Telecommunications (Interception and Access) Act 1979

Annual Report for the year ending 30 June 2009

Telecommunications (Interception and Access) Act 1979

Report for the year ending 30 June 2009

ISBN: 978-1-921725-04-3

Produced by the Public Affairs Unit
Australian Government Attorney-General's Department
Publication number

CONTENTS

LIST OF TABLES

ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACC	Australian Crime Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
ASIO	Australian Security Intelligence Organisation
Blunn Report	Report of the *Review of the Regulation of Access to Communications*
CAC	Communications Access Co-ordinator
CCC WA	Corruption and Crime Commission of Western Australian
CMC	Queensland Crime and Misconduct Commission
ICAC	Independent Commission Against Corruption (New South Wales)
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police
OPI	Office of Police Integrity (Victoria)
PIC	Police Integrity Commission (New South Wales)
Qld Police	Queensland Police
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-first Annual Report on the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This report relates to the period from 1 July 2008 to 30 June 2009.

1.2 Chapter 2 outlines the objectives and the structure of the TIA Act.

1.3 Chapter 3 records relevant developments that have occurred during the reporting period.

1.4 Chapter 4 presents the information collected in accordance with the statutory requirements of Part 2-8 of the TIA Act, relating to the interception of telecommunications.

1.5 Chapter 5 presents the information collected in accordance with the statutory requirements of Part 3-6 of the TIA Act, relating to accessing stored communications.

1.6 Chapter 6 presents the information collected in accordance with the statutory requirements of Part 4-2 of the TIA Act, relating to accessing telecommunications data.

CHAPTER 2—OVERVIEW OF THE ACT

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

Objectives of the legislation

2.2 The TIA Act has two key purposes. Its primary objective is to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act makes it an offence to intercept communications, or access stored communications, other than in accordance with the provisions of the TIA Act. The second purpose of the TIA Act is to specify the circumstances in which it is lawful to intercept, access communications or authorise the disclosure of telecommunications data.

2.3 A telecommunications service may be intercepted under the authority of a telecommunications interception warrant by an *interception agency* for the investigation of a serious offence, or by the Australian Security Intelligence Organisation (ASIO) for national security purposes. A stored communication may be covertly accessed under the authority of a stored communications warrant by an *enforcement agency* for the investigation of a serious contravention or by ASIO for national security purposes. Telecommunications data may be disclosed by a telecommunications service provider under the authorisation of an officer holding a management office or position of an *enforcement agency* for the enforcement of the criminal law or the enforcement of a law imposing a pecuniary penalty or protection of the public revenue.

Provisions relevant to this report

2.4 The foundations of the TIA Act are contained in subsections 7(1) and 108(1) which prohibit the interception of a communication passing over the telecommunications system or access to stored communications. Chapter 4 of the TIA Act allows the disclosure of telecommunications data which is ordinarily prohibited by the *Telecommunications Act 1997*.

2.5 Subsection 6(1) of the TIA Act defines interception as listening to or recording, by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication.

2.6 The effect of section 6AA and paragraph 108(1)(b) of the TIA Act is that accessing a stored communication comprises listening to, reading or recording a stored communication where that action is done with the assistance of a carrier. The access must be without the knowledge of either the sender or the intended recipient of the communication for it to fall within the parameters of the TIA Act.

2.7 Telecommunications data is not defined in the TIA Act. Section 172 excludes the content or substance of a call from being ‘telecommunications data’. Accordingly, telecommunications data could include the date, time, subscriber and location of a call.

2.8 There are exceptions to these prohibitions, the most relevant of which relate to the interception of communications, access to stored communications under a warrant or the disclosure of telecommunications data under an authorisation.

2.9 The TIA Act regulates the

- issue and revocation of warrants and authorisations
- scope of the authority conferred by warrants or authorisations
- execution of warrants, and
- use of information obtained under warrants or authorisations.

Telecommunications interception warrants

Offences for which telecommunications interception warrants may be obtained

2.10 Part 2-5 of the TIA Act provides for the issue of telecommunications interception warrants to interception agencies. This Part of the TIA Act provides that a telecommunications interception warrant can be sought to assist with the investigation of a serious offence.

2.11 A serious offence is exhaustively defined in section 5D which includes the following types of offences:

- murder, kidnapping and equivalent offences
- an offence against Division 307 of the *Criminal Code*, being serious drug import and export offences
- an offence constituted by conduct involving an act or acts of terrorism
- an offence against Subdivision A of Divisions 72, 101, 102 and 103 of the *Criminal Code*
- offences in relation to which the Australian Crime Commission (ACC) is conducting a special investigation within the meaning of the *Australian Crime Commission Act 2002*[1]
- offences relating to child pornography
- specified offences involving particular conduct such as loss of a person's life, serious personal injury or trafficking in prescribed substances where the offence is punishable by at least seven years imprisonment
- specified offences involving planning and organisation which involve conduct such as theft, handling of stolen goods, bribery or corruption where the offence is punishable by at least seven years imprisonment
- money laundering offences
- offences relating to people smuggling with exploitation, slavery, sexual servitude and deceptive recruiting
- serious drug offences

[1] This section applies only to warrants sought by the ACC.

- serious cartel offences
- computer-related offences, and
- ancillary offences, such as aiding, abetting and conspiring to commit serious offences.

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

Applying for telecommunications interception warrants

2.13 Applications for telecommunications interception warrants may only be made by an interception agency. An interception agency is the ACC, the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Federal Police (AFP) or an 'eligible authority' of a State or the Northern Territory which is the subject of a declaration under section 34 of the TIA Act.

2.14 In effect, a section 34 declaration, which can only be made by the Attorney-General, grants interception agency status to an eligible authority. This means that the agency can then apply for telecommunications interception warrants to assist in their investigations of serious offences. An eligible authority which is *not* the subject of a declaration is *not* able to apply for such a warrant but is able to receive intercepted information for permitted purposes from an interception agency.

2.15 The TIA Act defines eligible authorities to be the police force of each of the States and of the Northern Territory. During the reporting period, 'eligible authority' was defined as:

- in New South Wales – the NSW Crime Commission, the Independent Commission Against Corruption (ICAC), the Inspector of the ICAC, the Police Integrity Commission (PIC) and the Inspector of the PIC
- in Victoria – the Office of Police Integrity (OPI)
- in Queensland – the Crime and Misconduct Commission (CMC)
- in Western Australia – the Corruption and Crime Commission of Western Australia (CCC WA) and the Parliamentary Inspector of the CCC WA.

2.16 During the reporting period, the following eligible authorities were the subject of a declaration pursuant to section 34 of the TIA Act and therefore were able to apply for telecommunications interception warrants:

AGENCY[2]	DATE OF SECTION 34 DECLARATION
Victoria Police	28 October 1988
New South Wales Crime Commission	30 January 1989
New South Wales Police Force	30 January 1989
Independent Commission Against Corruption	6 June 1990
South Australia Police	10 July 1991
Western Australia Police	15 July 1997
Police Integrity Commission	14 July 1998
Corruption and Crime Commission of Western Australia	24 March 2004
Tasmania Police	5 February 2005
Northern Territory Police	25 October 2006
Office of Police Integrity Victoria	18 December 2006

Eligible Judges and nominated AAT members

2.17 Part 2-5 of the TIA Act provides that an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member may issue a telecommunications interception warrant on application by an agency.

2.18 An 'eligible Judge' refers to a Judge of a court created by the Parliament who has consented in writing and been declared by the Attorney-General to be an eligible Judge. In the reporting period, eligible Judges were members of the Federal Court of Australia, the Family Court of Australia and the Federal Magistrates Court.

2.19 A 'nominated AAT member' refers to a Deputy President, senior member or a member of the AAT who has been nominated by the Attorney-General to issue warrants. In the case of part-time senior members and members of the AAT, the member must have been enrolled as a legal practitioner of the High Court, the Federal Court or the Supreme Court of a State or Territory for no less than five years to be eligible for nomination to issue warrants.

Form of applications

2.20 The TIA Act requires that an application for a telecommunications interception warrant be in writing and be accompanied by a supporting affidavit. However, in urgent circumstances, applications may be made by telephone. In either case, the warrant takes effect only when completed and signed by the Judge or nominated AAT member.

2.21 The information required for a written application must also be verbally provided to a Judge or nominated AAT member at the time of a telephone application and subsequently provided in writing (within one day). Specific provision is made for the revocation of a warrant obtained by telephone where this condition is not complied with.

[2] Queensland Police Service and the Crime and Misconduct Commission were the subject of a declaration pursuant to section 34 of the TIA Act on 8 July 2009, outside the reporting period.

2.22 The TIA Act requires that an application contain the name of the agency and person making the application. The supporting affidavit must contain the facts on which the application is based, the period for which the warrant is sought to be in force and information regarding any previous warrants obtained in relation to the same matter.

Matters to be considered by an issuing authority

2.23 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.

2.24 Where an application for a warrant includes a request that the warrant authorise entry onto premises, section 48 requires that the Judge or nominated AAT member also be satisfied that it would be impracticable or inappropriate to intercept communications by less intrusive means.

Safeguards and controls relating to the telecommunications interception regime

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

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

2.26 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 warrant.

Reports by carrier

2.27 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

2.28 Section 81A of the TIA Act provides that the Secretary of the Attorney-General's Department must maintain a General Register which includes particulars of all telecommunications interception warrants. The particulars required to be recorded in the General Register are:

- the date of issue and period for which the warrant was to be in force
- the agency to which the warrant was issued and the Judge or nominated AAT member who issued the warrant
- the telecommunications service to which the warrant relates
- the name of the person specified in the warrant as the person using or likely to use the telecommunications service
- each serious offence in relation to which the Judge or nominated AAT member who issued the warrant was satisfied on the application for the warrant, and
- for named person warrants, the name of the person to whom the warrant relates and each telecommunications service that is specified in the warrant, or in relation to which interceptions authorised by the warrant have occurred.

2.29 Section 81B of the TIA Act provides that the Secretary of the Attorney-General's Department must deliver the General Register to the Attorney-General for inspection every three months. Interception agencies are notified once the Attorney-General has inspected the General Register to enable the destruction of restricted records.

Special Register of telecommunications interception warrants

2.30 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, directly or indirectly, to a prosecution within three months of the expiry of the warrant. The Secretary must deliver the Special Register to the Attorney-General for inspection every three months together with the General Register.

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 permitted purposes and the Attorney-General has inspected the relevant Register, those records must be destroyed.

Inspections

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. The imposition of parallel record keeping and reporting requirements with the Commonwealth legislation is a precondition to the State or Territory eligible authority being granted interception agency status. If the Attorney-General is satisfied that the State or Territory legislation is no longer parallel to the Commonwealth legislation, he or she may revoke their interception agency status.

2.35 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.[3] 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 supervisory and accountability provisions. This means that the TIA Act imposes a national scheme in relation to telecommunications interception and ensures that the Attorney-General is kept informed of the agencies' activities by means of reports from the agencies and the Ombudsman.

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.

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. Enforcement agencies will include all the defined interception agencies plus other regulatory bodies such as the Australian Customs and Border Protection Service and the Australian Securities and Investments Commission.

[3] 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).

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. 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. It should be noted that appointed State magistrates, while able to issue stored communications warrants, are not able to be declared to be able to issue telecommunications interception warrants.

2.42 Paragraph 6DB(1)(b) further defines an issuing authority as including a person who is a Deputy President, senior member or a member of the AAT and has been appointed as an issuing authority by the Attorney-General. The member must have been enrolled as a legal practitioner of a Federal court or of the Supreme Court of a State or a Territory for at least five years before they are eligible to be appointed as an issuing authority.

Form of applications

2.43 In the normal course of events, the TIA Act requires that an application for a stored communications warrant be in writing and accompanied by a supporting affidavit. However, in urgent circumstances, applications may be made by telephone. In either case, the warrant takes effect only when completed and signed by the issuing authority.

2.44 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.

2.45 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

2.46 An issuing authority must consider the following matters before issuing a stored communications warrant:

- 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

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

Recordkeeping

2.48 Section 151 of the TIA Act provides that the chief officer of an enforcement agency must cause to be kept:

- each stored communications warrant issued
- each instrument of revocation
- copies of authorisations which authorise persons to receive stored communications and
- particulars of the destruction of information.

Destruction of records

2.49 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

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

Annual report tabled by Attorney-General

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

Telecommunications data authorisations

Telecommunications data

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

2.54 Section 172 prohibits the disclosure of any content or substance of a communication. While telecommunications data is not defined in the TIA Act, it is taken to mean anything that is not the content or substance of a communication. It can include:

- subscriber information
- telephone numbers of the parties involved in the communication
- the date and time of a communication
- the duration of a communication
- Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication and
- location-based information.

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

Historical data

2.56 Historical or existing data is data which came into existence before the time the person from whom the disclosure is sought received notification of the authorisation. It does not include information which came into existence after notification was received but before the authorisation was executed.

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

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

Prospective data

2.58 Prospective data is data that comes into existence during the period for which the authorisation is in force. It does not include data that came into existence before the authorisation was in force.

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

2.60 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

2.61 A historical data authorisation may only be authorised by an authorised officer of the enforcement agency. A prospective data authorisation may only be authorised by an authorised officer of the criminal law-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

2.62 Section 183 of the TIA Act provides that an authorisation under Division 3 or 4 of Part 4-1, a notification, revocation or notification of revocation must be in written or electronic form and must comply with any requirements put in place by the Communications Access Co-ordinator (CAC). The requirements for an authorisation include:

- the identity of the agency
- the basis on which the agency is an enforcement agency or criminal 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
- for access to existing information or documents, a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or the protection of the public revenue
- for access to prospective information or documents, a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years
- for access to prospective information or documents, a statement that the authorised officer has had regard to how much the privacy of any person or persons would be likely to be interfered with and that the authorised officer is satisfied that the impact on privacy is outweighed by the seriousness of the conduct being investigated
- the date on which the authorisation is made, and for access to prospective information or documents, the date on which the authorisation is to end.

2.63 Section 184 requires a relevant staff member from an agency making an authorisation to notify the person from whom the disclosure is sought.

Safeguards and controls relating to the telecommunications data regime

Recordkeeping and inspections

2.64 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

2.65 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. It also outlines comments made by intercepting agencies in relation to the value and importance of interception under telecommunications interception warrants.

Recent legislative and policy developments

Telecommunications Interception Amendment Act 2008

3.2 Under section 35 of the TIA Act, an agency cannot be declared an interception agency unless the Minister is satisfied that the law of the requesting State makes satisfactory provision for the declared agency to comply with specified recordkeeping, reporting and inspection obligations and that the State has entered into an agreement to pay all expenses connected with the issue of warrants issued to the agency.

3.3 Queensland law enforcement agencies were not interception agencies for the purposes of the TIA Act. Following consultation between the Commonwealth and Queensland government's the *Telecommunications Interception Legislation Amendment Act 2008* was introduced into Parliament to enable the inclusion of Queensland agencies into the interception regime.

3.4 The 2008 Amendment Act was introduced to Parliament on 25 June 2008 with the majority of amendments commencing operation on 4 October 2008. The 2008 Amendment Act introduced the Queensland Public Interest Monitor (the PIM) into the interception regime. This enabled the State of Queensland to legislate for the PIM to be given specific oversight functions for the Queensland Police Service and the Queensland Crime and Misconduct Commission and allow for those agencies to be declared interception agencies under section 34 of the TIA Act.

3.5 The 2008 Amendment Act recognises the unique oversight role the PIM plays in law enforcement matters in Queensland. The PIM plays a similar oversight role in relation to applications for control orders under Division 104 of the *Criminal Code Act 1995*, and applications for warrants including surveillance and covert search warrants under the *Crime and Misconduct Act 2001* (Qld), and the *Police Powers and Responsibilities Act 2000* (Qld).

3.6 The amendments allow the PIM to make submissions to the eligible Judge or nominated Administrative Appeals Tribunal (AAT) member considering the application for an interception warrant and to ask questions of an officer representing the Queensland agency applying for the warrant or any other party required to give further information on the application. These provisions only operate where the applicant is representing either the Queensland Police Service or the Crime and Misconduct Commission. The PIM's power to make submissions is complemented by a requirement on the decision-maker considering an application by a Queensland agency, to consider the PIM's view in deciding whether or not to issue an interception warrant.

3.7 The 2008 Amendment Act also specified that the TIA Act does not affect the operation of Queensland law to the extent that it may authorise or require Queensland agencies to notify the PIM of either a proposed or actual interception warrant application, notify the PIM of any information that may relate to such applications and provide documentation that may relate to such applications.

3.8 The 2008 Amendment Act also made minor and technical amendments to:

- correct an error introduced by the *Telecommunications Interception Legislation Amendment Act 2008* that unintentionally limited a Police Force of a State's delegation powers in relation to a 'certifying officer' as defined by the TIA Act, and

- amend the definition of 'certifying officer' in subsection 5(1) of the TIA Act and the definition of 'appropriate authorising officer' in paragraph 6(1)(g) of the *Surveillance Devices Act 2004* to reflect changes to the structure of the Queensland Crime and Misconduct Commission.

Judicial decisions

R v Kashani-Malaki [2008] QSC

3.9 On 9 July 2008, the Supreme Court of Queensland upheld a claim for public interest immunity from law enforcement agencies ensuring the protection of capabilities and the integrity of the telecommunications interception regime. The defence in this case sought access to information generally provided for in evidentiary certificates.

3.10 The Court considered that the determination of public interest immunity was a balance of two competing aspects of public interest and the effect on the wider public interest if the documents were disclosed. The Court upheld the claim for public interest immunity on the basis that the information being sought did not prejudice the accused. Without the information, the accused was not prevented from challenging the content of the evidence being put before the court or the facts which went to prove the elements of the offence.

Khaled Cheikho & Ors v Regina [2008] NSWCCA 191

3.11 On 13 July 2008, the New South Wales Court of Criminal Appeal upheld the constitutional validity of evidentiary certificates from carriers.

3.12 A challenge to the conclusive nature of evidentiary certificates issued by carriers was made on the basis that the certificates were unconstitutional. The court upheld the validity of the certificates noting that they did not prove any of the 'ultimate facts' of the issue before the court and therefore did not violate Chapter III of the Constitution or the right to trial by jury in section 80 of the Constitution.

Previous Annual Report

3.13 The Annual Report for the year ending 30 June 2008 was tabled in the Senate and in the House of Representatives on 13 February 2009.

Effectiveness of interception

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

CHAPTER 4—TELECOMMUNICATIONS INTERCEPTION INFORMATION REQUIRED UNDER THE ACT

The information required

4.1 Part 2-8 of the TIA Act provides that this report must include the following information:

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

4.2 The TIA Act provides that the information must be set out in relation to each interception agency and, where relevant, each eligible authority. In addition, the information must be combined for all agencies to indicate the overall use and effectiveness of telecommunications interception under the TIA Act.

Which agencies may seek telecommunications interception warrants

4.3 During the reporting period, the following agencies[4] were entitled to apply for telecommunications interception warrants for law enforcement purposes:

- Australian Commission for Law Enforcement Integrity
- Australian Crime Commission
- Australian Federal Police
- Corruption and Crime Commission (Western Australia)
- Independent Commission Against Corruption (New South Wales)
- New South Wales Crime Commission
- New South Wales Police Force
- Northern Territory Police
- Office of Police Integrity (Victoria)
- Police Integrity Commission (New South Wales)
- South Australia Police
- Tasmania Police
- Victoria Police, and
- Western Australia Police.

Applications for telecommunications interception warrants

4.4 Paragraphs 100(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for telecommunications interception warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and for all agencies in total.

4.5 ACLEI did not apply for a warrant during the reporting period.

4.6 During the reporting period, 3,220 warrants were issued to law enforcement agencies under Part 2-5 of the TIA Act. The total number of warrants issued decreased by approximately 1% on the total number of warrants issued during the previous reporting period. 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.

[4] Queensland Police Service and the Crime and Misconduct Commission did not become interception agencies until 8 July 2009 and therefore were not eligible to apply for warrants during the reporting period.

Table 1 – Applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
ACC	Made	211	179	154
	Refused/withdrawn	-	-	-
	Issued	211	179	154
AFP	Made	537	533	573
	Refused/withdrawn	3	3	1
	Issued	534	530	572
CCC WA	Made	122	102	49
	Refused/withdrawn	-	-	-
	Issued	122	102	49
ICAC	Made	33	33	32
	Refused/withdrawn	-	-	-
	Issued	33	33	32
NSW CC	Made	790	672	622
	Refused/withdrawn	2	-	3
	Issued	788	672	619
NSW POLICE	Made	866	814	838
	Refused/withdrawn	1	3	7
	Issued	865	811	831
NT POLICE	Made	27	39	47
	Refused/withdrawn	-	2	2
	Issued	27	37	45
OPI	Made	14	78	65
	Refused/withdrawn	-	-	-
	Issued	14	78	65
PIC	Made	40	91	115
	Refused/withdrawn	-	-	-
	Issued	40	91	115
SA POLICE	Made	95	124	105
	Refused/withdrawn	-	-	-
	Issued	95	124	105
TAS POLICE	Made	13	17	15
	Refused/withdrawn	-	-	-
	Issued	13	17	15
VIC POLICE	Made	367	373	331
	Refused/withdrawn	1	-	-
	Issued	366	373	331
WA POLICE	Made	172	199	287
	Refused/withdrawn	-	-	-
	Issued	172	199	287
TOTAL [paragraph 100(2)(a)]	**Made**	**3,287**	**3,254**	**3,233**
	Refused/withdrawn	**7**	**8**	**13**
	Issued	**3,280**	**3,246**	**3,220**

Telephone applications for telecommunications interception warrants

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

4.8 The total number of telephone applications made in the reporting period has decreased by approximately 25% 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		
		06/07	07/08	08/09
AFP	Made	2	2	2
	Refused/withdrawn	-	-	-
	Issued	2	2	2
NSW CC	Made	2	-	-
	Refused/withdrawn	-	-	-
	Issued	2	-	-
NSW POLICE	Made	29	22	22
	Refused/withdrawn	-	-	-
	Issued	29	22	22
TAS POLICE	Made	-	6	1
	Refused/withdrawn	-	-	-
	Issued	-	6	1
VIC POLICE	Made	21	27	16
	Refused/withdrawn	-	-	-
	Issued	21	27	16
WA POLICE	Made	3	-	2
	Refused/withdrawn		-	-
	Issued	3	-	2
TOTAL [paragraph 100(2)(b)]	**Made**	**57**	**57**	**43**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**57**	**57**	**43**

Renewal applications for telecommunications interception warrants

4.9 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.

4.10 The number of renewal applications decreased by approximately 15% 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		
		06/07	07/08	08/09
ACC	Made	56	46	37
	Refused/withdrawn	-	-	-
	Issued	56	46	37
AFP	Made	74	103	112
	Refused/withdrawn	-	-	-
	Issued	74	103	112
CCC WA	Made	70	50	12
	Refused/withdrawn	-	-	-
	Issued	70	50	12
ICAC	Made	5	6	2
	Refused/withdrawn	-	-	-
	Issued	5	6	2
NSW CC	Made	128	111	70
	Refused/withdrawn	-	-	-
	Issued	128	111	70
NSW POLICE	Made	102	116	104
	Refused/withdrawn	-	-	-
	Issued	102	116	104
NT POLICE	Made	3	-	4
	Refused/withdrawn	-	-	-
	Issued	3	-	4
OPI	Made	2	23	2
	Refused/withdrawn	-	-	-
	Issued	2	23	2
PIC	Made	22	10	30
	Refused/withdrawn	-	-	-
	Issued	22	10	30
SA POLICE	Made	-	1	3
	Refused/withdrawn	-	-	-
	Issued	-	1	3
TAS POLICE	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
VIC POLICE	Made	56	56	43
	Refused/withdrawn	-	-	-
	Issued	56	56	43
WA POLICE	Made	25	29	51
	Refused/withdrawn	-	-	-
	Issued	25	29	51
TOTAL [paragraph 100(2)(c)]	**Made**	**544**	**551**	**470**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**544**	**551**	**470**

Applications for telecommunications interception warrants authorising entry onto premises

4.11 Subsection 48(1) of the TIA Act provides that an application for a telecommunications interception warrant may include a request that the warrant authorise entry onto premises. Paragraphs 100(1)(d) and (2)(d) of the TIA Act provide that the report must set out the number of applications for warrants that include requests for authorisation of entry onto premises. This information is set out in Table 4.

4.12 Agencies sought and were issued with a very small number of such warrants, which is consistent with the last three reporting periods.

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

AGENCY	RELEVANT STATISTICS	WARRANTS AUTHORISING ENTRY ON PREMISES		
		06/07	07/08	08/09
AFP	Made	3	7	7
	Refused/withdrawn	-	-	-
	Issued	3	7	7
ICAC	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
CCC WA	Made	-	1	2
	Refused/withdrawn	-	-	-
	Issued	-	1	2
NSW CC	Made	1	-	5
	Refused/withdrawn	-	-	-
	Issued	1	-	5
PIC	Made	3	-	3
	Refused/withdrawn	-	-	-
	Issued	3	-	3
VIC POLICE	Made	3	-	-
	Refused/withdrawn	-	-	-
	Issued	3	-	-
TOTAL [paragraph 100(2)(d)]	Made	11	8	17
	Refused/withdrawn	-	-	-
	Issued	11	8	17

Telecommunications interception warrants issued with specific conditions or restrictions

4.13 Subsection 49(1) of the TIA Act provides that a telecommunications interception warrant may specify conditions and restrictions regarding the interception of communications under that warrant. Paragraphs 100(1)(e) and (2)(e) of the TIA Act provide that the number of warrants issued with conditions and restrictions must be set out in the report. This information is set out in Table 5.

4.14 There was a significant decrease (47%) in the number of warrants issued with conditions or restrictions when compared to the previous reporting period. The ability to impose conditions or restrictions is at the discretion of the issuing authority.

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

AGENCY	WARRANTS ISSUED WITH CONDITIONS OR RESTRICTIONS		
	06/07	07/08	08/09
ACC	1	2	-
AFP	11	1	5
ICAC	1	-	2
NSW CC	61	26	10
NSW POLICE	12	13	4
PIC	1	3	-
TAS POLICE	-	-	3
TOTAL [paragraph 100(2)(e)]	**87**	**45**	**24**

Interpretative note relating to telecommunications interception warrants issued with specific conditions or restrictions

4.15 The decrease in telecommunications interception warrants issued with specific conditions or restrictions is attributable to an operational shift in obtaining warrants over mobile phones as opposed to landlines. This overcomes privacy issues which arise when a third party other than the target may be captured using a landline which is under interception.

Named person warrants

4.16 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.

4.17 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 decreased by approximately 9% from the number of warrants issued in the previous reporting period. The number of renewal applications for named person warrants decreased by approximately 15% from the previous reporting period. No named person warrants authorised entry onto premises during the reporting period.

Interpretative note relating to named person warrants

4.18 The decrease in named person warrants is attributable to operational priorities and the ability of interception agencies to obtain individual service warrants over services which a person may be using. 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		
		06/07	07/08	08/09
ACC	Made	115	99	103
	Refused/withdrawn	-	-	-
	Issued	115	99	103
AFP	Made	84	131	113
	Refused/withdrawn	-	1	-
	Issued	84	130	113
CCC WA	Made	-	3	2
	Refused/withdrawn	-	-	-
	Issued	-	3	2
ICAC	Made	2	-	1
	Refused/withdrawn	-	-	-
	Issued	2	-	1
NSW POLICE	Made	19	41	28
	Refused/withdrawn	-	1	-
	Issued	19	40	28
NSW CC	Made	33	57	60
	Refused/withdrawn	-	-	1
	Issued	33	57	59
NT POLICE	Made	5	7	7
	Refused/withdrawn	-	-	-
	Issued	5	7	7
OPI	Made	3	10	10
	Refused/withdrawn	-	-	-
	Issued	3	10	10
PIC	Made	-	-	4
	Refused/withdrawn	-	-	-
	Issued	-	-	4
SA POLICE	Made	8	10	6
	Refused/withdrawn	-	-	-
	Issued	8	10	6
TAS POLICE	Made	2	-	1
	Refused/withdrawn	-	-	-
	Issued	2	-	1
VIC POLICE	Made	82	90	66
	Refused/withdrawn	-	-	-
	Issued	82	90	66
WA POLICE	Made	27	30	33
	Refused/withdrawn	-	-	-
	Issued	27	30	33
TOTAL [paragraph 100(ea)]	**Made**	**380**	**478**	**434**
	Refused/withdrawn	**-**	**2**	**1**
	Issued	**380**	**476**	**433**

Table 7—Telephone applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
TAS POLICE	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
VIC POLICE	Made	5	5	4
	Refused/withdrawn	-	-	-
	Issued	5	5	4
TOTAL [paragraph 100(ed)]	**Made**	**6**	**5**	**4**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**6**	**5**	**4**

Table 8—Renewal applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
ACC	Made	39	40	30
	Refused/withdrawn	-	-	-
	Issued	39	40	30
AFP	Made	17	43	40
	Refused/withdrawn	-	-	-
	Issued	17	43	40
NSW CC	Made	5	13	14
	Refused/withdrawn	-	-	-
	Issued	5	13	14
NSW POLICE	Made	5	14	13
	Refused/withdrawn	-	-	0
	Issued	5	14	13
NT POLICE	Made	-	-	3
	Refused/withdrawn	-	-	-
	Issued	-	-	3
OPI	Made	-	6	-
	Refused/withdrawn	-	-	-
	Issued	-	6	-
SA POLICE	Issued	-	-	2
	Refused/withdrawn	-	-	-
	Issued	-	-	2
VIC POLICE	Made	13	24	9
	Refused/withdrawn	-	-	-
	Issued	13	24	9
WA POLICE	Made	5	4	11
	Refused/withdrawn	-	-	-
	Issued	5	4	11
TOTAL [paragraph 100(ed)]	**Made**	**84**	**144**	**122**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**84**	**144**	**122**

Table 9—Named person warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS WITH CONDITIONS		
		06/07	07/08	08/09
ACC	Issued	1	1	-
AFP	Issued	-	-	1
NSW CC	Issued	-	-	1
TOTAL [paragraph 100(2)(ea)]	**Issued**	**1**	**1**	**2**

4.19 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.

4.20 This information is included in Table 10.

Table 10—Number of services intercepted under named person warrants

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		06/07	07/08	08/09
ACC	1 service only	28	31	29
	2 – 5 services	76	59	66
	6 – 10 services	8	6	8
	10+ services	3	1	-
AFP	1 service only	17	27	13
	2 – 5 services	48	73	91
	6 – 10 services	9	18	10
	10+ services	2	8	2
CCC WA	1 service only	-	-	-
	2 – 5 services	-	2	2
	6 – 10 services	-	1	-
	10+ services	-	-	-

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		06/07	07/08	08/09
ICAC	1 service only	-	-	-
	2 – 5 services	-	2	1
	6 – 10 services	-	-	-
	10+ services	-	-	-
NSW CC	1 service only	5	12	9
	2 – 5 services	17	34	42
	6 – 10 services	11	10	8
	10+ services	-	1	-
NSW POLICE	1 service only	5	11	6
	2 – 5 services	17	29	20
	6 – 10 services	2	-	1
	10+ services	-	-	-
NT POLICE	1 service only	-	1	1
	2 – 5 services	3	5	5
	6 – 10 services	2	1	1
	10+ services	-	-	-
OPI	1 service only	-	1	1
	2 – 5 services	3	8	8
	6 – 10 services	-	1	1
	10+ services	-	-	-
PIC	1 service only	-	-	-
	2 – 5 services	-	-	2
	6 – 10 services	-	-	2
	10+ services	-	-	-
SA POLICE	1 service only	1	5	3
	2 – 5 services	6	4	3
	6 – 10 services	1	1	-
	10+ services	-	-	-
TAS POLICE	1 service only	-	-	-
	2 – 5 services	2	-	1
	6 – 10 services	-	-	-
	10+ services	-	-	-
VIC POLICE	1 service only	15	24	12
	2 – 5 services	70	60	46
	6 – 10 services	7	6	8
	10+ services	-	-	-
WA POLICE	1 service only	5	5	5
	2 – 5 services	18	17	19
	6 – 10 services	4	8	5
	10+ services	-	-	3
TOTAL [paragraph 100(2)(eb)]	**1 service only**	**76**	**117**	**79**
	2 – 5 services	**260**	**293**	**306**
	6 – 10 services	**44**	**52**	**44**
	10+ services	**5**	**10**	**5**

4.21 In previous reporting periods, paragraphs 100(1)(ec) and (2)(ec) of the TIA Act required the report to include, for each agency and in total, the total number of services and devices intercepted under named person warrants. This information is included in Table 11. From 1 July 2008 the TIA requires information in relation to named person warrants to distinguish between service based named person warrants and device based named person warrants. Accordingly, Table 11 will not be included in future reports.

4.22 Paragraphs 100(1)(ec) and 100(2)(ec) of the TIA Act now 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 12 and 13.

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

AGENCY	TOTAL NUMBER OF SERVICES INTERCEPTED	
	06/07	07/08
ACC	374	249
AFP	248	619
CCC WA	-	18
ICAC	-	6
NSW CC	131	205
NSW POLICE	88	92
NT POLICE	28	26
OPI	9	38
SA POLICE	31	24
TAS POLICE	9	-
VIC POLICE	246	231
WA POLICE	87	119
TOTAL	**1,251**	**1,627**

Table 12—Total number of services intercepted under *service* based named person warrants

AGENCY	TOTAL NUMBER OF SERVICES INTERCEPTED
	08/09
ACC	285
AFP	416
CCC WA	8
ICAC	2
NSW CC	209
NSW POLICE	70
NT POLICE	25
OPI	37
PIC	22
SA POLICE	9
TAS POLICE	3
VIC POLICE	225
WA POLICE	150
TOTAL	**1,461**

Table 13—Total number of services and devices intercepted under *device* based named person warrants

AGENCY	SERVICES	DEVICES
	08/09	08/09
AFP	-	16
NSW POLICE	-	1
VIC POLICE	-	1
TOTAL	**-**	**18**

B-Party warrants

4.23 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.

4.24 Paragraph 100(2)(ed) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 14 to 17 set out the information supplied by intercepting agencies regarding B-Party warrants. There has been a 24% decrease of applications for B-Party warrants since the last reporting period. This decrease can be attributed to operational needs of agencies.

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

Table 14—Applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		06/07	07/08	08/09
ACC	Made	-	2	1
	Refused/withdrawn	-	-	-
	Issued	-	2	1
AFP	Made	7	15	8
	Refused/withdrawn	-	-	-
	Issued	7	15	8
CCC WA	Made	-	3	-
	Refused/withdrawn	-	-	-
	Issued	-	3	-
ICAC	Made	1	3	1
	Refused/withdrawn	-	-	-
	Issued	1	3	1
NSW CC	Made	18	22	13
	Refused/withdrawn	-	-	-
	Issued	18	22	13
NSW POLICE	Made	39	26	40
	Refused/withdrawn	-	-	-
	Issued	39	26	40
OPI	Made	-	10	3
	Refused/withdrawn	-	-	-
	Issued	-	10	3
SA POLICE	Made	-	-	2
	Refused/withdrawn	-	-	-
	Issued	-	-	2
VIC POLICE	Made	5	15	5
	Refused/withdrawn	-	-	-
	Issued	5	15	5
WA POLICE	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
TOTAL [paragraph 100(2)(ed)]	**Made**	**71**	**96**	**73**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**71**	**96**	**73**

Table 15—Telephone applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		06/07	07/08	08/09
NSW POLICE	Made	7	7	5
	Refused/withdrawn	-	-	-
	Issued	7	7	5
VIC POLICE	Made	2	2	-
	Refused/withdrawn	-	-	-
	Issued	2	2	-
TOTAL [paragraph 100(2)(ed)]	**Made**	**9**	**9**	**5**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**9**	**9**	**5**

Table 16—Renewal applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		06/07	07/08	08/09
AFP	Made	2	1	4
	Refused/withdrawn	-	-	-
	Issued	2	1	4
NSW CC	Made	-	2	-
	Refused/withdrawn	-	-	-
	Issued	-	2	-
NSW POLICE	Made	4	-	2
	Refused/withdrawn	-	-	-
	Issued	4	-	2
VIC POLICE	Made	-	8	-
	Refused/withdrawn	-	-	-
	Issued	-	8	-
TOTAL [paragraph 100(2)(ed)]	**Made**	**6**	**11**	**6**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**6**	**11**	**6**

Table 17— B-Party warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		06/07	07/08	08/09
ICAC	Issued	-	-	1
TOTAL [paragraph 100(2)(ed)]	**Issued**	**-**	**-**	**1**

Interpretative note relating to B-Party warrants

4.26 These statistics demonstrate that B-Party warrants are only used sparingly. Of the thirteen agencies that were issued telecommunications interception warrants during the reporting period, only eight applied for and were issued B-Party warrants, with B-Party warrants representing approximately 2% of the total number of warrants issued.

4.27 It is important to note that only 6 of the 73 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

4.28 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.

4.29 The information required by paragraphs 100(1)(f) and (g) is set out in Tables 18 to 30. As in previous years, agencies obtained the majority of warrants to assist with investigations into drug-related offences.

4.30 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 18—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		
	06/07	07/08	08/09
ACC special investigations	208	160	153
Serious drug offences	3	16	1
Serious fraud or loss of revenue	-	3	-

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		
	06/07	07/08	08/09
Bribery or corruption	9	-	1
Child pornography	31[5]	-	-
Cybercrime	4	1	3
Kidnapping	5	4	4
Money laundering	48	106	104
Murder	1	2	21
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	-	3	-
Organised crime	11	16	26
People smuggling or sexual servitude	5	5	19
Serious drug offences	387	361	282
Serious fraud or loss of revenue	20	13	12
Serious personal injury or loss of life	21	14	27
Serious damage to property	3	5	-
Terrorism	28	10	91
Telecommunications offences	31[6]	3	11

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	06/07	07/08	08/09
Bribery or corruption	122	102	19
Child pornography	-	-	10
Cybercrime	-	3	27
Serious drug offences	-	-	11

[5] There was an error in the information provided in the 2006-2007 Annual Report. The category of child pornography was recorded as 31, when it should have read zero.

[6] The category of telecommunications offences was entered as zero, when it should have read 31.

Table 21—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		
	06/07	07/08	08/09
Bribery or corruption	33	30	32
Serious fraud or loss of revenue	-	3	-

Table 22—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		
	06/07	07/08	08/09
Cybercrime	15	-	6
Kidnapping	-	-	9
Money laundering	123	142	26
Murder	57	64	47
Administration of justice[7]	14	-	-
Organised crime	130	40	33
Serious damage to property	17	13	-
Serious drug offences	555	474	478
Serious fraud or loss of revenue	-	27	24
Serious personal injury or loss of life	25	16	16

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

Table 23—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		
	06/07	07/08	08/09
Bribery or corruption	26	33	10
Child pornography	-	5	-
Kidnapping	40	27	14
Murder	216	231	237
Organised crime	106	120	165
Serious damage to property	38	57	30
Serious drug offences	180	145	147
Serious fraud or loss of revenue	14	7	19
Serious personal injury or loss of life	265	208	194
Terrorism	-	19	10

Table 24—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		
	06/07	07/08	08/09
Murder	8	4	3
Organised crime	-	1	-
Serious drug offences	19	32	42
Serious personal injury or loss of life	-	2	-

Table 25—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		
	06/07	07/08	08/09
Bribery or corruption	3	68	58
Murder	10	11	-
Serious drug offences	3	1	-
Serious personal injury or loss of life	-	-	7

Table 26—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		
	06/07	07/08	08/09
Bribery or corruption	36	65	98
Money laundering	-	11	7
Murder	3	-	-
Organised crime	2	3	-
Serious drug offences	3	1	10
Serious personal injury or loss of life	-	12	-

Table 27—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		
	06/07	07/08	08/09
Bribery or corruption	5	4	-
Cybercrime	-	-	3
Kidnapping	-	1	-
Murder	12	37	23
Administration of justice[8]	14	-	4
Serious arson	-	-	1
Serious damage to property	3	3	-
Serious drug offences	57	71	65
Serious fraud or loss of revenue	7	-	6
Serious personal injury or loss of life	11	8	3

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

Table 28—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		
	06/07	07/08	08/09
Bribery or corruption	-	3	-
Murder	-	3	2
Serious drug offences	13	5	8
Serious fraud or loss of revenue	-	3	-
Serious personal injury of loss of life	-	3	5

Table 29—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		
	06/07	07/08	08/09
Bribery or corruption	3	-	28
Kidnapping	5	1	3
Murder	99	118	63
Organised crime	4	4	-
Serious arson	-	-	2
Serious damage to property	4	6	-
Serious drug offences	163	180	170
Serious fraud or loss of revenue	-	3	-
Serious personal injury or loss of life	88	61	65

Table 30—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		
	06/07	07/08	08/09
Bribery or corruption	3	5	9
Child pornography	1	-	9
Kidnapping	1	-	8
Money laundering	21	5	1
Murder	13	29	38
Organised crime	-	2	2
Serious damage to property	2	2	-
Serious drug offences	111	134	177
Serious fraud or loss of revenue	-	7	11
Serious personal injury or loss of life	15	15	32
Terrorism	5	-	-

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

4.31 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 31.

Table 31—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		
	06/07	07/08	08/09
ACC special investigations[9]	208	160	153
Administration of justice[10]	14	-	4
Bribery or corruption	240	310	255
Child pornography	32	5	19
Cybercrime	19	4	39
Kidnapping	51	33	38
Money laundering	192	264	138
Murder	419	499	434
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995*	-	3	-
Organised crime	253	186	226
People smuggling or sexual servitude	5	5	19
Serious arson	-	-	3
Serious damage to property	67	86	30
Serious drug offences	1494	1420	1391
Serious fraud or loss of revenue	34	66	72
Serious personal injury or loss of life	425	339	349
Telecommunications offences	-	3	11
Terrorism	33	29	101

[9] Applies only to the ACC.

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

Duration of telecommunications interception warrants

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

Duration of original telecommunications interception warrants

4.33 Paragraph 101(1)(a) of the TIA Act provides that the report must set out the average period specified in original telecommunications interception warrants in relation to each agency. Paragraph 101(1)(b) provides that the report must set out the average of the periods for which those warrants were actually in force. Paragraphs 101(2)(a) and (b) provide that the same information must be averaged across all agencies. This information is set out in Table 32.

4.34 The average duration of warrants, both specified and actual, has increased overall. However the average duration has increased for some agencies while it has decreased for others, meaning that there is no general trend relating to the duration of warrants.

4.35 However, as in previous reporting periods, the average actual duration of warrants is again significantly less than the average specified duration of warrants, meaning that agencies continue to regularly review warrants and revoke those that are no longer required prior to their expiration. This demonstrates that agencies do not intercept telecommunications services longer than they need to for their investigations.

Table 32—Duration of original telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	06/07	07/08	08/09	06/07	07/08	08/09
ACC	89	87	89	58	57	62
AFP	76	77	73	46	41	49
CCC OF WA	85	77	90	62	49	80
ICAC	88	79	83	55	61	55
NSW CC	79	82	85	48	53	52
NSW POLICE	49	46	49	29	37	46
NT POLICE	68	83	86	51	69	66
OPI	89	76	70	64	67	44
PIC	87	88	89	69	77	76
SA POLICE	78	82	74	48	55	61
TAS POLICE	75	54	74	59	18	46
VIC POLICE	58	52	52	45	37	43
WA POLICE	57	64	62	39	41	39
AVERAGE [paragraphs 101(2)(a)-(b)]	**67**	**68**	**69**	**48**	**46**	**55**

Duration of renewal telecommunications interception warrants

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

Table 33—Duration of renewal of telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	06/07	07/08	08/09	06/07	07/08	08/09
ACC	42	90	83	60	71	68
AFP	88	89	87	70	73	73
CCC WA	90	90	83	84	71	85
ICAC	90	74	90	32	51	22
NSW CC	71	76	86	46	54	60
NSW POLICE	50	52	55	48	59	47
NT POLICE	60	-	90	60	-	90
OPI	90	85	45	-[11]	84	41
PIC	88	90	90	79	83	71
SA POLICE	-	90	60	-	42	60
TAS POLICE	90	-	-	47	-	-
VIC POLICE	67	55	59	51	48	52
WA POLICE	53	68	64	47	61	49
AVERAGE [paragraphs 101(2)(a)-(b)]	**66**	**74**	**74**	**51**	**62**	**56**

[11] An average period was not recorded as the warrant was still in force at the end of the reporting period.

Interpretative note relating to average duration of warrants across all agencies

4.37 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.

4.38 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

4.39 As with all telecommunications interception warrants, a B-Party warrant must specify the period for which it is to be in force and may be revoked before the specified period lapses. The obligation on the chief officer of an agency to revoke a B-Party warrant where he or she is satisfied that the grounds on which the warrant was issued have ceased to exist is particularly important in the case of B-Party warrants. For example, if a B-Party warrant was issued because the telecommunications service of the target was not able to be identified, once the service is identified, the warrant must be revoked.

4.40 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 34.

Table 34—Duration of original B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	06/07	07/08	08/09	06/07	07/08	08/09
ACC	-	26	45	-	4	13
AFP	45	36	45	21	19	44
CCC WA	-	45	-	-	15	-
ICAC	45	15	45	0[12]	15	45
NSW CC	45	42	42	21	28	15
NSW POLICE	32	22	27	22	18	18
OPI	-	45	34	-	16	21
SA POLICE	-	-	30	-	-	30
VIC POLICE	34	34	45	28	25	16
WA POLICE	30	-	-	26	-	-
AVERAGE [paragraph 101(2)(da)]	**38**	**33**	**34**	**25**	**23**	**21**

[12] No actual duration is known as the warrant was still in force at the end of the reporting period.

Duration of renewal B-Party warrants

4.41 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 35.

Table 35—Duration of renewal of B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	06/07	07/08	08/09	06/07	07/08	08/09
AFP	45	45	45	45	40	42
NSW CC	43	44	-	43	32	-
NSW POLICE	35	-	30	35	-	29
VIC POLICE	-	45	-	-	45	-
AVERAGE [paragraphs 101(2)(da)]	**39**	**45**	**40**	**39**	**42**	**38**

Number of final renewals of telecommunications interception warrants

4.42 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.

4.43 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 36.

4.44 The figures in Table 36 show slight increases in 90 and 150 day renewals, and a decrease in 180 day renewals. This is consistent with operational activities.

Table 36—Number of 'final renewals'

AGENCY	90 DAYS			150 DAYS			180 DAYS		
	06/07	07/08	08/09	06/07	07/08	08/09	06/07	07/08	08/09
ACC	1	7	7	5	14	7	23	10	7
AFP	7	10	18	30	30	24	9	31	37
CCC WA	-	5	-	-	1	-	27	10	-
ICAC	3	4	2	-	2	-	-	-	-
NSW CC	7	4	6	3	3	7	-	3	2
NSW POLICE	32	41	50	8	7	6	2	2	11
NT POLICE	-	-	-	3	-	-	-	-	1
OPI	-	3	1	-	3	-	-	7	-
PIC	-	2	8	5	-	8	10	1	5
SA POLICE	-	3	2	-	-	1	-	-	-
TAS POLICE	1	-	-	-	-	-	-	-	-
VIC POLICE	22	18	17	12	9	2	7	1	2
WA POLICE	8	7	13	13	1	28	1	10	1
TOTAL [paragraph 101(2)(e)]	**81**	**104**	**124**	**79**	**70**	**83**	**79**	**75**	**66**

Effectiveness of telecommunications interception warrants

4.45 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.

4.46 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.

4.47 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.

4.48 The communication of that information may result in further investigation and possibly arrests and prosecution by an eligible authority on the basis of lawfully intercepted information. That is notwithstanding that the authority is itself unable to obtain a warrant. An example of such a situation might be the interception under warrant by a Commonwealth agency of information pointing to the commission of a State offence where the police force of that State has not been declared to be an interception agency for the purposes of the TIA Act but is an eligible authority. In these circumstances, it may be possible for the Commonwealth agency to communicate the information to the State police service in accordance with Part 2-6 of the TIA Act.

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

- the Queensland Police
- the Queensland Crime and Misconduct Commission
- the Inspector of the Police Integrity Commission
- the Inspector of the Independent Commission against Corruption, and
- the Parliamentary Inspector of the Corruption and Crime Commission of Western Australia.

Arrests on the basis of lawfully intercepted information

4.50 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.

4.51 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 37. The number of arrests made during the reporting period represents a 17% decrease on the figures reported during 2007-08.

Table 37—Arrests on the basis of lawfully intercepted information

AGENCY	NUMBER OF ARRESTS		
	06/07	07/08	08/09
ACC	116	166	133
AFP	99	165	133
CCC WA	5	3	1
CMC	66	231[13]	-
ICAC	-	-	-
NSW CC	438	306	175
NSW POLICE	345	321	402
NT POLICE	18	27	31
OPI	-	-	1
PIC	2	85	139[14]
QLD POLICE	-	18	48[15]
SA POLICE	76	67	89
TAS POLICE	6	7	9
VIC POLICE	439	493	420
WA POLICE	131	167	134
TOTAL [paragraph 102(2)(a)]	**1,741**	**2,056**	**1,715**

[13] As the CMC was not entitled to apply for warrants under the TIA Act during the reporting period, it obtained access to TI material through joint operations with other law enforcement agencies. Therefore the statistics supplied by the CMC may duplicate or be included in the totals supplied by those agencies.
[14] This figure is drawn from court attendance notices. The 139 charges relate to 5 persons.
[15] As the Qld Police was not entitled to apply for warrants under the TIA Act during the reporting period, it obtained access to TI material through joint operations with other law enforcement agencies. Therefore the statistics supplied by the Qld Police may duplicate or be included in the totals supplied by those agencies.

Prosecutions in which lawfully intercepted information was given in evidence

4.52 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 38 to 40.

4.53 During the reporting period, there was a 26% decrease in the number of prosecutions commenced and a 17% decrease in the number of convictions obtained on the basis of lawfully intercepted information.

4.54 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.

4.55 In these tables, the category ‘other offences’ refers to any other offence punishable by imprisonment for life or for a period of at least 3 years, or to any related ancillary offences. It should also be noted that, to assist readability, the categories of offences in the tables are grouped thematically.

Table 38—Prosecutions in which lawfully intercepted information used in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC WA	ICAC	NSW CC	NSW POL	NT POL	OPI	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
Administration of Justice		1			1				2						**4**
Bribery or corruption		1	21					3			5		2		**32**
Child pornography		5				45					1			1	**52**
Conspiring	4	4													**8**
Kidnapping					1	20							1		**22**
Money laundering	2	16			27						2				**47**
Murder		3				49					10		7		**69**
Organised crime					32	233			1				8	25	**299**
People Smuggling		3													**3**
Serious arson		2											1	2	**5**
Serious damage to property						25								3	**28**
Serious drug offences	23	113			225	551	9	4	9	11	111	9	289	677	**2,031**
Serious fraud or loss of revenue					55	43		1			2		1	24	**126**
Serious personal injury/ loss of life	1	4			1	268			1		7		39	23	**344**
Special Investigation of the ACCC		1					2								**3**
Terrorism		15													**15**
Other offences	32	11		28		76			20	4	2		77	82	**332**
TOTAL	**62**	**179**	**21**	**28**	**342**	**1,310**	**11**	**8**	**33**	**15**	**140**	**9**	**425**	**837**	**3,420**

Table 39—Convictions in which lawfully intercepted information given in evidence

CATEGORIES OF OFFENCES	ACC	AFP	CCC WA	ICAC	NSW CC	NSW POL	NT POL	OPI	PIC	SA POL	VIC POL	WA POL	TOTAL
Administration of Justice									2				**2**
Bribery or corruption		1	8					1			2		**12**
Child pornography						44						1	**45**
Kidnapping						5					1		**6**
Money laundering	2	2			20								**24**
Murder						29					3		**32**
Organised crime	0				22	148			1		8	4	**183**
Serious arson											1	1	**2**
Serious damage to property						24						3	**27**
Serious drug offences	20	14			157	320	9	4	9	44	288	396	**1,261**
Serious fraud or loss of revenue					46	34					1	2	**83**
Serious personal injury/ loss of life	1				1	170				2	38	8	**220**
Terrorism		6											**6**
Other offences	6			8		59			14	7	76	36	**206**
TOTAL	**29**	**23**	**8**	**8**	**246**	**833**	**9**	**5**	**26**	**53**	**418**	**451**	**2,109**

Table 40—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		
		06/07	07/08	08/09	06/07	07/08	08/09
ACC	Serious Offence	41	55	30	44	52	23
	Other[16]	24	5	32	18	5	6
	Agency Total	65	60	62	62	57	29
AFP	Serious Offence	99	136	168	19	14	23
	Other	17	6	11	-	-	-
	Agency Total	116	142	179	19	14	23
CCC WA	Serious Offence	-	3	21	-	3	8
	Other	18	2	-	18	2	-
	Agency Total	18	5	21	18	5	8
CMC	Serious Offence	216	231	-	37	49	-
	Other	11	26	-	5	12	-
	Agency Total	227	257	-	42	61	-
ICAC	Serious Offence	21	-	-	21	-	-
	Other	37	-	28	37	-	8
	Agency Total	58	-	28	58	-	8
NSW CC	Serious Offence	414	736	342	414	734	246
	Other	3	-	-	3	-	-
	Agency Total	417	736	342	417	734	246
NSW POLICE	Serious Offence	1,000	1,428	1,234	480	629	774
	Other	2	-	76	2	-	59
	Agency Total	1,002	1,428	1,310	482	629	833
NT POLICE	Serious Offence	-	21	11	-	9	9
	Other	-	-	-	-	-	-
	Agency Total	-	21	11	-	9	9
OPI	Serious Offence	-	-	8	-	-	5
	Other	-	-	-	-	-	-
	Agency Total	-	-	8	-	-	5
PIC	Serious Offence	15	20	13	15	20	12
	Other	9	8	20	9	8	14
	Agency Total	24	28	33	24	28	26
QLD POLICE	Serious Offence	-	20	11	-	2	-
	Other	-	-	4	-	-	-
	Agency Total	-	20	15	-	2	-
SA POLICE	Serious Offence	86	60	138	54	45	46
	Other	1	8	2	1	8	7
	Agency Total	87	68	140	55	53	53

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

AGENCY	CATEGORIES OF OFFENCES PROSECUTED	NUMBER OF OFFENCES PROSECUTED FOR EACH CATEGORY			NUMBER OF CONVICTIONS RECORDED FOR EACH CATEGORY		
		06/07	07/08	08/09	06/07	07/08	08/09
TAS POLICE	Serious Offence	3	4	9	-	-	-
	Other	13	-	-	-	-	-
	Agency Total	16	4	9	-	-	-
VIC POLICE	Serious Offence	220	295	348	216	280	342
	Other	81	167	77	78	162	76
	Agency Total	301	462	425	294	442	418
WA POLICE	Serious Offence	301	666	755	702	503	415
	Other	39	19	82	82	5	36
	Agency Total	340	685	837	784	508	451
TOTAL	**Serious Offence**	**2,445**	**3,675**	**3,088**	**2,008**	**2,340**	**1,903**
	Other	**228**	**241**	**332**	**247**	**202**	**206**
	Grand Total	**2,671**	**3,916**	**3,420**	**2,255**	**2,255**	**2,109**

Interpretative note relating to prosecutions and convictions statistics

4.56 The statistics presented in Tables 38 to 40 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.

4.57 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'

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

4.59 Subsection 102(3) of the TIA Act provides that the report must set out the number of eligible warrants issued to each agency during the reporting period and the percentage of warrants issued to that agency that were eligible warrants. An 'eligible warrant' is defined in subsection 102(3) as a warrant that was in force during the reporting period (not necessarily a warrant that was issued during the reporting period) where a prosecution was instituted or was likely to be instituted on the basis of information obtained by interceptions under the warrant.[17]

4.60 Subsection 102(4) of the TIA Act provides that the report must set out the percentage of each agency's total warrants in force during the reporting period, that were eligible warrants. These figures are set out in Table 41, and indicate a 1% decrease in the proportion of eligible warrants when compared to the previous reporting period.

Table 41—Percentage of 'eligible warrants'

AGENCY	NUMBER OF ELIGIBLE WARRANTS	TOTAL NUMBER OF WARRANTS	%
ACC	167	176	95
AFP	415	814	51
CCC WA	39	52	75
ICAC	22	32	69
NSW CC	589	724	81
NSW POLICE	741	927	80
NT POLICE	44	52	85
OPI	32	64	50
PIC	46	139	33
SA POLICE	83	105	79
TAS POLICE	5	12	42
VIC POLICE	287	375	77
WA POLICE	265	312	85
TOTAL [subsection 102(4)]	**2,735**	**3,784**	**72**

[17] If the warrant was a renewal, this includes information obtained under the original or any renewal of the original warrant; if the warrant was an original warrant, this includes information obtained under any renewal of that original warrant.

Emergency interception

4.61 Section 102A of the TIA Act provides that the report must set out the number of occasions on which an officer or staff member of the agency intercepted a communication in reliance on subsection 7(4) or (5) of the TIA Act. These provisions permit the 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.

4.62 An interception in reliance on subsection 7(4) of the TIA Act may be carried out by an officer of one of the above agencies where the officer is a party to the communication, and because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a telecommunications interception warrant to be made. 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, or
- threatened to kill or seriously injure another person or to cause serious damage to property, or
- threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety.

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

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

4.65 In the reporting period no interceptions were carried out in reliance on subsection 7(5). The information required by section 102A is set out in Table 42.

Table 42—Interceptions made in reliance on subsection 7(5) of the TIA Act

SUSPICION OF	AFP			NSW POLICE		
	06/07	07/08	08/09	06/07	07/08	08/09
An act that may result in loss of life or serious injury	-	-	-	-	2	-
Threat to kill or seriously injure	-	2	-	-	-	-
TOTAL	**-**	**2**	**-**	**-**	**2**	**-**

Other information

Total expenditure incurred by agencies

4.66 Paragraph 103(a) of the TIA Act provides that the report include details of the total expenditure (including expenditure of a capital nature) incurred by agencies in connection with the execution of telecommunications interception warrants for law enforcement purposes. The information required by this subsection is set out in Table 43.

4.67 Total expenditure incurred by agencies in connection with telecommunications interception increased by approximately 15% from the previous reporting period.

Table 43—Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants

AGENCY	TOTAL EXPENDITURE ($)		
	06/07	07/08	08/09
ACC	5,452,586	5,078,973	5,767,648
AFP	6,128,468	8,256,034	8,221,162
CCC WA	1,649,035	1,638,018	1,817,120
ICAC	180,861	236,021	214,446
NSW CC	4,043,947	4,274,442	4,473,035
NSW POLICE	4,331,722	4,268,907	8,019,292
NT POLICE	1,545,000	886,000	693,458
OPI	1,358,331	1,914,644	1,671,170
PIC	1,887,274	1,189,530	1,351,587
SA POLICE	2,041,918	2,492,495	2,656,404
TAS POLICE	442,000	548,000	3,258
VIC POLICE	4,298,337	4,145,055	4,483,582
WA POLICE	3,209,047	1,810,687	2,816,442
TOTAL	**36,568,526**	**36,738,806**	**42,188,604**

Average expenditure per telecommunications interception warrant

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

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

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.

4.69 The average expenditure incurred by agencies per warrant over the reporting period is presented in Table 44.

Table 44—Average expenditure per telecommunications interception warrant

AGENCY	AVERAGE EXPENDITURE ($)		
	06/07	07/08	08/09
ACC	25,842	28,374	37,452
AFP	11,477	15,577	14,373
CCC WA	13,517	16,059	37,084
ICAC	5,481	7,152	6,701
NSW CC	5,132	6,361	7,226
NSW POLICE	5,008	5,264	9,650
NT POLICE	57,222	23,946	15,410
OPI	97,024	24,547	25,710
PIC	47,182	13,072	11,753
SA POLICE	21,494	20,101	25,299
TAS POLICE	34,000	32,235	217
VIC POLICE	11,744	11,113	13,546
WA POLICE	18,657	9,099	9,813

Availability of eligible judges and nominated AAT members

4.70 Paragraph 103(ab) of the TIA Act provides that the report must set out information about the availability of Judges to issue telecommunications interception warrants and the extent to which nominated AAT members have been used for that purpose. This information is set out in Tables 45 and 46.

Table 45—Availability of Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT Members to issue telecommunications interception warrants[18]

ISSUING AUTHORITY	NUMBER ELIGIBLE
FEDERAL COURT JUDGES	10
FAMILY COURT JUDGES	12
FEDERAL MAGISTRATES	34
NOMINATED AAT MEMBERS	37

4.71 During the reporting period, approximately 86.7% of telecommunications interception warrants were issued by AAT members, 9% by Family Court Judges, 4% by Federal Magistrates and 0.3% 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.

[18] 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.

Table 46—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	-	-	10	144
AFP	-	-	45	527
CCC WA	-		-	49
ICAC	-	-	-	32
NSW CC	-	-	23	596
NSW POLICE	-	3	22	806
NT POLICE	10	-	31	4
OPI	-	-	-	65
PIC	-	-	-	115
SA POLICE	-	-	-	105
TAS POLICE	-	-	-	15
VIC POLICE	-	-	-	331
WA POLICE	-	282	-	5
TOTAL	**10**	**285**	**131**	**2,794**

Interceptions on behalf of other agencies

4.72 Paragraph 103(ac) of the TIA Act provides that the report must set out the number (if any) of interceptions carried out by each agency on behalf of other agencies. Table 47 sets out the number of interceptions executed by agencies on behalf of other agencies during the reporting period.

4.73 The main circumstances in which this type of interception occurs is where a larger agency assists a smaller agency to intercept to reduce the costs of the smaller agency, or where, due to a higher than usual number of warrants or a system failure, an agency is required to utilise another agency's facilities.

Table 47—Number of interceptions carried out on behalf of other agencies[19]

INTERCEPTION CARRIED OUT BY	INTERCEPTION CARRIED OUT ON BEHALF OF	
	TASMANIA POLICE	TOTAL
VIC POLICE	18	18

[19] SA Police has been removed from the 'interception carried out by' column as they did not perform interception for another agency in the reporting period. ACC has been removed from the 'interception carried out on behalf of' column as they did not have another interception agency carry out interception on their behalf in the reporting period.

Resources devoted to telecommunications interception

4.74 In addition to the total expenditure figures provided in Table 43, the figures in Table 48 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 48—Recurrent costs of interceptions per agency

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL ($)
ACC	3,984,087	27,171	1,162,513	593,877	**5,767,648**
AFP	5,740,585	142,693	811,592	1,484,565	**8,179,435**
CCC WA	1,538,711	-	127,424	150,985	**1,817,120**
ICAC	72,337	37,690	-	104,419	**214,446**
NSW CC	2,287,448	58,191	605,909	1,521,486	**4,473,034**
NSW POLICE	3,114,860	419,136	4,000,000	485,296	**8,019,292**
NT POLICE	536,045	-	-	157,413	**693,458**
OPI	1,339,416	100,454	181,000	50,300	**1,671,170**
PIC	1,205,022	-	52,130	99,435	**1,356,587**
SA POLICE	2,143,390	254,624	134,719	123,672	**2,656,405**
TAS POLICE	349,395	53,000	66,380	3,258	**472,033**
VIC POLICE	3,515,453	439,373	154,072	374,684	**4,483,582**
WA POLICE	2,293,167	317,644	-	205,631	**2,816,442**

Emergency services facility declarations

4.75 Paragraph 103(ad) of the TIA Act provides that the report must include the number and type of premises for each State and Territory that have been declared by the Attorney-General to be emergency services facilities pursuant to subsection 6(2A) of the TIA Act during the reporting period. The declarations enable such facilities to record incoming and outgoing calls without a telecommunications interception warrant. Table 49 provides the required information.

Table 49—Emergency service facility declarations

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

Reports by Commonwealth Ombudsman

4.76 The Commonwealth Ombudsman has the function of inspecting the records of Commonwealth interception agencies and reporting to the Attorney-General regarding the outcome of those inspections. Paragraph 103(ae) of the TIA Act provides that a summary of the information included in the Ombudsman's report must be included in this report, including:

- a summary of the inspections conducted during the financial year under section 83 of the Act
- particulars of any deficiencies identified that impact on the integrity of the telecommunications interception regime, and
- particulars of any remedial action taken or proposed to be taken to address those deficiencies.

4.77 The Ombudsman completed two inspections each of the ACC's and AFP's records during the reporting period. The reports concluded that there was generally a high degree of compliance with the detailed record keeping requirements of the TIA Act. Both agencies implemented a range of measures to improve compliance with reporting obligations under the TIA Act.

The ACC

4.78 The Ombudsman identified a deficiency relating to 'use and communication logs' not containing sufficient detail. The ACC advised that it has revised its procedures to enhance compliance with the Act and is further reviewing policies. The ACC is also reviewing procedures in relation to the dissemination of information.

4.79 The Ombudsman reported delays in relation to the sending of certified true copies of interception warrants and instruments of revocation to carriers as required by the TIA Act. The ACC advised that it will review its procedures in this regard.

4.80 The Ombudsman was unable to verify if the ACC had provided all reports to the Attorney-General under sections 94(2) and 94B of the TIA Act within the statutory timeframe. The ACC will continue to use a quality assurance process to reinforce its compliance with these obligations.

4.81 The Ombudsman found several instances where warrants were applied for, and issued to ACC staff members who were not eligible to obtain warrants. The ACC has made changes which will require applicants for TI warrants to confirm their status as persons who are eligible to apply for warrants.

The AFP

4.82 The Ombudsman identified deficiencies in relation 'use and communication logs' not containing sufficient details. The AFP advised it is reviewing its procedures in this regard.

4.83 The Ombudsman reported delays in relation to the sending of certified true copies of interception warrants and instruments of revocation to carriers. The AFP advised that ongoing reviews of processes will occur in this regard.

4.84 The Ombudsman reported a deficiency in the records relating to destruction, specifically the destruction dates of several restricted records and the nature of the document that was destroyed. The AFP has reviewed its procedures to enhance its record keeping processes.

4.85 The Ombudsman also noted that several warrants noted that two affidavits did not include rejected warrants. The AFP advised this was a technical issue, and a new database has been implemented to enable applicants to interrogate existing records more effectively. The database will enable applicants to identify all previous applications, including those that were rejected.

4.86 The Ombudsman found in one instance that information communicated to another agency was not reported to the Attorney-General, and in another two instances, the file held insufficient information to positively establish that the report was sent to the Attorney-General. The AFP advised that it will closely monitor it's business practices to support the AFP's legislative compliance.

Other information

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

CHAPTER 5—STORED COMMUNICATIONS INFORMATION REQUIRED UNDER THE ACT

The information required

5.1 The reporting requirements of the TIA Act in relation to accessing stored communications are contained in Part 3-6 of the Act, which provides that this report must include information on:

- the relevant statistics relating to applications for stored communication warrants that were made by the agency during the reporting period (paragraph 162(2)(a))
- the relevant statistics relating to telephone applications for stored communication warrants made by the agency during the reporting period (paragraph 162(2)(b))
- the relevant statistics relating to renewal warrants that were made by the agency during the reporting period (paragraph 162(2)(c))
- the number of warrants which were issued with specified conditions or restrictions (paragraph 162(2)(d))
- the number of arrests made during the reporting period based on lawfully intercepted information (paragraph 163(a)), and
- the number of proceedings which ended in the reporting period in which information collected by means of a warrant was given in evidence (paragraph 163(b)).

5.2 The TIA Act provides that the information must be set out in relation to each agency that is entitled to be issued with warrants authorising access to stored communications. In addition, the information must be combined for all agencies to indicate the overall extent and effectiveness of access to stored communications under the TIA Act.

5.3 It is possible for an enforcement agency to record arrests, proceedings in which lawfully accessed information was given in evidence or convictions based on lawfully accessed information where the agency has not applied for stored communications warrants. This can arise where an agency has received stored communications for purposes provided for by section 139 of the TIA Act but was not the agency that applied for the warrant.

Which agencies may seek stored communications warrants?

5.4 Any enforcement agency may apply for a stored communications warrant. The definition of enforcement agency includes criminal law enforcement agencies, civil penalty enforcement agencies or public revenue agencies. This includes all the bodies mentioned as interception agencies and eligible authorities for the purposes of telecommunications interception warrants, as well as other regulatory bodies such as the

- Australian Customs Service
- the Australian Securities and Investments Commission
- the Australian Competition and Consumer Commission
- the Australian Taxation Office, and
- Centrelink

Applications for stored communications warrants

5.5 Paragraphs 162(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting year for each agency and in total. This information is presented in Table 50. Only those enforcement agencies that applied for stored communications warrants during the reporting period are included in the table.

5.6 There was a 164% increase in the use of stored communications warrants in the reporting period. This increase was anticipated as more agencies became aware of the regime in the third year of its operation. Agencies utilised the stored communications regime to investigate serious contraventions.

5.7 It is expected that increases in the stored communications regime will continue as agencies become more familiar with the regime.

Table 50—Applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
ACC	Made	4	12	8
	Refused/withdrawn	-	-	-
	Issued	4	12	8
AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE	Made	1	1	9
	Refused/withdrawn	-	-	-
	Issued	1	1	9
AFP	Made	12	13	41
	Refused/withdrawn	-	-	0
	Issued	12	13	41
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	Made	-	1	6
	Refused/withdrawn	-	-	-
	Issued	-	1	6
CCC WA	Made	1	-	4
	Refused/withdrawn	-	-	-
	Issued	1	-	4
CMC	Made	-	-	29
	Refused/withdrawn	-	-	1
	Issued	-	-	28
NSW CC	Made	4	1	6
	Refused/withdrawn	-	-	-
	Issued	4	1	6
NSW POLICE	Made	24	27	26
	Refused/withdrawn	-	-	-
	Issued	24	27	26
NT POLICE	Made	-	6	-
	Refused/withdrawn	-	-	-
	Issued	-	6	-
OPI	Made	-	-	12
	Refused/withdrawn	-	-	-
	Issued	-	-	12
PIC	Made	-	3	-
	Refused/withdrawn	-	-	-
	Issued	-	3	-
QLD POLICE	Made	1	27	119
	Refused/withdrawn	1	-	-
	Issued	-	27	119
SA POLICE	Made	3	1	8
	Refused/withdrawn	-	-	-
	Issued	3	1	8

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
TAS POLICE	Made	1	8	36
	Refused/withdrawn	-	-	-
	Issued	1	8	36
VIC POLICE	Made	6	5	9
	Refused/withdrawn	-	-	-
	Issued	6	5	9
WA POLICE	Made	-	12	8
	Refused/withdrawn	-	-	-
	Issued	-	12	8
TOTAL [paragraph 162(2)(a)]	Made	57	117	321
	Refused/withdrawn	1	-	1
	Issued	56	117	320

Telephone applications for stored communications warrants

5.8 Paragraphs 162(1)(b) and (2)(b) of the TIA Act provide that the report must set out how many telephone applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and in total.

Table 51— Telephone applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
NSW POLICE	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1

Renewal applications for stored communications warrants

5.9 Paragraph 162(2)(c) of the TIA Act provides that the report must set out how many renewal applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting period for each agency and in total.

Table 52— Renewal applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
CMC	Made	-	-	15
	Refused/withdrawn	-	-	-
	Issued	-	-	15

Stored communications warrants subject to conditions or restrictions

5.10 Paragraph 162(2)(d) of the TIA Act provides that the report must set out how many stored communications warrants issued on application made during the reporting period specified conditions or restrictions, for each agency and in total.

Table 53—Stored communications warrants subject to conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		06/07	07/08	08/09
QLD POLICE	Made	-	-	20
	Refused/withdrawn	-	-	-
	Issued	-	-	20

Effectiveness of stored communications warrants

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

5.11 Section 163 of the TIA Act provides that the report must set out the number of arrests made on the basis of lawfully accessed information and the number of proceedings in which lawfully accessed information was given in evidence. This information is set out in Table 54. The table also includes the number of convictions recorded based on lawfully accessed information.

Table 54—Number of arrests, proceedings and convictions made on the basis of lawfully accessed information

AGENCY	ARRESTS			PROCEEDINGS			CONVICTIONS		
	06/07	07/08	08/09	06/07	07/08	08/09	06/07	07/08	08/09
AFP	-	-	27	-	-	5	-	-	-
NSW CC	6	-	-	-	-	-	-	-	-
NSW POLICE	13	7	21	1	1	24	1	1	19
QLD POLICE	-	36	69	-	-	1	-	-	1
SA POLICE	2	-	-	-	-	-	-	-	-
TAS POLICE	2	-	10	-	-	2	-	-	-
VIC POLICE	-	3	8	1	-	-	1	-	-
WA POLICE	-	-	4	-	-	-	-	-	-
TOTAL	**23**	**46**[20]	**139**	**2**	**1**	**32**	**2**	**1**	**20**

Interpretative note relating to prosecutions and convictions statistics

5.12 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.

5.13 Additionally, the information in table 54 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.

[20] The 2006-07 Annual Report incorrectly reported the total as '45'.

CHAPTER 6—TELECOMMUNICATIONS DATA - INFORMATION REQUIRED UNDER THE ACT

The information required

6.1 The reporting requirements of the TIA Act in relation to authorising the disclosure of telecommunications data are contained in Part 4-2 of the Act. Part 4-2 provides that this report must include information on:

- the number of authorisations made under section 178 (paragraph 186(1)(a))
- the number of authorisations made under section 179 (paragraph 186(1)(b))
- for criminal law-enforcement agencies – the number of authorisations made under section 180 (paragraph 186(1)(c)), and
- any other matter requested by the Minister in relation to those authorisations (paragraph 186(1)(d)).

Which agencies may authorise the disclosure of telecommunications data

6.2 Agencies 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 Communications Access Coordinator of the positions which can authorise the disclosure of telecommunications data.

Authorisations granted

6.4 The telecommunications data regime was transferred to the TIA Act on 1 November 2007. Therefore, statistics were sought from agencies for authorisations made from that date. The 2007-2008 statistics are lower than the 2008-2009 reporting period, because figures were only reported for part of the 2007-2008 reporting period.

6.5 The number of authorisations made for access to existing information or documents in the enforcement of the criminal law is given at Table 55. 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 56.

Table 55—Number of authorisations made for access to existing information or documents in the enforcement of the criminal law

AGENCY	AUTHORISATIONS	
	07/08	08/09
AUSTRALIAN COMPETITION & CONSUMER COMMISSION	2	7
ACC	5,639	9,038
ACLEI	5	28
AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE	2,022	9,040
AFP	12,996	16,942
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	1,076	2,319
AUSTRALIAN TAXATION OFFICE	17	644
CCC WA	265	394
CMC	5,716	9,468
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	3	110
DEPARTMENT OF COMMERCE (WA)	217	152
DEPARTMENT OF DEFENCE	13	48
DEPARTMENT OF ENVIRONMENT AND CLIMATE CHANGE NSW	19	60
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFIARS	-	22
DEPARTMENT OF JUVENILE JUSTICE NSW	-	1
DEPARTMENT OF PRIMARY INDUSTRIES VIC	191	421
ICAC	199	260
NSW CC	3,011	4,620
NSW POLICE	88,368	100,585
NT POLICE	979	807
OPI INTEGRITY	1,001	873
PIC	2,048	1,815
QLD POLICE	4,529	9,344
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS QLD	2	-
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS VIC	8	7
SA POLICE	7,852	3,442

AGENCY	AUTHORISATIONS	
	07/08	08/09
TAS POLICE	-	9,627
TRANSPORT ACCIDENT COMMISSION	3	-
VIC POLICE	46,643	40,617
WA POLICE	275	24,606
TOTAL	**183,099**	**245,297**

Table 56—Number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue

AGENCY	AUTHORISATIONS	
	07/08	08/09
AUSTRALIAN BUILDING AND CONSTUCTION COMMISSIONER	13	14
ACT REVENUE OFFICE	7	5
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	29	-
ACLEI	-	4
AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE	1,526	1,096
AFP	481	549
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	-	7
AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION	111	148
AUSTRALIA POST	229	298
AUSTRALIAN TAXATION OFFICE	1,407	645
BRISBANE CITY COUNCIL	-	-
CENTRELINK	2	1,926
CHILD SUPPORT AGENCY	532	192
CONSUMER AFFAIRS AND FAIR TRADING TASMANIA	3	-
CONSUMER AFFAIRS VICTORIA	328	441
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	22	6
DEPARTMENT OF CONSUMER AND EMPLOYMENT PROTECTION WA	10	-
DEPARTMENT OF DEFENCE	44	1
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFAIRS	-	1

DEPARTMENT OF SUSTAINABILITY AND ENVIRONMENT VIC	105	11
HEALTH CARE COMPLAINTS COMMISSION NSW	1	2
ICAC	82	227
NSW DEPARTMENT OF PRIMARY INDUSTRIES	33	81
NT POLICE	14	-
OFFICE OF CONSUMER AND BUSINESS AFFAIRS SA	51	124
OFFICE OF FAIR TRADING – DEPARTMENT OF COMMERCE NSW	439	658
OFFICE OF STATE REVENUE NSW	-	132
OFFICE OF STATE REVENUE QLD	1	53
QLD ENVIRONMENTAL PROTECTION AGENCY	15	50
QLD POLICE	1	-
REVENUE SA	53	36
STATE REVENUE OFFICE VIC	68	103
TAS POLICE	-	189
TAS PRISON SERVICE	-	8
TERRITORY REVENUE OFFICE	1	1
WORKCOVER QLD	41	6
TOTAL	**5,649**	**7,014**

6.6 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 57. The table also outlines the number of days the authorisations were specified in force, and for how many days they were in force. The number of authorisations still in force at the end of the reporting period is also given.

Table 57—Prospective authorisations

AGENCY	NUMBER OF AUTHORISATIONS MADE		DAYS SPECIFIED IN FORCE		ACTUAL DAYS IN FORCE		AUTHORISATIONS DISCOUNTED	
	07/08	08/09	07/08	08/09	07/08	08/09	07/08	08/09
AFP	68	103	2,164	3,152	927	2,879	8	12
ACC	37	42	1,481	1,459	1,019	1,031	2	2
CCC WA	-	49	-	1,609	-	1,098	-	16
CMC	11	129	44	1,554	44	1,466	-	9
NSW CC	330	720	6,590	16,612	4,959	12,539	29	61
NSW POLICE	196	237	5,452	5,027	3,220	3,908	11	10
NT POLICE	81	356	3,577	16,020	2,955	14,507	26	-
OPI	54	75	2,147	4,299	1,824	3,146	1	8
PIC	79	106	2,994	3,466	1,966	4,143	20	3
QLD POLICE	61	192	1,326	3,109	867	2,164	10	15
SA POLICE	45	53	1,290	1,560	723	1,078	1	4
TAS POLICE	26	65	985	2,771	455	1,660	-	1
VIC POLICE	214	211	4,896	7,614	2,500	4,887	11	11
WA POLICE	113	233	4,747	8,808	1778	4,463	4	18
TOTAL	**1,315**	**2,571**	**37,693**	**77,060**	**23,237**	**58,969**	**123**	**170**

6.7 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 58.

Table 58—Average specified and actual time in force

AGENCY	AVERAGE PERIOD SPECIFIED		AVERAGE PERIOD ACTUAL	
	07/08	08/09	07/08	08/09
AFP	32	31	15	32
ACC	40	35	29	26
CCC WA	-	33	-	32
CMC	4	12	4	12
NSW CC	20	23	16	19
NSW POLICE	28	21	17	17
NT POLICE	44	45	54	41
OPI	40	57	34	47
PIC	38	33	33	40
QLD POLICE	22	16	17	12
SA POLICE	29	29	16	22
TAS POLICE	38	43	18	26
VIC POLICE	23	36	12	24
WA POLICE	42	38	16	21
TOTAL	**29**	**30**	**19**	**23**