as a result of operational fluctuations and indicates a number of long term investigations during the reporting period.

Table 38—Number of 'final renewals'

AGENCY	90 DAYS			150 DAYS			180 DAYS		
	08/09	09/10	10/11	08/09	09/10	10/11	08/09	09/10	10/11
ACC	7	6	9	7	4	9	7	6	10
AFP	18	4	7	24	21	10	37	24	30
CCC	-	3	-	-	-	6	-	-	3
CMC	-	-	-	-	-	-	-	-	1
ICAC	2	3	1	-	-	-	-	-	-
NSW CC	6	7	9	7	4	26	2	5	23
NSW POLICE	50	74	107	6	4	8	11	5	23
NT POLICE	-	3	1	-	-	1	1	1	-
OPI	1	8	-	-	-	4	-	9	-
PIC	8	-	-	8	-	4	5	-	6
QLD POLICE	-	4	7	-	-	-	-	-	-
SA POLICE	2	-	-	1	-	-	-	-	-
TAS POLICE	-	-	-	-	-	-	-	-	3
VIC POLICE	17	24	20	2	5	1	2	2	-
WA POLICE	13	19	11	28	12	9	1	3	5
TOTAL [paragraph 101(2)(e)]	**124**	**155**	**172**	**83**	**50**	**78**	**66**	**55**	**104**

Effectiveness of telecommunications interception warrants

4.40 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.

4.41 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.

4.42 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.

4.43 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 an intercepting agency of information pointing to a matter that falls within the jurisdiction of a Parliamentary Inspector, which is defined as an eligible has not been declared to be an interception agency for the purposes of the TIA Act. In these circumstances, it may be possible for the agency to communicate the information to the Parliamentary Inspector in accordance with Part 2-6 of the TIA Act.

4.44 Eligible authorities that were not interception agencies for the purposes of the TIA Act during the reporting period are:

- 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

4.45 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.

4.46 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 39. The number of arrests made during the reporting period represents a 27% increase from the previous reporting period.

Table 39—Arrests on the basis of lawfully intercepted information

AGENCY	NUMBER OF ARRESTS		
	08/09	09/10	10/11
ACC	133	72	92
AFP	133	116	67
CCC	1	1	17
CMC	-	52	4
ICAC	-	2	-
NSW CC	175	135	124
NSW POLICE	402	429	1,070
NT POLICE	31	48	34
OPI	1	-	-
PIC	139	189	28[7]
QLD POLICE	48	268	393
SA POLICE	89	176	112
TAS POLICE	9	54	12
VIC POLICE	420	371	400
WA POLICE	134	123	88
TOTAL [paragraph 102(2)(a)]	**1,715**	**1,913**	**2,441**

[7] PIC has advised that this statistic is drawn from the number of offences on court attendance notices issued during the reporting period, as such the 28 charges related to 12 people.

Prosecutions in which lawfully intercepted information was given in evidence

4.47 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 40 to 42.

4.48 During the reporting period, there was a 3% increase in the number of prosecutions commenced, and a 7% decrease in the number of convictions obtained on the basis of lawfully intercepted information.

4.49 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 as information obtained may be used in later reporting periods.

4.50 In these tables, the category 'other offences' refers to any other offence punishable by imprisonment for life or for a period of at least three years, or to any related ancillary offences.

Table 40—Prosecutions in which lawfully intercepted information used in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC	CMC	ICAC	NSW CC	NSW POL	NT POL	OPI	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
Administration of Justice	-	-	9	-	-	-	-	-	-	-	-	-	-	3	-	**12**
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	-	-	-	3	5	-	-	-	-	-	-	16	-	**24**
Bribery or corruption	-	-	15	-	-	-	13	-	-	-	-	2	-	1	-	**31**
Child pornography	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	**1**
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	-	-	-	3	18	-	-	-	-	-	-	-	1	**22**
Cybercrime	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	**1**
Kidnapping	-	-	-	-	-	1	12	-	-	-	-	-	-	2	-	**15**
Money laundering	-	6	-	-	-	10	13	-	-	-	-	-	-	1	-	**30**
Murder	-	-	-	-	-	-	38	-	-	-	-	3	-	9	3	**53**
Offences involving planning and organisation	-	-	-	-	-	23	145	-	-	-	-	-	-	2	90	**260**
Organised crime	-	-	-	-	-	1	201	-	-	-	-	-	-	-	-	**202**
People Smuggling	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Serious arson	-	5	-	-	-	-	5	-	-	-	-	1	-	1	-	**12**
Serious damage to property	-	-	-	-	-	-	3	-	-	-	-	-	-	6	2	**11**
Serious drug offences	3	39	-	2	-	122	475	17	-	-	23	49	25	318	458	**1,531**
Serious fraud or loss of revenue	-	1	-	-	-	14	85	-	-	2	1	2	-	3	-	**108**
Serious personal injury/ loss of life	-	4	-	-	-	2	427	-	-	-	-	5	-	51	5	**494**
Special Investigation of the ACC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism	-	41	-	-	-	-	-	-	-	-	-	-	-	-	-	**41**
Other offences	9	-	9	-	1	1	191	-	1	-	21	2	-	85	-	**320**
TOTAL	**12**	**96**	**33**	**2**	**1**	**180**	**1,631**	**17**	**1**	**2**	**45**	**65**	**25**	**498**	**560**	**3,168**

Table 41—Convictions in which lawfully intercepted information given in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC	CMC	ICAC	NSW CC	NSW POL	NT POL	OPI	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
Administration of Justice	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	**5**
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	-	-	-	3	4	-	-	-	-	-	-	16	-	**23**
Bribery or corruption	-	-	15	-	-	-	5	-	-	4	-	2	-	1	-	**27**
Child pornography	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	**1**
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	-	-	-	3	16	-	-	1	-	-	-	-	-	**20**
Cybercrime	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	**1**
Kidnapping	-	-	-	-	-	1	20	-	-	-	-	-	-	2	-	**23**
Money laundering	-	-	-	-	-	9	5	-	-	-	-	-	-	1	-	**15**
Murder	-	-	-	-	-	-	31	-	-	-	-	2	-	8	-	**41**
Offences involving planning and organisation	-	-	-	-	-	20	69	-	-	-	-	-	-	2	36	**127**
Organised crime	-	-	-	-	-	1	213	-	-	-	-	-	-	-	-	**214**
Serious arson	-	-	-	-	-	-	2	-	-	-	-	1	-	1	-	**4**
Serious damage to property	-	-	-	-	-	-	3	-	-	-	-	-	-	6	1	**10**
Serious drug offences	3	9	-	-	-	104	365	8	-	1	17	47	19	304	169	**1,046**
Serious fraud or loss of revenue	-	1	-	-	-	11	100	-	-	28	1	2	-	3	-	**146**
Serious personal injury/ loss of life	-	-	-	-	-	2	103	-	-	-	-	4	-	32	2	**143**
Special Investigation of the ACC	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism	-	8	-	-	-	-	-	-	-	-	-	-	-	-	-	**8**
Other offences	6	-	6	10	1	1	42	-	1	9	20	2	-	82	-	**180**
TOTAL	**9**	**18**	**26**	**10**	**1**	**155**	**981**	**8**	**1**	**43**	**38**	**61**	**19**	**458**	**209**	**2,034**

Table 42—Prosecutions and convictions in which lawfully intercepted information given in evidence

AGENCY	CATEGORIES OF OFFENCES PROSECUTED	NUMBER OF OFFENCES PROSECUTED FOR EACH CATEGORY			NUMBER OF CONVICTIONS RECORDED FOR EACH CATEGORY		
		08/09	09/10	10/11	08/09	09/10	10/11
ACC	Serious Offence	30	76	3	23	17	3
	Other[8]	32	-	9	6	1	6
	Agency Total	62	76	12	29	18	9
AFP	Serious Offence	168	96	96	23	31	18
	Other	11	1	-	-	-	-
	Agency Total	179	97	96	23	31	18
CCC	Serious Offence	21	123	24	8	118	20
	Other	-	-	9	-	-	6
	Agency Total	21	123	33	8	118	26
CMC	Serious Offence	-	-	2	-	-	-
	Other	-	-	-	-	-	10
	Agency Total	-	-	2	-	-	10
ICAC	Serious Offence	-	3	-	-	-	-
	Other	28	-	1	8	-	1
	Agency Total	28	3	1	8	-	1
NSW CC	Serious Offence	342	385	179	246	286	154
	Other	-	-	1	-	-	1
	Agency Total	342	385	180	246	286	155
NSW POLICE	Serious Offence	1,234	1,149	1,440	774	970	936
	Other	76	46	191	59	35	42
	Agency Total	1,310	1,195	1,631	833	1,005	978
NT POLICE	Serious Offence	11	21	17	9	17	8
	Other	-	-	-	-	-	-
	Agency Total	11	21	17	9	17	8
OPI	Serious Offence	8	2	-	5	1	-
	Other	-	-	2	-	-	1
	Agency Total	8	2	2	5	1	1
PIC	Serious Offence	13	7	2	12	5	34
	Other	20	15	-	14	7	9
	Agency Total	33	22	2	26	12	43
QLD POLICE	Serious Offence	11	18	24	-	6	18
	Other	4	1	21	-	1	20
	Agency Total	15	19	45	-	7	38
SA POLICE	Serious Offence	138	44	63	46	36	59
	Other	2	4	2	7	4	2
	Agency Total	140	48	65	53	40	61
TAS POLICE	Serious Offence	9	-	25	-	-	19
	Other	-	-	-	-	-	-
	Agency Total	9	-	25	-	-	19
VIC POLICE	Serious Offence	348	403	413	342	418	376
	Other	77	90	85	76	87	82
	Agency Total	425	493	498	418	505	458
WA POLICE	Serious Offence	755	545	560	415	120	209
	Other	82	50	-	36	20	-
	Agency Total	837	595	560	451	140	209
TOTAL	**Serious Offence**	**3,088**	**2,872**	**2,848**	**1,903**	**2,025**	**1,854**
	Other	**332**	**207**	**320**	**206**	**155**	**180**
	Grand Total	**3,420**	**3,079**	**3,168**	**2,109**	**2,180**	**2,034**

[8] 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.

Interpretative note relating to prosecutions and convictions statistics

4.51 The statistics presented in Tables 40 to 42 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.

4.52 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.

Percentage of 'eligible warrants'

4.53 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.

4.54 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.[9]

4.55 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 43, and indicate an 8% increase in the proportion of eligible warrants when compared to the previous reporting period.

[9] 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.

Table 43—Percentage of 'eligible warrants'

AGENCY	NUMBER OF ELIGIBLE WARRANTS		TOTAL NUMBER OF WARRANTS		%	
	09/10	10/11	09/10	10/11	09/10	10/11
ACC	193	119	222	145	87	82
ACLEI	-	-	-	4	-	-
AFP	542	686	754	513	72	134
CCC	29	37	50	44	58	84
CMC	15	4	15	22	100	18
ICAC	7	6	7	13	100	46
NSW CC	392	342	438	496	90	69
NSW POLICE	869	1,063	1233	1,437	70	74
NT POLICE	44	39	51	46	86	84
OPI	1	15	36	47	3	32
PIC	16	21	63	70	25	30
QLD POLICE	159	165	172	193	92	85
SA POLICE	110	104	116	113	95	92
TAS POLICE	6	28	15	21	40	133
VIC POLICE	291	244	420	335	69	73
WA POLICE	105	73	307	250	34	29
TOTAL [subsection 102(4)]	**2,779**	**2,946**	**3,899**	**3,749**	**71**	**79**

Emergency interception

4.56 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 AFP 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.

4.57 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. There also must be 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
- 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.

4.58 In the reporting period no interceptions were carried out in reliance on subsection 7(4).

4.59 Interception of communications carried out pursuant to subsection 7(5) of the TIA Act must have the consent of the person to whom the communication is directed, and must satisfy the same conditions specified for subsection 7(4).

4.60 In the reporting period two interceptions were carried out in reliance on subsection 7(5). The information required by section 102A is set out in Table 44.

Table 44—Interceptions made in reliance on subsection 7(5) of the TIA Act

SUSPICION OF	NSW POLICE		
	08/09	09/10	10/11
An act that may result in loss of life or serious injury	-	2	-
Threat to kill or seriously injure	-	-	-
TOTAL	**-**	**2**	**-**

Other information

Total expenditure incurred by agencies

4.61 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 45.

4.62 Total expenditure incurred by agencies in connection with telecommunications interception increased by approximately 9% from the previous reporting period.

Table 45—Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants

AGENCY	TOTAL EXPENDITURE ($)		
	08/09	09/10	10/11
ACC	5,767,648	5,437,135	6,173,566
ACLEI	-	7,460	23,309
AFP	8,221,162	9,586,423	9,488,869
CCC	1,817,120	1,520,265	3,103,641
CMC	-	1,254,986[10]	1,557,672
ICAC	214,446	153,907	108,032
NSW CC	4,473,035	4,063,904	3,927,948
NSW POLICE	8,019,292	5,296,367	5,327,911
NT POLICE	693,458	701,485	832,000
OPI	1,671,170	2,034,841	1,244,783
PIC	1,351,587	1,141,823	1,248,984
QLD POLICE	-	3,321,572[11]	5,231,250
SA POLICE	2,656,404	2,717,562	2,688,290
TAS POLICE	3,258	416,000	502,591
VIC POLICE	4,483,582	5,531,058	5,755,955
WA POLICE	2,816,442	3,116,737	3,270,702
TOTAL	**42,188,604**	**46,301,525**	**50,462,194**

[10] This figure includes start up costs for the Crime and Misconduct Commission

[11] This figure includes start up costs for the Queensland Police Service

Average expenditure per telecommunications interception warrant

4.63 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:

$$\frac{\text{Total warrant expenditure}}{\text{Number of warrants}}$$

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.

4.64 The average expenditure incurred by agencies per warrant over the reporting period is presented in Table 46.

Table 46—Average expenditure per telecommunications interception warrant

AGENCY	AVERAGE EXPENDITURE ($)		
	08/09	09/10	10/11
ACC	37,452	25,891	32,492
ACLEI	-	7,460	5,827
AFP	14,373	14,924	18,143
CCC	37,084	38,007	88,675
CMC	-	73,823	66,307
ICAC	6,701	10,993	9,003
NSW CC	7,226	11,073	9,650
NSW POLICE	9,650	4,642	4,166
NT POLICE	15,410	14,030	18,305
OPI	25,710	56,523	27,662
PIC	11,753	23,788	19,825
QLD POLICE	-	19,311	29,555
SA POLICE	25,299	24,049	25,124
TAS POLICE	217	20,800	18,614
VIC POLICE	13,546	14,225	18,158
WA POLICE	9,813	9,590	14,159

Availability of eligible judges and nominated AAT members

4.65 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 47 and 48.

Table 47—Availability of Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT Members to issue telecommunications interception warrants[12]

ISSUING AUTHORITY	NUMBER ELIGIBLE
FEDERAL COURT JUDGES	12
FAMILY COURT JUDGES	12
FEDERAL MAGISTRATES	39
NOMINATED AAT MEMBERS	46

4.66 During the reporting period, approximately 85% of telecommunications interception warrants were issued by AAT members, 7% by Federal Magistrates, 7% by Family Court Judges and 1% by Federal Court Judges. The number of warrants issued by authorities is influenced by an agency's operational needs and the availability of an issuing authority at the time of application.

Table 48—Number of telecommunications interception warrants issued by Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT members

AGENCY	ISSUING AUTHORITY			
	FEDERAL COURT JUDGES	FAMILY COURT JUDGES	FEDERAL MAGISTRATES	NOMINATED AAT MEMBERS
ACC	-	1	1	188
ACLEI	-	-	2	2
AFP	2	5	26	490
CCC	3	3	-	29
CMC	-	-	-	25
ICAC	8	-	-	4
NSW CC	-	-	9	401
NSW POLICE	1	23	29	1,226
NT POLICE	-	-	11	35
OPI	-	-	-	45
PIC	1	-	-	62
QLD POLICE	-	4	168	5
SA POLICE	-	-	-	107
TAS POLICE	-	-	-	27
VIC POLICE	-	-	-	317
WA POLICE	-	220	-	10
TOTAL	**15**	**256**	**246**	**2,973**

Interceptions on behalf of other agencies

4.67 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 49 sets out the number of interceptions executed by agencies on behalf of other agencies during the reporting period.

[12] The number eligible may be higher than the number eligible at any given time as the figure includes issuing authorities who may have retired and their replacements.

4.68 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 49—Number of interceptions carried out on behalf of other agencies

INTERCEPTION CARRIED OUT BY	INTERCEPTION CARRIED OUT ON BEHALF OF	
ACC	**ACLEI**	4
ACC	**AFP**	3
ACC	**CMC**	30
ACC	**QLD POLICE**	217
AFP	**NSW POLICE**	4
AFP	**WA POLICE**	12
VIC POLICE	**TAS POLICE**	27
TOTAL		**297**

Resources devoted to telecommunications interception

4.69 In addition to the total expenditure figures provided in Table 45, the figures in Table 50 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 50—Recurrent costs of interceptions per agency

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL ($)
ACC	5,282,185	356,821	8,589	525,971	**6,173,566**
ACLEI	22,129	-	-	1,180	**23,309**
AFP	6,617,346	109,234	2,420,080	342,209	**9,488,869**
CCC	1,472,288	27,040	1,390,925	213,388	**3,103,641**
CMC	1,109,538	40,655	0	407,469	**1,557,672**
ICAC	40,105	4,843	15,438	47,646	**108,032**
NSW CC	2,146,369	99,957	711,955	969,666	**3,927,947**
NSW POLICE	3,928,153	555,962	-	843,796	**5,327,911**
NT POLICE	624,000	-	-	218,000	**842,000**
OPI	1,142,169	40,454	-	62,160	**1,244,783**
PIC	1,139,915	-	-	109,069	**1,248,984**
QLD POLICE	2,772,647	126,292	797,927	1,534,384	**5,231,250**
SA POLICE	2,194,792	230,841	181,583	81,074	**2,688,290**
TAS POLICE	380,487	-	117,642	4,462	**502,591**
VIC POLICE	4,550,437	274,903	372,243	558,372	**5,755,955**
WA POLICE	2,982,615	142,621	-	145,466	**3,270,702**

Emergency services facility declarations

4.70 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 51 provides the required information.

Table 51—Emergency service facility declarations

STATE/TERRITORY	POLICE	FIRE BRIGADE	AMBULANCE	DESPATCHING
NEW SOUTH WALES	8	98[13]	7	1
VICTORIA	6	1	9	8
QUEENSLAND	21	9	9	-
WESTERN AUSTRALIA	1	2	1	-
SOUTH AUSTRALIA	1	2	1	-
TASMANIA	1	2	1	-
AUSTRALIAN CAPITAL TERRITORY	4	-	-	1
NORTHERN TERRITORY	3	1	2	1
TOTAL	**45**	**115**	**30**	**11**

Reports by Commonwealth Ombudsman

4.71 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 TIA 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.

4.72 The Ombudsman completed two inspections each of the ACC's and AFP's records during the reporting period. The Ombudsman completed one inspection of ACLEI's records for warrants that ceased in the period 1 January to 30 June 2010. A second inspection was not undertaken as ACLEI advised that it had not obtained any further telecommunications interception warrants after 30 June 2010.

[13] There has been an increase in declared facilities in NSW due to that State's request from the Rural Fire Service to declare each facility in its decentralised model.

ACLEI

4.73 The Ombudsman commented that the inspection conducted in 2010-11 was the first instance of ACLEI's use of the telecommunications interception provisions within the Act.

4.74 The Ombudsman found ACLEI to be compliant with the requirements for the keeping of records connected with the issue of warrants (section 80) and not compliant with the other record keeping requirements in connection with interceptions (section 81).

4.75 The Ombudsman identified some inconsistencies in record keeping where interception was conducted with the AFP's assistance, and an instance of interception of SMS messages after a warrant had been revoked. ACLEI quarantined information where necessary.

4.76 The Ombudsman made two recommendations as a result of the inspection and, as a consequence, ACLEI has amended its procedures to prevent future errors.

The ACC

4.77 The Ombudsman commented that the ACC's Electronic Product Management Centre continues its effective management of the ACC's interception activities and seeks to continuously improve its administrative processes and procedures. The Ombudsman also noted the ACC's cooperative approach to inspections.

4.78 The Ombudsman found the ACC to be compliant with the destruction requirements of the TIA Act (section 79) and the requirements for the keeping of records connected with the issue of warrants (section 80) and other records in connection with interceptions (section 81).

4.79 The Ombudsman's report identifies that the ACC self-disclosed interceptions in joint operations where the ACC had not obtained authorisation under section 55(3) of the Act. The ACC has amended its guidelines to improve its process for obtaining proper authorisation under section 55(3).

4.80 The Ombudsman did not make any recommendation as a result of either inspection of the ACC.

The AFP

4.81 The Ombudsman commented that the AFP's Telecommunications Interception Division continues its effective management of the AFP's interception activities and seeks continuously to improve its administrative processes and procedures. The Ombudsman also noted the AFP's cooperative approach to inspections.

4.82 The Ombudsman found the AFP to be compliant with all the requirements of the Act, relating to destruction of records (section 79), keeping of records connected with the issue of warrants (section 80) and other records in connection with interceptions (section 81).

4.83 The Ombudsman did not make any recommendations as a result of either inspection of the AFP.

Other information

4.84 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.

Stored communications

4.85 The Ombudsman inspected the records of 14 enforcement agencies pursuant to the stored communications provisions of the TIA Act and provided the reports to the Department under section 153(1) of the TIA Act. The agencies inspected were the ACC, AFP, ASIC, CCC, CMC, Customs, NSW CC, NSW Police, NT Police, OPI, Qld Police, SA Police, Tas Police, Vic Police, WA Police.

4.86 The Ombudsman found that all enforcement agencies were compliant with the record keeping requirements relating to the issue of stored communications warrants under section 151 of the TIA Act. The Ombudsman found that of the three agencies which destroyed records under section 150 of the TIA Act two were compliant. It could not be determined if the third agency was compliant due to inadequate records about destruction, but the agency has since advised that it has implemented processes to prevent the error recurring.

Period of warrant

4.87 The Ombudsman commented on a systemic issue of agencies being unable to determine the date a carrier accessed a stored communication on their behalf under a warrant. Section 119(1) of the TIA Act limits the period a stored communication warrant remains in force until it is first executed or until five days after the day on which the warrant was issued, whichever occurs sooner.

4.88 The Ombudsman identified 168 (out of 283) warrants issued during the 2009-10 period where the agency did not have information available to determine whether or not the stored communications had been lawfully accessed under the warrant. This is an ongoing issue which was identified in the 2009-2010 report, with legislative change suggested as a possible solution. The Ombudsman, the Department, agencies and industry are continuing to work to address this issue.

4.89 The Ombudsman found that access to stored communications in eight out of 283 warrants appeared to have occurred after the warrant expired. In these cases, agencies have quarantined the information from further use by investigators.

Subject of warrant

4.90 In seven out of 283 warrants, the Ombudsman found that agencies accessed stored communications of persons either not on a warrant or not involved in a serious contravention.

4.91 The Ombudsman recommended that agencies ensure that their officers only apply for a stored communications warrant for a person involved in a serious contravention. The Ombudsman also recommended that, where stored communications were accessed outside the authority of a warrant, agencies should quarantine the product from use by its investigators until the product is able to be destroyed in accordance with the Act.

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 TIA 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:

- ACBPS
- ASIC
- 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 52. Only those enforcement agencies that applied for stored communications warrants during the past three reporting period are included in the table.

Table 52—Applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
ACBPS	Made	9	7	7
	Refused/withdrawn	-	-	-
	Issued	9	7	7
ACC	Made	8	55	27
	Refused/withdrawn	-	-	-
	Issued	8	55	27
AFP	Made	41	39	25
	Refused/withdrawn	0	-	-
	Issued	41	39	25
ASIC	Made	6	10	-
	Refused/withdrawn	-	-	-
	Issued	6	10	-
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	Made	-	-	5
	Refused/withdrawn	-	-	-
	Issued	-	-	5
CCC	Made	4	1	-
	Refused/withdrawn	-	-	-
	Issued	4	1	-
CMC	Made	29	9	2
	Refused/withdrawn	1	-	-
	Issued	28	9[14]	2
NSW CC	Made	6	1	-
	Refused/withdrawn	-	-	-
	Issued	6	1	-
NSW POLICE	Made	26	22	90
	Refused/withdrawn	-	-	1
	Issued	26	22	89
NT POLICE	Made	-	2	11
	Refused/withdrawn	-	-	-
	Issued	-	2	11
OPI	Made	12	2	2
	Refused/withdrawn	-	-	-
	Issued	12	2	2
PIC	Made	-	-	8
	Refused/withdrawn	-	-	-
	Issued	-	-	8
QLD POLICE	Made	119	66	48
	Refused/withdrawn	-	-	-
	Issued	119	66	48
SA POLICE	Made	8	5	5
	Refused/withdrawn	-	-	-
	Issued	8	5	5
TAS POLICE	Made	36	46	45
	Refused/withdrawn	-	-	1
	Issued	36	46	44
VIC POLICE	Made	9	6	11
	Refused/withdrawn	-	-	-
	Issued	9	6	11
WA POLICE	Made	8	14	14
	Refused/withdrawn	-	-	-
	Issued	8	14	14
TOTAL [paragraph 162(2)(a)]	**Made**	**321**	**285**	**300**
	Refused/withdrawn	**1**	**-**	**2**
	Issued	**320**	**285**	**298**

[14] CMC advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

Telephone applications for stored communications warrants

5.6 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. This information is presented in Table 53.

Table 53—Telephone applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
NSW POLICE	Made	1	3	3
	Refused/withdrawn	-	-	-
	Issued	1	3	3
VIC POLICE	Made	-	2	-
	Refused/withdrawn	-	-	-
	Issued	-	2	-

Renewal applications for stored communications warrants

5.7 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. This information is presented in Table 54.

Table 54—Renewal applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
CMC	Made	15	-	-
	Refused/withdrawn	-	-	-
	Issued	15	-	-

Stored communications warrants subject to conditions or restrictions

5.8 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. This information is presented in Table 55.

Table 55—Stored communications warrants subject to conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		08/09	09/10	10/11
AFP	Made	-	1	-
	Refused/withdrawn	-	-	-
	Issued	-	1	-
CMC	Made	-	-	2
	Refused/withdrawn	-	-	-
	Issued	-	-	2
SA Police	Made	-	-	4
	Refused/withdrawn	-	-	-
	Issued	-	-	4
QLD POLICE	Made	20	1	2
	Refused/withdrawn	-	-	-
	Issued	20	1	2
TOTAL	**Made**	**20**	**2**	**8**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**20**	**2**	**8**

Effectiveness of stored communications warrants

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

5.9 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 56. The table also includes the number of convictions recorded based on lawfully accessed information.

Table 56—Number of arrests, proceedings and convictions made on the basis of lawfully accessed information

AGENCY	ARRESTS			PROCEEDINGS			CONVICTIONS		
	08/09	09/10	10/11	08/09	09/10	10/11	08/09	09/10	10/11
ACBPS	-	3	-	-	1	-	-	-	1
ACC	**-**	10	8	**-**	**-**	**-**	**-**	**-**	**-**
AFP	27	1	2	5	1	2	-	-	2
CMC	-	15	1	-	-	2	-	-	2
NSW POLICE	21	10	25	24	22	3	19	20	2
NT POLICE	-	1	-	-	-	-	-	-	-
QLD POLICE	69	47	35	1	12	14	1	12	14
SA POLICE	-	-	1	-	2	1	-	2	1
TAS POLICE	10	25	16	2	7	11	-	8	11
VIC POLICE	8	1	3	-	3	-	-	7	-
WA POLICE	4	-	-	-	-	-	-	-	-
TOTAL	**139**	**113**	**91**	**32**	**48**	**33**	**20**	**49**	**33**

Interpretative note relating to prosecutions and convictions statistics

5.10 It should 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.

5.11 Additionally, the information in Table 56 should be interpreted with caution. Due to operational priorities, 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.

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 TIA 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 are able to authorise the disclosure of telecommunications data if they are an enforcement agency. An enforcement agency is an agency responsible for the administration of a legislation which enables them to enforce a criminal law, impose pecuniary penalties or protect the public revenue.

6.3 An authorised officer of an enforcement agency is able to make the authorisation. An authorised officer means the head, deputy head, or a person who holds an office or position covered by an authorisation under subsection 5AB(1) of the TIA Act. Enforcement agencies notify the CAC of the positions which can authorise the disclosure of telecommunications data.

Authorisations granted

6.4 The number of authorisations made for access to existing information or documents in the enforcement of the criminal law is given at Table 57. 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 58.

Table 57—Number of authorisations made for access to existing information or documents in the enforcement of the criminal law

AGENCY	AUTHORISATIONS		
	08/09	09/10	10/11
ACBPS	9,040	4,157	4,017
ACC	9,038	12,467	12,467
ACLEI	28	65	160
AFP	16,942	20,869	22,992
ASIC	2,319	2,874	1,602
AUSTRALIAN COMPETITION & CONSUMER COMMISSION	7	35	25
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	-	2	4
AUSTRALIAN TAXATION OFFICE	644	610	724
CCC	394	506	357
CMC	9,468	9,577[15]	8,395
CORRECTIVE SERVICES NSW	-	37	63
CORRECTIONS VICTORIA	-	-	82
DEPARTEMENT OF ENVIRONMENT AND RESOURCE MANAGEMENT (QLD)	-	-	8
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	110	89	22
DEPARTMENT OF COMMERCE (WA)	152	184	314
DEPARTMENT OF DEFENCE	48	30	20
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFIARS	22	7	23
DEPARTMENT OF HEALTH AND AGEING	24[16]	22[17]	47
DEPARTMENT OF IMMIGRATION AND CITIZENSHIP	-	86	180
DEPARTMENT OF PRIMARY INDUSTRIES (VIC)	421	464	469
DEPARTMENT OF SUSTAINABILITY, ENVIRONMENT, WATER, POPULATION AND COMMUNITIES[18]	-	22	12
ICAC	260	450	596
INSOLVENCY AND TRUSTEE SERVICE AUSTRALIA	-	211	135
JUVENILE JUSTICE (NSW)	1	-	3
NSW CC	4,620	3,602	2,915

[15] OPI advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[16] Department of Health and Ageing advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[17] Department of Health and Ageing advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[18] Previously known as the Department of Environment, Water, Heritage and the Arts

AGENCY	AUTHORISATIONS		
	08/09	09/10	10/11
NSW POLICE	100,585	115,343	41,340
NT POLICE	807	1,834	3,695
OFFICE OF ENVIRONMENT & HERITAGE (NSW)[19]	60	119	192
OPI	873	2,235	5,246
PIC	1,815	1,242	1,731
QLD POLICE	9,344	10,223	30,896[20]
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS QUEENSLAND	-	46	52
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS VICTORIA	7	16	31
SA POLICE	3,442	11,631	7,094
TAS POLICE	9,627	6,689	9,845
TRANSPORT ACCIDENT COMMISSION (VIC)	-	2	4
VIC POLICE	40,617	50,234	65,703[21]
VICTORIAN TAXI DIRECTORATE	-	3	18
WA POLICE	24,606	26,234	22,152
TOTAL	**245,297**	**282,195**	**243,631**

[19] Previously known as the Department of Environment, Climate Change and Water (NSW)

[20] Qld Police have advised that the increase is due to improved accuracy in reporting data collection

[21] Vic Police has had an increase in utilisation of this tool as investigator knowledge becomes more widely known, technology changes and auto processing have simplified the process, and due to its effectiveness it is also widely used as a precurser to T.I. warrants

Table 58—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		
	08/09	09/10	10/11
ACBPS	1,096	225	173
ACLEI	4	-	-
ACT REVENUE OFFICE	5	-	-
AFP	549	267	359
ASIC	148	123	209
AUSTRALIA POST	298	361	160
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	-	10	66
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	7	4	-
AUSTRALIAN TAXATION OFFICE	645	504	249
CENTRELINK	1,926	2,579	2,127
CHILD SUPPORT PROGRAM[22]	192	74	67
CMC	-	1	-
CONSUMER AFFAIRS VICTORIA	441	235	269
CONSUMER AND BUSINESS SERVICES (SA)[23]	124	201	178
CORRECTIONS VICTORIA	-	52	67
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	6	-	-
DEPARTMENT OF COMMERCE WA	-	20	99
DEPARTMENT OF DEFENCE	1	8	2
DEPARTMENT OF EMPLOYMENT, ECONOMIC DEVELOPMENT AND INNOVATION (QLD)	4	21	41
DEPARTMENT OF ENVIRONMENT AND CONSERVATION (WA)	-	18	39
DEPARTMENT OF ENVIRONMENT AND RESOURCE MANAGEMENT (QLD)	-	3	1
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFAIRS	1	-	-
DEPARTMENT OF HEALTH AND AGEING	3[24]	4[25]	6
DEPARTMENT OF IMMIGRATION AND CITIZENSHIP	-	204	76
DEPARTMENT OF JUSTICE (NT)	-	2	-
DEPARTMENT OF PRIMARY INDUSTRIES (NSW)[26]	81	108	65

[22] Previously known as Child Support Agency

[23] Previously known as the Office of Consumer and Business Affairs

[24] Department of Health and Ageing advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[25] Department of Health and Ageing advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[26] Previously known as Department of Industry and Investment NSW

AGENCY	AUTHORISATIONS		
	08/09	09/10	10/11
DEPARTMENT OF PRIMARY INDUSTRIES (VIC)	-	1	3
DEPARTMENT OF SUSTAINABILITY AND ENVIRONMENT (VIC)	11	75	108
ENVIRONMENTAL PROTECTION AGENCY (QLD)	50	-[27]	-[28]
FAIR TRADING (NSW)	658	1,012	935
HEALTH CARE COMPLAINTS COMMISSION (NSW)	2	8	30
ICAC	227	24	-
JUVENILE JUSTICE (NSW)	-	1	2
MEDICARE AUSTRALIA	22[29]	10[30]	21
NSW POLICE	-	-	2,076
NT POLICE	-	-	-
OFFICE OF LIQUOR, GAMING AND RACING (NSW)[31]	-	-	2
OFFICE OF STATE REVENUE (NSW)	132	132	224
OFFICE OF STATE REVENUE (QLD)	53	27	20
OFFICE OF THE AUSTRALIAN BUILDING AND CONSTRUCTION COMMISSIONER	14	12	31
PRISON SERVICE (TAS)	8	3	5
QLD POLICE	-	-	56
REVENUE SA	36	77	90
SA POLICE	-	-	1
STATE REVENUE OFFICE VICTORIA	103	130	106
TAS POLICE	189	-	-
TERRITORY REVENUE OFFICE (NT)	1	-	-
VICTORIAN TAXI DIRECTORATE	-	3	4
WORKCOVER QUEENSLAND	6	4	-
WORKSAFE VICTORIA	-	27	13
WYNDHAM CITY COUNCIL[32]	-	-	20
TOTAL	**7,014**	**6,583**	**8,000**

6.5 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 59. 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.

[27] Now captured under Department of Environment and Resource Management

[28] Now captured under Department of Environment and Resource Management

[29] Medicare Australia advised that the information supplied for the 08/09 period was inaccurate, this report reflects the accurate figure

[30] Medicare Australia advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure

[31] NSW Liquor and Gaming was not an enforcement agency in previous reporting periods

[32] Wyndham City Council was not an 'enforcement agency' in previous reporting periods

Table 59—Prospective authorisations

AGENCY	NUMBER OF AUTHORISATIONS MADE			DAYS SPECIFIED IN FORCE			ACTUAL DAYS IN FORCE			AUTHORISATIONS DISCOUNTED		
	08/09	09/10	10/11	08/09	09/10	10/11	08/09	09/10	10/11	08/09	09/10	10/11
ACBPS	-	3	86	-	46	3,830	-	46	3,055	-	-	10
ACC	42	114	422	1,459	4,461	17,229	1,031	2,884	15,851	2	-	29
AFP	103	148	683	3,152	4,577	6,643	2,879	3,714	4,697	12	7	23
CCC	49	67	51	1,069	2,502	1,817	1,098	1,840	1,273	16	6	5
CMC	129	174	86	1,554	6,927	3,830	1,466	6,919	3,055	9	20	10
ICAC	-	2	-	-	3	-	-	3	-	-	-	-
NSW CC	720	967	850	16,612	27,078	22,097	12,539	24,740	19,586	61	64	74
NSW POLICE	237	221	370	5,027	5,771	10,311	3,908	3,960	6,110	10	10	32
NT POLICE	356	322	435	16,020	14,448	15,975	14,507	12,234	13,936	-	20	36
OPI[33]	97	19	19	4,299	719	510	3,146	653	396	8	9	-
PIC	106	127	94	3,466	5,299	3,882	4,143	4,218	3,108	3	25	8
QLD POLICE	192	451	641	3,109	9,775	18,931	2,164	8,684	17,753	15	41	43
SA POLICE	53	83	181	1,560	2,953	6,426	1,078	1,755	4,057	4	6	10
TAS POLICE	65	40	110	2,771	1,800	4,950	1,660	1,007	2,332	1	-	11
VIC POLICE	211	797	547	7,614	25,335	20,789	4,887	18,357	13,896	11	32	30
WA POLICE[34]	233	272	347	8,808	12,240	15,615	4,463	6,989	7,783	18	33	35
TOTAL	**2,571**	**3,804**	**4,836**	**77,060**	**123,934**	**149,005**	**58,969**	**97,911**	**113,833**	**170**	**273**	**346**

[33] OPI advised that the information supplied for the 09/10 period was inaccurate for *Actual Days in Force*, and that information supplied for the 08/09 and 09/10 period was inaccurate for *Number of Authorisations Made*. This report reflects the accurate figure

[34] WA Police advised that the information supplied for the 09/10 period was inaccurate for *Days Specified in Force* and *Actual Days in Force*. This report reflects the accurate figure

6.6 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 60.

Table 60—Average specified and actual time in forces

AGENCY	AVERAGE PERIOD SPECIFIED			AVERAGE PERIOD ACTUAL		
	08/09	09/10	10/11	08/09	09/10	10/11
ACBPS	-	15	-	-	15	-
ACC	35	39	41	26	25	40
AFP	31	31	10	32	26	7
CCC	33	37	36	32	30	28
CMC	12	40	45	12	45	40
ICAC	-	2	-	-	2	-
NSW CC	23	28	26	19	27	25
NSW POLICE	21	26	28	17	19	18
NT POLICE	45	45	37	41	41	35
OPI[35]	44	38	27	24	33	21
PIC	33	42	41	40	41	36
QLD POLICE	16	22	30	12	21	30
SA POLICE	29	36	35	22	23	23
TAS POLICE	43	45	45	26	25	23
VIC POLICE	36	32	38	24	24	27
WA POLICE	38	45	45	21	29[36]	25
TOTAL	**30**	**33**	**34**	**23**	**30**	**27**

[35] OPI advised that the information supplied for the 08/09 and 09/10 period was inaccurate for *Average Period Specified* and *Average Period Actual*. This report reflects the accurate figure

[36] WA Police advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure