Telecommunications (Interception and Access) Act 1979

Report for the year ending 30 June 2012

ISBN 978-1-922032-22-5

Contact us
Enquiries regarding the licence and any use of this document are welcome at:

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

Telephone: 02 6141 6666

copyright@ag.gov.au

CONTENTS

LIST OF TABLES

ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
ASIC	Australian Securities and Investments Commission
Blunn Report	Report of the *Review of the Regulation of Access to Communications*
CAC	Communications Access Co-ordinator
CCC WA	Corruption and Crime Commission (Western Australia)
CMC QLD	Crime and Misconduct Commission (Queensland)
ICAC	Independent Commission Against Corruption (New South Wales)
NSW CC	New South Wales Crime Commission
NSW Police	New South Wales Police Force
NT Police	Northern Territory Police
OPI	Office of Police Integrity (Victoria)
PIC	Police Integrity Commission (New South Wales)
QLD Police	Queensland Police Service
SA Police	South Australia Police
TAS Police	Tasmania Police
VIC Police	Victoria Police
WA Police	Western Australia Police
2008 Amendment Act	*Telecommunications Interception Legislation Amendment Act 2008*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
Telecommunications Act	*Telecommunications Act 1997*

CHAPTER 1—INTRODUCTION

1.1 This is the twenty-fourth Annual Report on the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This report relates to the period from 1 July 2011 to 30 June 2012.

1.2 In this report:

- Chapter 2 outlines of the objectives and structure of the TIA Act
- Chapter 3 outlines legislative amendments, policy developments and significant cases decided during the reporting year
- Chapter 4 provides information about the use of interception powers
- Chapter 5 provides information about the use of powers enabling access to stored communications, and
- Chapter 6 provides information about the of use powers enabling access to telecommunications data.

CHAPTER 2—OVERVIEW OF THE ACT

2.1 This chapter provides an overview of the TIA Act, including:

- an outline of its objectives
- a description of the provisions that are most relevant to the contents of this report, and
- an outline of the accountability provisions.

Objectives of the legislation

2.2 The objectives of the TIA Act are to:

- protect the privacy of individuals who use the Australian telecommunications system, and
- specify the circumstances in which it is lawful to intercept and access communications, and to authorise the disclosure of telecommunications data.

2.3 The TIA Act achieves these objectives by:

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

Key privacy protections

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

2.5 The term 'interception' is defined in section 6 to mean listening to or recording, by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication.

2.6 Section 108 of the TIA Act prohibits access to stored communications.

2.7 The term 'stored communication' is defined in section 5 to mean communications which:

(a) have passed over the telecommunications system, and

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

2.8 Voice mail, e-mail and SMS messages are examples of stored communications. Section 6AA provides that 'accessing' a stored communication means listening to, reading or recording it, by means of equipment operated by a carrier, without the knowledge of its intended recipient.

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

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

Telecommunications interception warrants

Offences for which telecommunications interception warrants may be obtained

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

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

- murder, kidnapping and equivalent offences
- serious drug offences
- terrorism offences
- offences punishable by at least 7 years imprisonment that involve conduct such as:
    - risk of loss of a person life, serious personal injury, serious property damage endangering personal safety
    - serious arson
    - bribery or corruption, and
    - tax evasion, fraud, loss of revenue to the Commonwealth.
- offences relating to people smuggling, slavery, sexual servitude, deceptive recruiting and trafficking in persons
- sexual offences against children and offences involving child pornography
- money laundering offences, cybercrime offences, serious cartel offences
- offences involving organised crime, and

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

Applying for telecommunications interception warrants

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

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

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

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

AGENCY	DATE OF SECTION 34 DECLARATION
Victoria Police	28 October 1988
New South Wales Crime Commission	30 January 1989
New South Wales Police Force	30 January 1989
Independent Commission Against Corruption	6 June 1990
South Australia Police	10 July 1991
Western Australia Police	15 July 1997
Police Integrity Commission	14 July 1998
Corruption and Crime Commission (Western Australia)	24 March 2004
Tasmania Police	5 February 2005
Northern Territory Police	25 October 2006
Office of Police Integrity Victoria	18 December 2006
Queensland Police Service	8 July 2009
Crime and Misconduct Commission (Queensland)	8 July 2009

Eligible Judges and nominated AAT members

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

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

- the Federal Court of Australia

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

2.18 A 'nominated AAT member' refers to a Deputy President, senior member or member of the AAT who has been nominated by the Attorney-General to issue warrants.

2.19 Part-time senior members and members of the AAT must have been enrolled as a legal practitioner of the High Court, another federal court or the Supreme Court of a State or Territory for no less than five years to be eligible for nomination.

Form of applications

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

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

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

Matters to be considered by an issuing authority

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

- how much the privacy of any person or persons would be likely to be interfered with
- the gravity of the offence under investigation
- how much the information likely to be obtained would assist the investigation
- the availability of alternative methods of investigation
- how much the use of alternative methods would assist the investigation, and
- how much the use of alternative 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 TIA Act.

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 requires the Secretary of the Attorney-General's Department to maintain a General Register which includes particulars of all telecommunications interception warrants.

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.

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

Special Register of telecommunications interception warrants

2.31 Section 81C of the TIA Act provides that the Secretary of the Attorney-General's Department must maintain a Special Register recording the details of telecommunications interception warrants which did not lead to a prosecution within three months of the expiry of the warrant. The Special Register is delivered to the Attorney-General for inspection together with the General Register.

Destruction of records

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

Independent oversight

2.33 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.

2.34 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.

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

2.36 While the Commonwealth Ombudsman is responsible for inspecting the records of the ACC, ACLEI and the AFP, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies.[1] The reports of the inspections of the declared State and Territory agencies are given to the responsible State or Territory Minister who must provide a copy to the Commonwealth Attorney-General.

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

Annual Report tabled by Attorney-General

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

Stored communications warrants

Offences for which stored communications warrants may be obtained

2.39 Part 3-3 of the TIA Act enables an issuing authority to issue a stored communications warrant to an enforcement agency. The definition of enforcement agency includes listed criminal law enforcement agencies as well as agencies responsible for administering a law imposing a pecuniary penalty or relating to the protection of the public revenue.

Applying for a stored communications warrant

2.40 A stored communications warrant authorises covert access to stored communications in connection with the investigation of a serious contravention. A 'serious contravention' is defined by the TIA Act as:

---

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

- a serious offence (being an offence for which a telecommunications interception warrant may be obtained)
- an offence punishable by a maximum period of imprisonment of at least three years imprisonment, or
- an offence with an equivalent monetary penalty.

Issuing authorities

2.41 Part 3-3 of the TIA Act provides that an enforcement agency may apply to an issuing authority for a stored communications warrant to access stored communications. Section 6DB of the TIA Act provides that the Attorney-General may appoint issuing authorities to issue stored communications warrants.

2.42 Paragraph 6DB(1)(a) defines an issuing authority as:

- a Judge of a court created by the Parliament, a Federal Magistrate or a State magistrate
- who has consented in writing to being appointed by the Attorney-General, and
- who has been so appointed by the Attorney-General.

2.43 In the reporting period, issuing authorities included members of the:

- Federal Court of Australia
- Family Court of Australia
- Federal Magistrates Court, and
- State magistrates.

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

2.45 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

2.46 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.

2.47 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.

2.48 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

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

- how much the privacy of any person or persons would be likely to be interfered with
- the gravity of the conduct constituting the serious contravention
- how much the 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

2.50 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

2.51 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

2.52 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

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

Annual report tabled by Attorney-General

2.54 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

2.55 Part 4-1 of the TIA Act enables enforcement agencies to authorise the disclosure of telecommunications data in certain circumstances. Telecommunications data is not defined in the TIA Act. It is also referred to as 'metadata', 'communications data' and 'communications associated data', and is generally understood as comprising information that allows a communication to occur, and information about the parties to the communication.

2.56 Examples of information that allows a communication to occur, include the internet identifier or service identifier (for example, an e-mail address, phone number or VoIP number), the time and date of the communication, general location information (such as cell tower data), and information about the duration of the communication.

2.57 Examples of information about the parties to the communication include the names and addresses (home, postal, billing if different) of the parties, as well as other contact details such as telephone numbers and e-mail addresses to the extent they are known.

2.58 Telecommunications data does not include the content or substance of a communication. Section 172 specifically prohibits the disclosure of the content or substance of a communication under part 4.1.

Historical data

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

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

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

Prospective data

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

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

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

2.64 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

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

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

Forms of application

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

- the identity of the agency
- the basis on which the agency is an enforcement agency or criminal law-enforcement agency
- the identity of the authorised officer who is making the authorisation
- the basis on which the authorised officer is an authorised officer
- the relevant provisions of the TIA Act
- the name of the person from whom the disclosure is sought
- details of the information or documents to be disclosed
- a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or the protection of the public revenue
- authorisations for prospective access must also include:
    - a statement that the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years

- a statement that the officer had regard to the impact on privacy
- a statement that any impact on privacy was outweighed by the seriousness of the conduct being investigated, and
- the date on which the authorisation is due to end.

Safeguards and controls relating to the telecommunications data regime

Recordkeeping and inspections

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

Annual report tabled by Attorney-General

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

CHAPTER 3—DEVELOPMENTS IN THE REPORTING PERIOD

3.1 This chapter sets out the principal legislative developments and judicial decisions affecting the TIA Act during the reporting period.

Recent legislative and policy developments

Review by Parliamentary Joint Committee on Intelligence and Security

3.2 On 4 May 2012, the Attorney-General, the Hon Nicola Roxon MP, announced that the Government had asked the Parliamentary Joint Committee on Intelligence and Security to review and consider potential reforms to security-related legislation including the TIA Act to ensure Australia's national security capability can evolve to meet emerging threats, while also delivering the right checks and balances for a civil society.

3.3 The Committee's review was in progress at the end of the reporting year.

Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012

3.4 Extradition and mutual assistance are key international crime cooperation tools. Mutual assistance is the formal Government to Government process countries use to assist one another in the investigation and prosecution of criminal offences. The reforms in the *Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012* (the Act) focus on Government to Government assistance and, with some very minor exceptions, do not affect forms of agency to agency assistance.

3.5 The Act amends the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979* to allow information lawfully obtained for domestic purposes under an interception or stored communications warrant to be provided directly to a foreign country, following a mutual assistance request from that foreign country and Attorney-General approval. Prior to the commencement of these amendments, this information could only be provided to a foreign country by producing the material before a magistrate.

3.6 The Act received the Royal Assent on 20 March 2012 and will commence on 20 September 2012.

Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012

3.7 The *Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012* (the Act) amended the TIA Act to add three new State agencies as eligible authorities, namely the Victorian Independent Broad-based Anti-corruption Commission, the Victorian Inspectorate and the South Australian Independent Commissioner Against Corruption. The inclusion of these agencies as eligible authorities will allow the Attorney-General to declare them to be interception agencies once the conditions in section 35 of the TIA Act have been met.

3.8 The Act also amended the TIA Act to introduce the Victorian Public Interest Monitor (PIM) into the interception regime. Under the *Public Interest Monitor Act 2011* of Victoria, the PIM has oversight functions in relation to several Acts, including the *Telecommunications (Interception) (State Provisions) Act 1998* of Victoria.

3.9 The amendments to the TIA Act allow the PIM to make submissions to the issuing authority considering an application for an interception warrant from a Victorian interception agency and to ask questions of an officer representing the agency applying for the warrant or any other party required to give further information on the application. These provisions will only operate where the applicant is representing a declared Victorian agency.

3.10 The Act received the Royal Assent on 27 June 2012. Commencement will occur at the same time as commencement of the State legislation establishing the new agencies.

Cybercrime Legislation Amendment Act 2012

3.11 Cybercrime is a growing threat to Australian consumers, businesses and government. The international nature of cybercrime is such that no nation alone can effectively combat the problem. It is essential that Australia has in place appropriate arrangements, both domestically and internationally, to be in the best possible position to combat cybercrime.

3.12 The Council of Europe Convention on Cybercrime (the Convention) is the first international treaty on crimes committed either against or via computer networks, dealing particularly with online fraud, offences related to child pornography and unauthorised access, use or modification of data stored on computers. The Convention's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Convention also contains a series of powers and procedures relating to accessing important evidence of cybercrimes, including by way of mutual assistance.

3.13 The Cybercrime Legislation Amendment Act 2012 makes a number of amendments necessary to facilitate Australia's accession to the Convention. The Bill amends the TIA Act, the *Criminal Code Act 1995*, the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications Act 1997* to ensure that Australian legislation meets all the Convention's requirements, subject to certain reservations. Specifically, the Act:

- requires carriers and carriage service providers (C/CSPs) to preserve the stored communications and telecommunications data for specific persons when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign countries

- ensures Australian agencies are able to obtain and disclose telecommunications data and stored communications for the purposes of a foreign investigation

- provides for the extraterritorial operation of certain offences in the TIA Act

- amends the computer crime offences in the Criminal Code Act 1995 so that they have adequate scope, and

- creates confidentiality requirements in relation to authorisations to disclose telecommunications data.

3.14 The Cybercrime Legislation Amendment Bill 2011 first passed the House of Representatives on 24 August 2011. It passed the Senate on 22 August 2012, and received the Royal Assent on 12 September 2012. This allows the Federal Executive Council to approve Australia's accession to the Convention.

Recent case law

3.15 In the case of *R v Kashani-Malaki* [2011] QSC 308 (5 October 2011), the Supreme Court of Queensland considered an application for exclusion of evidence obtained by telephone interception, under otherwise valid warrants, on the basis that section 60(1) of the TIA Act had not been complied with. The accused argued that section 60(1) of the TIA Act requires that the managing director of a carrier be notified personally of the issue of a warrant authorising the interception of communications passing over the carriers networks. In this case, the notification had been received by a carrier employee on behalf of the managing director. The court rejected this argument, finding that personal notification of the managing director is not required. The intercepted information was therefore admitted into evidence.

3.16 Amendments to the TIA Act made before the reporting year by the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* now expressly allow for a carrier's managing director to delegate the function of receiving warrant documentation to an 'authorised representative'.

Previous Annual Report

3.17 The Annual Report for the year ending 30 June 2011 was tabled in both Houses of Parliament on 1 November 2011. Corrigenda were tabled in the Senate on 7 November 2011 and in the House of Representatives on 21 November 2011.

3.18 Copies of previous Annual Reports can be found on the Attorney-General's Department website: www.ag.gov.au.

CHAPTER 4—TELECOMMUNICATIONS INTERCEPTION INFORMATION REQUIRED UNDER THE ACT

The information required

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

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

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

Which agencies may seek telecommunications interception warrants

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

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

Applications for telecommunications interception warrants

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

4.5 During the reporting period 3,755 warrants were issued to law enforcement agencies under Part 2-5 of the TIA Act. The total number of warrants issued increased by approximately 7.7% on the total number of warrants issued during the previous reporting period. Fluctuations in the number of warrants issued over the past three reporting periods are consistent with operational practices. This information is presented in Table 1.

Table 1 – Applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
ACC	Made Refused/withdrawn Issued	210 - 210	190 - 190	143 - 143
ACLEI	Made Refused/withdrawn Issued	1 - 1	4 - 4	9 - 9
AFP	Made Refused/withdrawn Issued	642 1 641	523 - 523	541 1 540
CCC WA	Made Refused/withdrawn Issued	40 - 40	35 - 35	34 2 32
CMC QLD	Made Refused/withdrawn Issued	18 - 18	25 - 25	41 - 41
ICAC	Made Refused/withdrawn Issued	14 - 14	12 - 12	24 - 24
NSW CC	Made Refused/withdrawn Issued	368 1 367	410 3 407	348 2 346
NSW POLICE	Made Refused/withdrawn Issued	1,142 1 1,141	1,282 3 1,279	1,574 4 1,570
NT POLICE	Made Refused/withdrawn Issued	50 - 50	46 - 46	54 - 54
OPI	Made Refused/withdrawn Issued	36 - 36	45 - 45	12 - 12
PIC	Made Refused/withdrawn Issued	48 - 48	63 - 63	62 - 62
QLD POLICE	Made Refused/withdrawn Issued	173 1 172	177 - 177	218 - 218
SA POLICE	Made Refused/withdrawn Issued	113 - 113	107 - 107	102 - 102
TAS POLICE	Made Refused/withdrawn Issued	21 1 20	27 - 27	33 - 33
VIC POLICE	Made Refused/withdrawn Issued	388 - 388	317 - 317	293 - 293
WA POLICE	Made Refused/withdrawn Issued	325 - 325	232 1 231	276 - 276
TOTAL [paragraph 100(2)(a)]	**Made** **Refused/withdrawn** **Issued**	**3,589** **5** **3,584**	**3,495** **7** **3,488**	**3,764** **9** **3,755**

Telephone applications for telecommunications interception warrants

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

4.7 The total number of telephone applications made in the reporting period has increased by approximately 52.1% from the previous reporting period.

Table 2—Telephone applications for telecommunications interception warrants

AGENCY	RELEVANT STATISTICS	TELEPHONE APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
AFP	Made Refused/withdrawn Issued	5 - 5	- - -	1 - 1
NSW POLICE	Made Refused/withdrawn Issued	38 - 38	50 - 50	86 - 86
TAS POLICE	Made Refused/withdrawn Issued	- - -	- - -	3 - 3
VIC POLICE	Made Refused/withdrawn Issued	23 - 23	21 - 21	16 - 16
WA POLICE	Made Refused/withdrawn Issued	1 - 1	2 - 2	5 - 5
TOTAL [paragraph 100(2)(b)]	**Made** **Refused/withdrawn** **Issued**	**67** **-** **67**	**73** **-** **73**	**111** **-** **111**

Renewal applications for telecommunications interception warrants

4.8 Agencies may apply for a new warrant in respect of a service or person while an existing warrant is still in force – this is known as a renewal warrant. Paragraphs 100(1)(c) and (2)(c) of the TIA Act provide that the report must set out the number of renewal applications made in relation to each agency and in total for all agencies. This information is presented in Table 3.

4.9 The number of renewal applications decreased by approximately 25.4% 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		
		09/10	10/11	11/12
ACC	Made	50	44	34
	Refused/withdrawn	-	-	-
	Issued	50	44	34
ACLEI	Made	-	-	5
	Refused/withdrawn	-	-	-
	Issued	-	-	5
AFP	Made	220	173	135
	Refused/withdrawn	-	-	-
	Issued	220	173	135
CCC WA	Made	7	6	5
	Refused/withdrawn	-	-	-
	Issued	7	6	5
CMC QLD	Made	3	1	8
	Refused/withdrawn	-	-	-
	Issued	3	1	8
ICAC	Made	3	1	2
	Refused/withdrawn	-	-	-
	Issued	3	1	2
NSW CC	Made	42	85	75
	Refused/withdrawn	-	-	-
	Issued	42	85	75
NSW POLICE	Made	169	242	155
	Refused/withdrawn	-	-	-
	Issued	169	242	155
NT POLICE	Made	5	1	2
	Refused/withdrawn	-	-	-
	Issued	5	1	2
OPI	Made	11	4	5
	Refused/withdrawn	-	-	-
	Issued	11	4	5
PIC	Made	25	19	14
	Refused/withdrawn	-	-	-
	Issued	25	19	14
QLD POLICE	Made	14	16	21
	Refused/withdrawn	-	-	-
	Issued	14	16	21
SA POLICE	Made	1	3	10
	Refused/withdrawn	-	-	-
	Issued	1	3	10
TAS POLICE	Made	5	7	1
	Refused/withdrawn	-	-	-
	Issued	5	7	1
VIC POLICE	Made	56	49	26
	Refused/withdrawn	-	-	-
	Issued	56	49	26
WA POLICE	Made	45	37	15
	Refused/withdrawn	-	-	-
	Issued	45	37	15
TOTAL [paragraph 100(2)(c)]	**Made**	**656**	**688**	**513**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**656**	**688**	**513**

Applications for telecommunications interception warrants authorising entry onto premises

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

4.11 Agencies continue to seek this type of warrant on rare occasions only. Also the number of agencies seeking this type of warrant is not large which is also consistent with previous reporting periods.

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

AGENCY	RELEVANT STATISTICS	WARRANTS AUTHORISING ENTRY ON PREMISES		
		09/10	10/11	11/12
AFP	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
CCC WA	Made	2	-	1
	Refused/withdrawn	-	-	-
	Issued	2	-	1
NSW CC	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
NSW POLICE	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
PIC	Made	1	2	-
	Refused/withdrawn	-	-	-
	Issued	1	2	-
TOTAL [paragraph 100(2)(d)]	**Made**	**4**	**2**	**3**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**4**	**2**	**3**

Telecommunications interception warrants issued with specific conditions or restrictions

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

4.13 There has been a significant increase in the number of warrants sought by agencies under subsection 49(1) of the TIA Act from previous reporting periods, increasing in this period by 35 warrants. This is generally attributed to a larger number of agencies seeking this type of warrant due to specific operational needed.

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

AGENCY	WARRANTS ISSUED WITH CONDITIONS OR RESTRICTIONS		
	09/10	10/11	11/12
ACC	-	3	-
ACLEI	-	2[2]	9
AFP	2	2	3
CMC QLD	-	-	5
ICAC	-	-	1
NSW CC	-	-	3
NSW POLICE	4	6	19
PIC	1	1	5
QLD POLICE	-	-	2
TOTAL [paragraph 100(2)(e)]	**7**	**14**	**47**

Named person warrants

4.14 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.

4.15 Paragraph 100(2)(ea) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 6 to 9 set out the information supplied by intercepting agencies regarding named person warrants. The number of named person warrants issued to agencies increased by approximately 11.4% from the number of warrants issued in the previous reporting period. The number of renewal applications for named person warrants decreased by approximately 8% from the previous reporting period. No named person warrants authorised entry onto premises during the reporting period.

Interpretative note relating to named person warrants

4.16 The increase in named person warrants is consistent with operational fluctuations. This demonstrates the high impact on privacy that named person warrants have, and that

[2] ACLEI advised that the information supplied for the 10/11 period was inaccurate, this report reflects the accurate figure.

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 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		
		09/10	10/11	11/12
ACC	Made	103	115	100
	Refused/withdrawn	-	-	-
	Issued	103	115	100
ACLEI	Made	-	-	3
	Refused/withdrawn	-	-	-
	Issued	-	-	3
AFP	Made	155	191	209
	Refused/withdrawn	-	-	1
	Issued	155	191	208
CCC WA	Made	3	1	-
	Refused/withdrawn	-	-	-
	Issued	3	1	-
CMC QLD	Made	8	6	8
	Refused/withdrawn	-	-	-
	Issued	8	6	8
ICAC	Made	2	-	-
	Refused/withdrawn	-	-	-
	Issued	2	-	-
NSW CC	Made	48	75	100
	Refused/withdrawn	-	1	-
	Issued	48	74	100
NSW POLICE	Made	25	41	97
	Refused/withdrawn	-	-	-
	Issued	25	41	97
NT POLICE	Made	10	5	1
	Refused/withdrawn	-	-	-
	Issued	10	5	1
OPI	Made	-	8	3
	Refused/withdrawn	-	-	-
	Issued	-	8	3
PIC	Made	2	2	2
	Refused/withdrawn	-	-	-
	Issued	2	2	2
QLD POLICE	Made	26	29	30
	Refused/withdrawn	-	-	-
	Issued	26	29	30
SA POLICE	Made	27	21	22
	Refused/withdrawn	-	-	-
	Issued	27	21	22
TAS POLICE	Made	1	-	2
	Refused/withdrawn	-	-	-
	Issued	1	-	2
VIC POLICE	Made	87	81	71
	Refused/withdrawn	-	-	-
	Issued	87	81	71
WA POLICE	Made	53	54	54
	Refused/withdrawn	-	-	-
	Issued	53	54	54
TOTAL [paragraph 100(ea)]	**Made**	**550**	**629**	**702**
	Refused/withdrawn	**-**	**1**	**1**
	Issued	**550**	**628**	**701**

Table 7—Telephone applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
NSW POLICE	Made	-	-	3
	Refused/withdrawn	-	-	-
	Issued	-	-	3
VIC POLICE	Made	2	1	-
	Refused/withdrawn	-	-	-
	Issued	2	1	-
WA POLICE	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
TOTAL [paragraph 100(ed)]	**Made**	**2**	**1**	**4**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**2**	**1**	**4**

Table 8—Renewal applications for named person warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
ACC	Made	36	35	28
	Refused/withdrawn	-	-	-
	Issued	36	35	28
ACLEI	Made	-	-	2
	Refused/withdrawn	-	-	-
	Issued	-	-	2
AFP	Made	62	79	61
	Refused/withdrawn	-	-	-
	Issued	62	79	61
CCC WA	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
CMC QLD	Made	2	1	1
	Refused/withdrawn	-	-	-
	Issued	2	1	1
ICAC	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
NSW CC	Made	8	11	28
	Refused/withdrawn	-	-	-
	Issued	8	11	28
NSW POLICE	Made	4	10	18
	Refused/withdrawn	-	-	-
	Issued	4	10	18
NT POLICE	Made	2	1	-
	Refused/withdrawn	-	-	-
	Issued	2	1	-
OPI	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
PIC	Made	-	1	1
	Refused/withdrawn	-	-	-
	Issued	-	1	1
QLD POLICE	Made	5	5	4
	Refused/withdrawn	-	-	-
	Issued	5	5	4
SA POLICE	Made	1	-	1
	Refused/withdrawn	-	-	-
	Issued	1	-	1

VIC POLICE	Made Refused/withdrawn Issued	17 - 17	22 - 22	12 - 12
WA POLICE	Made Refused/withdrawn Issued	12 - 12	9 - 9	4 - 4
TOTAL [paragraph 100(ed)]	**Made** **Refused/withdrawn** **Issued**	**152** **-** **152**	**174** **-** **174**	**160** **-** **160**

Table 9—Named person warrants issued with conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS WITH CONDITIONS		
		09/10	10/11	11/12
ACC	Issued	-	3	-
ACLEI	Issued	-	-	3
AFP	Issued	-	-	2
CMC QLD	Issued	-	-	4
NSW CC	Issued	-	2	-
NSW POLICE	Issued	-	-	1
QLD POLICE	Issued	-	-	1
TOTAL [paragraph 100(2)(ea)]	**Issued**	**-**	**5**	**11**

4.17 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.

4.18 This information is included in Table 10.

Table 10—Number of services intercepted under named person warrants

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		09/10	10/11	11/12
ACC	1 service only 2 – 5 services 6 – 10 services 10+ services	19 76 7 1	29 66 15 1	32 50 12 1
ACLEI	1 service only 2 – 5 services 6 – 10 services 10+ services	- - - -	- - - -	1 2 - -

AGENCY	RELEVANT STATISTICS	NUMBER OF SERVICES		
		09/10	10/11	11/12
AFP	1 service only	31	22	30
	2 – 5 services	96	126	114
	6 – 10 services	13	17	24
	10+ services	1	4	8
CCC WA	1 service only	1	-	-
	2 – 5 services	2	-	-
	6 – 10 services	-	-	-
	10+ services	-	1	-
CMC QLD	1 service only	3	2	4
	2 – 5 services	5	4	3
	6 – 10 services	1	-	1
	10+ services	-	-	-
ICAC	1 service only	-	-	-
	2 – 5 services	2	-	-
	6 – 10 services	-	-	-
	10+ services	-	-	-
NSW CC	1 service only	9	14	39
	2 – 5 services	27	52	57
	6 – 10 services	12	6	8
	10+ services	-	1	1
NSW POLICE	1 service only	3	8	28
	2 – 5 services	18	25	58
	6 – 10 services	2	5	10
	10+ services	-	-	1
NT POLICE	1 service only	1	2	-
	2 – 5 services	9	3	1
	6 – 10 services	-	-	-
	10+ services	-	-	-
OPI	1 service only	-	1	-
	2 – 5 services	2	5	2
	6 – 10 services	-	2	1
	10+ services	-	0	-
PIC	1 service only	-	-	-
	2 – 5 services	2	-	2
	6 – 10 services	2	2	-
	10+ services	-	-	-
QLD POLICE	1 service only	3	5	3
	2 – 5 services	23	22	26
	6 – 10 services	-	1	1
	10+ services	-	-	-
SA POLICE	1 service only	5	7	4
	2 – 5 services	19	13	16
	6 – 10 services	2	1	2
	10+ services	-	-	-
TAS POLICE	1 service only	-	-	-
	2 – 5 services	1	-	2
	6 – 10 services	-	-	-
	10+ services	-	-	-
VIC POLICE	1 service only	9	12	12
	2 – 5 services	67	56	52
	6 – 10 services	9	12	7
	10+ services	2	2	-
WA POLICE	1 service only	11	8	14
	2 – 5 services	34	44	39
	6 – 10 services	7	2	1
	10+ services	1	-	-
TOTAL [paragraph 100(2)(eb)]	**1 service only**	**95**	**110**	**167**
	2 – 5 services	**383**	**416**	**424**
	6 – 10 services	**55**	**63**	**67**
	10+ services	**5**	**9**	**11**

4.19 Paragraphs 100(1)(ec) and 100(2)(ec) of the TIA Act provide that the report must include, for each agency and in total, the total number of services intercepted under service based named person warrants and the number of devices intercepted under a device based named person warrant. This information is presented in Tables 11 and 12.

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

AGENCY	TOTAL NUMBER OF SERVICES INTERCEPTED		
	09/10	10/11	11/12
ACC	311	337	251
ACLEI	-	-	6
AFP	459	586	759
CCC WA	6	11	0
CMC QLD	22	12	23
ICAC	4	-	0
NSW CC	181	212	280
NSW POLICE	75	125	278
NT POLICE	28	12	3
OPI	2	8	12
PIC	6	14	6
QLD POLICE	68	68	83
SA POLICE	78	53	62
TAS POLICE	5	-	9
VIC POLICE	296	293	207
WA POLICE	175	169	136
TOTAL	**1,716**	**1,900**	**2,115**

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

AGENCY	SERVICES			DEVICES		
	09/10	10/11	11/12	09/10	10/11	11/12
ACC	-	-	-	-	9	24
AFP	-	-	-	12	21	31
NSW POLICE	2	2	16	7	4	11
QLD POLICE	-	-	-	2	-	-
NSW CC	1	-	-	5	-	10
NSW POLICE	-	-	16	-	-	11
SA POLICE	-	-	9	-	-	2
TOTAL	**3**	**2**	**41**	**26**	**34**	**89**

B-Party warrants

4.20 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.

4.21 Paragraph 100(2)(ed) of the TIA Act provides that the report must also include these statistics in total across all agencies. Tables 13 to 16 set out the information supplied by intercepting agencies regarding B-Party warrants. There has been a 34.2% increase of applications for B-Party warrants since the last reporting period. This increase can be attributed to the operational needs of agencies.

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

Table 13—Applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		09/10	10/11	11/12
ACC	Made	-	2	1
	Refused/withdrawn	-	-	-
	Issued	-	2	1
ACLEI	Made	-	-	1
	Refused/withdrawn	-	-	-
	Issued	-	-	1
AFP	Made	43	42	47
	Refused/withdrawn	-	-	-
	Issued	43	42	47
CCC WA	Made	1	4	-
	Refused/withdrawn	-	-	-
	Issued	1	4	-
NSW CC	Made	4	10	19
	Refused/withdrawn	-	-	-
	Issued	4	10	19
NSW POLICE	Made	38	44	66
	Refused/withdrawn	-	-	-
	Issued	38	44	66
OPI	Made	-	3	1
	Refused/withdrawn	-	-	-
	Issued	-	3	1
QLD POLICE	Made	1	1	-
	Refused/withdrawn	-	-	-
	Issued	1	1	-
SA POLICE	Made	-	-	-
	Refused/withdrawn	-	-	-
	Issued	-	-	-
VIC POLICE	Made	32	5	14
	Refused/withdrawn	-	-	-
	Issued	32	5	14
WA POLICE	Made	1	-	-
	Refused/withdrawn	-	-	-
	Issued	1	-	-
TOTAL [paragraph 100(2)(ed)]	**Made**	**120**	**111**	**149**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**120**	**111**	**149**

Table 14—Telephone applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		09/10	10/11	11/12
AFP	Made Refused/withdrawn Issued	3 - 3	**-** **-** **-**	1 - 1
NSW POLICE	Made Refused/withdrawn Issued	8 - 8	9 - 9	13 - 13
VIC POLICE	Made Refused/withdrawn Issued	- - -	1 - 1	- - -
TOTAL [paragraph 100(2)(ed)]	**Made** **Refused/withdrawn** **Issued**	**11** **-** **11**	**10** **-** **10**	**14** **-** **14**

Table 15—Renewal applications for B-Party warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		09/10	10/11	11/12
AFP	Made Refused/withdrawn Issued	26 - 26	24 - 24	26 - 26
NSW CC	Made Refused/withdrawn Issued	- - -	- - -	4 - 4
NSW POLICE	Made Refused/withdrawn Issued	4 - 4	5 - 5	2 - 2
VIC POLICE	Made Refused/withdrawn Issued	15 - 15	- - -	- - -
TOTAL [paragraph 100(2)(ed)]	**Made** **Refused/withdrawn** **Issued**	**45** **-** **45**	**29** **-** **29**	**32** **-** **32**

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

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		
		09/10	10/11	11/12
ACLEI	Issued	-	-	1
NSW POLICE	Issued	-	-	2
TOTAL [paragraph 100(2)(ed)]	**Issued**	**-**	**-**	**3**

Interpretative note relating to B-Party warrants

4.23 These statistics demonstrate that B-Party warrants continue to be used sparingly. Of the sixteen agencies that were issued telecommunications interception warrants during the reporting period, only eleven applied for and were issued B-Party warrants representing no change for the previous reporting period. B-Party warrants represented approximately 4% of the total number of warrants issued, which is only a slight increase from 3% for the previous reporting period.

4.24 Agencies sought 32 renewals of B-Party warrants, representing a slight increase from the previous reporting period. This illustrates that agencies are continuing to 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

4.25 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.

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

4.27 Care should be taken in interpreting the following table as warrants may have been issued in the investigation of more than one serious offence. The data for each serious offence includes figures for any related ancillary offences, such as assisting in the commission of, or conspiring to commit, a principal offence.

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
ACC special investigations	210	171	137
Serious drug offences	-	19	12

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the Criminal Code Act 1995	1	4	9

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		
	09/10	10/11	11/12
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	1	-
Bribery or corruption	1	-	7
Child pornography	3	-	3
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	1
Cybercrime	3	12	6
Kidnapping	-	-	1
Money laundering	136	137	93
Murder	16	2	1
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the Criminal Code Act 1995	2	3	8
Offences involving planning and organisation	13	23	6
People smuggling or sexual servitude	30	10	27
Serious arson	-	-	3
Serious damage to property	-	-	8
Serious drug offences	391	443	392
Serious fraud or loss of revenue	18	12	16
Serious personal injury or loss of life	73	16	54
Telecommunications offences	17	3	1
Terrorism	141	61	71

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		
	09/10	10/11	11/12
Bribery or corruption	39	28	22
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	4
Cybercrime	4	-	-
Offences involving planning and organisation	-	3	-
Serious drug offences	-	12	-
Serious personal injury or loss of life	-	1	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	7	9	13
Serious drug offences	11	15	21
Serious fraud or loss of revenue	-	-	7
Serious personal injury or loss of life	-	1	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	14	9	24
Cybercrime offences	-	3	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	22	14
Bribery or corruption	-	-	4
Conspiring to commit or aiding or abetting the commission of a serious offence	-	27	23
Kidnapping	-	3	-
Money laundering	61	36	22
Murder	61	65	52
Offences involving planning and organisation	24	5	8
Organised crime offences	-	-	1
Serious arson	-	-	4
Serious damage to property	-	-	2
Serious drug offences	228	257	209
Serious fraud or loss of revenue	10	16	1
Serious personal injury or loss of life	20	-	13

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	6
Bribery or corruption	15	27	7
Child pornography	-	-	4
Conspiring to commit or aiding or abetting the commission of a serious offence	2	8	20
Kidnapping	22	-	27
Money laundering	-	-	15
Murder	293	296	228
Offences involving planning and organisation	152	155	116
Organised crime	-	-	11
People smuggling or sexual servitude	-	1	-
Serious arson	9	23	48
Serious damage to property	20	15	4
Serious drug offences	389	410	472
Serious fraud or loss of revenue	46	24	38
Serious personal injury or loss of life	164	293	565
Terrorism	29	35	9

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	-	-	3
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	1
Murder	7	4	3
Serious arson	-	1	
Serious drug offences	43	37	47
Serious personal injury or loss of life	-	4	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	36	40	9
Conspiring to commit or aiding or abetting the commission of a serious offence	-	2	3
Murder	-	1	-
Serious drug offences	-	2	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	41	56	54
Money laundering	-	-	8
People smuggling or sexual servitude	-	-	3
Serious drug offences	3	7	-
Serious fraud or loss of revenue	-	-	3
Serious personal injury or loss of life	4	-	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	11	-	3
Conspiring to commit or aiding or abetting the commission of a serious offence	-	-	2
Murder	26	31	23
Offences involving planning and organisation	7	-	7
Serious arson	1	-	2
Serious drug offences	115	127	169
Serious fraud or loss of revenue	7	-	3
Serious personal injury or loss of life	9	19	9

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	5	6	1
Child Pornography	6	-	-
Conspiring to commit or aiding or abetting the commission of a serious offence	16	10	1
Cybercrime	-	3	-
Kidnapping	-	1	-
Money Laundering	4	2	17
Murder	17	7	14
Offences involving planning and organisation	-	2	-
Serious drug offences	90	63	57
Serious fraud or loss of revenue	1	-	-
Serious personal injury or loss of life	14	15	18

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Conspiring to commit or aiding or abetting the commission of a serious offence	1	-	-
Murder	17	10	10
Serious arson	-	1	-
Serious drug offences	8	26	21
Serious personal injury or loss of life	-	-	2

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	4	8	13
Child pornography offences	-	1	-
Kidnapping	11	12	13
Money Laundering	1	-	6
Murder	113	49	82
Offences involving planning and organisation	-	1	3
Serious arson	3	3	1
Serious damage to property	-	2	-
Serious drug offences	191	154	102
Serious fraud or loss of revenue	-	4	3
Serious personal injury or loss of life	65	71	71
Terrorism	-	8	-

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

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
Bribery or corruption	-	-	7
Child pornography	-	2	-
Kidnapping	8	-	1
Money laundering	3	-	-
Murder	34	26	49
Offences involving planning and organisation	14	11	16
Serious arson	10	-	5
Serious damage to property	1	-	-
Serious drug offences	209	168	169
Serious fraud or loss of revenue	-	2	-
Serious personal injury or loss of life	46	22	29

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

4.28 Paragraphs 100(2)(f) and (g) of the TIA Act provide that the categories of serious offences specified in telecommunications interception warrants for all agencies must be set out in combined form. This information is set out in Table 33.

4.29 The total number of serious offences fluctuated according to operational needs during the reporting period.

Table 33—Categories of serious offences specified in telecommunications interception warrants in relation to all agencies

CATEGORIES OF SERIOUS OFFENCES	NUMBER OF SERIOUS OFFENCES SPECIFIED IN EACH CATEGORY		
	09/10	10/11	11/12
ACC special investigations[3]	210	171	137
Administration of justice[4]	-	-	-
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	11	23	23
Bribery or corruption	162	183	164
Child pornography	9	3	7
Conspiring to commit or aiding or abetting the commission of a serious offence	19	47	55
Cybercrime	7	18	6
Kidnapping	41	16	42
Money laundering	205	175	161
Murder	584	491	462
Offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the Criminal Code Act 1995	3	7	17
Offences involving planning and organisation	210	200	156
Organised crime offences	-	-	12
People smuggling or sexual servitude	30	11	30
Serious arson	13	28	59
Serious damage to property	21	17	18
Serious drug offences	1,678	1,222	1,671
Serious fraud or loss of revenue	82	58	44
Serious personal injury or loss of life	395	442	760
Telecommunications offences	17	3	1
Terrorism	170	104	80

Duration of telecommunications interception warrants

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

Duration of original telecommunications interception warrants

4.31 Paragraph 101(1)(a) of the TIA Act provides that the report must set out the average period specified in original telecommunications interception warrants in relation to each

[3] Applies only to the ACC.

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

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 34.

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

Table 34—Duration of original telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	09/10	10/11	11/12	09/10	10/11	11/12
ACC	86	84	87	45	83	55
ACLEI	60[5]	90	71	25	33	78
AFP	80	66	79	54	44	50
CCC WA	73	72	86	64	78	53
CMC QLD	53	72	58	48	53	49
ICAC	90	52	83	84	30	41
NSW CC	84	88	80	71	89	87
NSW POLICE	61	48	72	52	39	45
NT POLICE	86	81	78	61	64	42
OPI	55	78	81	47	61	62
PIC	90	65	77	69	53	60
QLD POLICE	40	46	59	31	39	41
SA POLICE	83	72	79	64	54	59
TAS POLICE	84	81	83	68	74	67
VIC POLICE	55	55	56	41	41	41
WA POLICE	86	86	85	48	58	48
AVERAGE [paragraphs 101(2)(a)-(b)]	**73**	**71**	**76**	**52**	**56**	**55**

Duration of renewal telecommunications interception warrants

4.33 Paragraphs 101(1)(c), (1)(d), (2)(c) and (2)(d) of the TIA Act provide that the report set out corresponding information in relation to telecommunications interception warrants that have been renewed. This information is set out in Table 35. While the average period in force is slightly higher, there is no significant variation in the average specified or actual durations of renewal warrants from previous reporting periods.

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

Table 35—Duration of renewal of telecommunications interception warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	09/10	10/11	11/12	09/10	10/11	11/12
ACC	76	78	81	79	76	77
ACLEI	-	-	90	-	-	62
AFP	83	65	79	66	35	72
CCC WA	73	90	54	60[6]	58	38
CMC QLD	65	90	88	61	41	63
ICAC	90	90	90	17	26	-
NSW CC	89[7]	85	86	68	74	85
NSW POLICE	66	61	73	64	49	61
NT POLICE	81	60	75	45	9	26
OPI	-	90	90	-	88	56
PIC	90	86	90	88	75	90
QLD POLICE	42	51	49	32	44	37
SA POLICE	90	57	74	-	18	38
TAS POLICE	90	80	90	90	73	90
VIC POLICE	59	59	60	40	19	60
WA POLICE	74	85	88	53	67	59
AVERAGE [paragraphs 101(2)(a)-(b)]	**75**	**75**	**79**	**63**	**50**	**61**

Interpretative note relating to average duration of warrants across all agencies

4.34 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.

4.35 These figures illustrate that the duration of warrants does not vary to a significant extent from year to year, and that the actual duration of warrants is typically shorter than the specified duration.

Duration of original B-Party warrants

4.36 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.

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

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

4.37 Paragraph 101(1)(da) of the TIA Act provides that the report must set out the average period specified in original B-Party warrants in relation to each agency and the average of the periods for which those warrants were actually in force. Paragraph 101(2)(da) provides that the same information must be averaged across all agencies. This information is set out in Table 36.

Table 36—Duration of original B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	09/10	10/11	11/12	09/10	10/11	11/12
ACC	-	45	45	-	45	45
ACLEI	-	-	45	-	-	-
AFP	45	43	44	33	36	28
CCC WA	45	45	-	38	42	-
NSW CC	45	45	55	32	36	44
NSW POLICE	34	29	32	25	15	19
OPI	-	45	45	-	6	43
QLD POLICE	8	3	-	8	3	-
VIC POLICE	45	41	44	45	43	33
WA POLICE	14	-	-	14	-	-
AVERAGE [paragraph 101(2)(da)]	**34**	**37**	**44**	**28**	**28**	**36**

Duration of renewal B-Party warrants

4.38 Paragraphs 101(1)(da) and (2)(da) of the TIA Act also provide that the report must set out corresponding information in relation to B-Party warrants that have been renewed. This information is set out in Table 37.

Table 37—Duration of renewal of B-Party warrants

AGENCY	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)			AVERAGE PERIOD WARRANTS IN FORCE (DAYS)		
	09/10	10/11	11/12	09/10	10/11	11/12
AFP	46	45	45	47	45	40
NSW CC	-	-	43	-	-	40
NSW POLICE	29	28	40	29	21	35
VIC POLICE	45	-	-	29	-	-
AVERAGE [paragraphs 101(2)(da)]	**40**	**36**	**43**	**35**	**33**	**38**

Number of final renewals of telecommunications interception warrants

4.39 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.

4.40 This information gives some indication of the overall duration of warrants that have been renewed. Paragraph 101(2)(e) of the Act provides that the same information must be set out in total across all agencies. This information is set out in Table 38.

4.41 Table 38 shows a significant rise in 90 day renewals of 41.8% during the current reporting period. It should also be noted that there has been a substantial decrease in 150 day and 180 day renewals, seeing both returned to similar levels as reported in the 2009/10 reporting period.

Table 38—Number of 'final renewals'

AGENCY	90 DAYS			150 DAYS			180 DAYS		
	09/10	10/11	11/12	09/10	10/11	11/12	09/10	10/11	11/12
ACC	6	9	18	4	9	2	6	10	1
ACLEI	-	-	0	-	-	0	-	-	1
AFP	4	7	58	21	10	7	24	30	18
CCC WA	3	-	4	-	6	1	-	3	0
CMC QLD	-	-	3	-	-	1	-	1	0
ICAC	3	1	0	-	-	0	-	-	0
NSW CC	7	9	42	4	26	3	5	23	3
NSW POLICE	74	107	84	4	8	22	5	23	12
NT POLICE	3	1	1	-	1	0	1	-	0
OPI	8	-	1	-	4	0	9	-	2
PIC	-	-	0	-	4	10	-	6	3
QLD POLICE	4	7	14	-	-	0	-	-	1
SA POLICE	-	-	3	-	-	0	-	-	0
TAS POLICE	-	-	0	-	-	0	-	3	1
VIC POLICE	24	20	16	5	1	5	2	-	3
WA POLICE	19	11	0	12	9	6	3	5	7
TOTAL [paragraph 101(2)(e)]	**155**	**172**	**244**	**50**	**78**	**57**	**55**	**104**	**52**

Effectiveness of telecommunications interception warrants

4.42 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.

4.43 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.

4.44 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.

4.45 The communication of that information may result in further investigation and possibly arrests and prosecution by an eligible authority on the basis of lawfully intercepted information. That is notwithstanding that the authority is itself unable to obtain a warrant. An example of such a situation might be the interception under warrant by an intercepting agency of information pointing to a matter that falls within the jurisdiction of a Parliamentary Inspector, which is defined as an eligible has not been declared to be an interception agency for the purposes of the TIA Act. In these circumstances, it may be possible for the agency to communicate the information to the Parliamentary Inspector in accordance with Part 2-6 of the TIA Act.

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

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

Arrests on the basis of lawfully intercepted information

4.47 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.

4.48 Paragraph 102(2)(a) provides that the total number of arrests across agencies and eligible authorities must be reported. This information is set out in Table 39. The number of arrests made during the reporting period shows a slight increase of 0.9% from the previous reporting period.

Table 39—Arrests on the basis of lawfully intercepted information

AGENCY	NUMBER OF ARRESTS		
	09/10	10/11	11/12
ACC	72	92	53
AFP	116	67	183
CCC WA	1	17	6
CMC QLD	52	4	38
ICAC	2	-	-
NSW CC	135	124	58
NSW POLICE	429	1,070	1,200
NT POLICE	48	34	51
PIC	189	28[8]	6
QLD POLICE	268	393	378
SA POLICE	176	112	80
TAS POLICE	54	12	47
VIC POLICE	371	400	267
WA POLICE	123	88	97
TOTAL [paragraph 102(2)(a)]	**1,913**	**2,441**	**2,464**

Prosecutions in which lawfully intercepted information was given in evidence

4.49 Paragraphs 102(1)(b) and (c) of the TIA Act provide that the report must set out, for each agency and each eligible authority, the categories of prescribed offences prosecuted, and the number of offences in each category, in which lawfully intercepted information was given in evidence, and the number of offences in each category in respect of which convictions were recorded. Paragraphs 102(2)(b) and (c) provide that this information must be set out in total across all agencies and eligible authorities. The information required is set out in Tables 40 to 42.

4.50 During the reporting period, there was an 87.1% increase in the number of prosecutions commenced, and an 11.5% increase in the number of convictions obtained on the basis of lawfully intercepted information.

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

4.51 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.

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

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

CATEGORIES OF OFFENCES	ACC	AFP	CCC WA	CMC QLD	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
Administration of Justice	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	-	-	2	9	-	-	-	-	-	3	-	**14**
Bribery or corruption	-	3	3	-	-	345	1	1	-	10	-	-	45	**408**
Child pornography	-	-	-	-	-	2	-	-	-	-	-	3	-	**5**
Conspiring to commit or aiding or abetting the commission of a serious offence	-	8	-	-	-	113	-	-	-	2	-	1	-	**124**
Cybercrime	-	-	-	-	-	-	-	1	-	-	-	-	-	**1**
Kidnapping	-	-	-	-	1	49	-	-	-	-	-	6	16	**72**
Money laundering	-	34	-	-	53	23	-	-	-	-	-	-	-	**110**
Murder	-	-	-	-	13	61	4	-	-	2	-	11	14	**105**
Offences involving planning and organisation	-	1	-	-	2	237	-	-	-	-	-	3	154	**397**
Organised crime	-	-	-	-	96	178	-	-	-	-	-	-	-	**274**
People Smuggling	-	6	-	-	-	-	-	-	-	-	-	-	-	**6**
Serious arson	-	-	-	-	-	12	-	-	-	-	-	1	6	**19**
Serious damage to property	-	1	-	-	-	13	-	1	-	-	-	4	-	**19**
Serious drug offences	5	110	-	37	360	1,464	42	-	17	32	8	233	457	**2,765**
Serious fraud or loss of revenue	-	5	-	-	61	18	-	2	-	-	-	7	6	**99**
Serious personal injury or loss of life	-	-	-	-	2	743	-	-	-	2	-	56	18	**821**
Special Investigation of the ACC	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Telecommunications offences	-	-	-	-	-	3	-	-	-	-	-	-	-	**3**
Terrorism	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Other offences	-	-	4	2	-	413	-	2	44	2	5	214	-	**686**
TOTAL	**5**	**168**	**7**	**39**	**590**	**3,683**	**47**	**7**	**61**	**50**	**13**	**542**	**716**	**5,928**

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

CATEGORIES OF OFFENCES	ACC	AFP	CMC QLD	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
Administration of Justice	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Assisting a person to escape punishment for or to dispose of the proceeds of a serious offence	-	-	-	2	-	-	-	-	-	-	3	-	**5**
Bribery or corruption	-	3	-	-	3	-	1	-	10	-	-	2	**19**
Child pornography	-	-	-	-	-	-	-	-	-	-	3	-	**3**
Conspiring to commit or aiding or abetting the commission of a serious offence	-	6	-	-	16	-	-	-	2	-	1	-	**25**
Cybercrime	-	-	-	-	-	-	1	-	-	-	-	-	**1**
Kidnapping	-	-	-	1	3	-	-	-	-	-	6	7	**17**
Money laundering	1	4	-	23	-	-	-	-	-	-	-	-	**28**
Murder	-	-	-	12	20	1	-	-	2	-	10	5	**50**
Offences involving planning and organisation	-	1	-	2	47	-	-	-	-	-	3	75	**128**
Organised crime	-	-	-	41	48	-	-	-	-	-	-	-	**89**
Serious arson	-	-	-	-	1	-	-	-	-	-	1	2	**4**
Serious damage to property	-	1	-	-	5	-	1	-	-	-	4	-	**11**
Serious drug offences	2	22	22	207	519	18	-	17	30	7	228	239	**1,311**
Serious fraud or loss of revenue	-	-	-	45	-	-	-	-	-	-	7	2	**54**
Serious personal injury or loss of life	-	-	-	2	76	-	-	-	1	-	54	9	**142**
Special Investigation of the ACC	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Telecommunications offences	-	-	-	-	3	-	-	-	-	-	-	-	**3**
Terrorism	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Other offences	-	-	-	-	112	-	2	43	2	5	213	-	**377**
TOTAL	**3**	**37**	**22**	**335**	**853**	**19**	**5**	**60**	**47**	**12**	**533**	**341**	**2,267**

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

AGENCY	CATEGORIES OF OFFENCES PROSECUTED	NUMBER OF OFFENCES PROSECUTED FOR EACH CATEGORY			NUMBER OF CONVICTIONS RECORDED FOR EACH CATEGORY		
		09/10	10/11	11/12	09/10	10/11	11/12
ACC	Serious Offence	76	3	5	17	3	3
	Other[9]	-	9	-	1	6	-
	Agency Total	76	12	5	18	9	3
AFP	Serious Offence	96	96	168	31	18	37
	Other	1	-	-	-	-	-
	Agency Total	97	96	168	31	18	37
CCC WA	Serious Offence	123	24	3	118	20	-
	Other	-	9	4	-	6	-
	Agency Total	123	33	7	118	26	-
CMC QLD	Serious Offence	-	2	37	-	-	22
	Other	-	-	2	-	10	-
	Agency Total	-	2	39	-	10	22
ICAC	Serious Offence	3	-	-	-	-	-
	Other	-	1	-	-	1	-
	Agency Total	3	1	-	-	1	-
NSW CC	Serious Offence	385	179	590	286	154	335
	Other	-	1	-	-	1	-
	Agency Total	385	180	590	286	155	335
NSW POLICE	Serious Offence	1,149	1,440	3,270	970	936	741
	Other	46	191	413	35	42	112
	Agency Total	1,195	1,631	3,683	1,005	978	853
NT POLICE	Serious Offence	21	17	47	17	8	19
	Other	-	-	-	-	-	-
	Agency Total	21	17	47	17	8	19
OPI	Serious Offence	2	-	-	1	-	-
	Other	-	2	-	-	1	-
	Agency Total	2	2	-	1	1	-
PIC	Serious Offence	7	2	5	5	34	3
	Other	15	-	2	7	9	2
	Agency Total	22	2	7	12	43	5
QLD POLICE	Serious Offence	18	24	17	6	18	17
	Other	1	21	44	1	20	43
	Agency Total	19	45	61	7	38	60
SA POLICE	Serious Offence	44	63	48	36	59	45
	Other	4	2	2	4	2	2
	Agency Total	48	65	50	40	61	47
TAS POLICE	Serious Offence	-	25	8	-	19	7
	Other	-	-	5	-	-	5
	Agency Total	-	25	13	-	19	12
VIC POLICE	Serious Offence	403	413	328	418	376	320
	Other	90	85	214	87	82	213
	Agency Total	493	498	542	505	458	533
WA POLICE	Serious Offence	545	560	716	120	209	341
	Other	50	-	-	20	-	-
	Agency Total	595	560	716	140	209	341
TOTAL	**Serious Offence**	**2,872**	**2,848**	**5,242**	**2,025**	**1,854**	**1,890**
	Other	**207**	**320**	**686**	**155**	**180**	**377**
	Grand Total	**3,079**	**3,168**	**5,928**	**2,180**	**2,034**	**2,267**

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

Interpretative note relating to prosecutions and convictions statistics

4.53 The statistics presented in Tables 40 to 42 should be interpreted with some caution, particularly in presuming a relationship between the number of arrests, prosecutions (which include committal proceedings) and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution/committal (if at all) until a later reporting period and any resulting conviction may be recorded in that or an even later reporting period. Additionally, the number of arrests may not equate to the number of charges laid as an arrested person may be prosecuted and convicted for a number of offences, some or all of which may be prosecuted at a later time.

4.54 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'

4.55 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.

4.56 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.[10]

4.57 Subsection 102(4) of the TIA Act provides that the report must indicate what percentage of each agency's total warrants in force during the reporting period were eligible warrants. These figures are set out in Table 43, and indicate that overall a smaller proportion of agencies' total warrants were eligible warrants when compared to the previous reporting period.

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

Table 43—Percentage of 'eligible warrants'

AGENCY	NUMBER OF ELIGIBLE WARRANTS		TOTAL NUMBER OF WARRANTS		%	
	10/11	11/12	10/11	11/12	10/11	11/12
ACC	119	93	145	109	82	85
ACLEI	-	-	4	11	-	-
AFP	686	551	513	711	134	78
CCC WA	37	19	44	38	84	50
CMC QLD	4	22	22	45	18	49
ICAC	6	14	13	25	46	56
NSW CC	342	308	496	406	69	76
NSW POLICE	1,063	1,162	1,437	1,524	74	76
NT POLICE	39	50	46	64	84	78
OPI	15	4	47	17	32	24
PIC	21	32	70	67	30	48
QLD POLICE	165	219	193	233	85	94
SA POLICE	104	107	113	116	92	92
TAS POLICE	28	22	21	42	133	52
VIC POLICE	244	240	335	336	73	71
WA POLICE	73	117	250	308	29	38
TOTAL [subsection 102(4)]	**2,946**	**2,960**	**3,749**	**4,052**	**79**	**60**

Emergency interception

4.58 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.

4.59 An interception in reliance on subsection 7(4) of the TIA Act may be carried out by an officer of one of the above agencies where the officer is a party to the communication, and because of the urgency of the need for the act to be done, it is not reasonably practicable for an application for a telecommunications interception warrant to be made. There also must be reasonable grounds for suspecting that the other party to the communication has:

- done an act that has resulted or may result in loss of life or the infliction of serious personal injury
- threatened to kill or seriously injure another person or to cause serious damage to property, or
- threatened to take his or her own life or to do an act that would or may endanger his or her own life or create a serious threat to his or her health or safety.

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

4.61 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).

4.62 In the reporting period one interception was carried out in reliance on subsection 7(5). The information required by section 102A is set out in Table 44.

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

SUSPICION OF	AFP
An act that may result in loss of life or serious injury	1
TOTAL	**1**

Other information

Total expenditure incurred by agencies

4.63 Paragraph 103(a) of the TIA Act provides that the report include details of the total expenditure (including expenditure of a capital nature) incurred by agencies in connection with the execution of telecommunications interception warrants for law enforcement purposes. The information required by this subsection is set out in Table 45. Total expenditure incurred by agencies in connection with telecommunications interception increased only slightly by 0.6% from the previous reporting period. This is in contrast to the 9% increase between the 2009/10 and 2010/11 reporting periods.

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

AGENCY	TOTAL EXPENDITURE ($)		
	09/10	10/11	11/12
ACC[11]	5,324,765	5,962,085	6,425,353
ACLEI	7,460	23,309	598,099
AFP	9,586,423	9,488,869	10,602,387
CCC WA	1,520,265	3,103,641	1,372,745
CMC QLD	1,254,986[12]	1,557,672	1,566,801
ICAC	153,907	108,032	473,941
NSW CC	4,063,904	3,927,948	3,418,025
NSW POLICE	5,296,367	5,327,911	4,456,690
NT POLICE	701,485	832,000	864,160
OPI	2,034,841	1,244,783	1,293,041
PIC	1,141,823	1,248,984	1,288,457
QLD POLICE	3,321,572[13]	5,231,250	6,153,040
SA POLICE	2,717,562	2,688,290	2,716,991
TAS POLICE	416,000	502,591	580,378
VIC POLICE	5,531,058	5,755,955	5,484,280
WA POLICE	3,116,737	3,270,702	3,259,619
TOTAL	**46,189,155**	**50,274,022**	**50,554,007**

[11] ACC advised that the information supplied for the 09/10 and 10/11 periods was inaccurate, and this report reflects the accurate figure.

[12] This figure includes start-up costs for the Crime and Misconduct Commission.

[13] This figure includes start-up costs for the Queensland Police Service.

Average expenditure per telecommunications interception warrant

4.64 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.

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

Table 46—Average expenditure per telecommunications interception warrant

AGENCY	AVERAGE EXPENDITURE ($)		
	09/10	10/11	11/12
ACC[14]	25,356	31,379	44,933
ACLEI	7,460	5,827	66,455
AFP	14,924	18,143	19,634
CCC WA	38,007	88,675	42,898
CMC QLD	73,823	66,307	38,215
ICAC	10,993	9,003	19,748
NSW CC	11,073	9,650	9,879
NSW POLICE	4,642	4,166	2,839
NT POLICE	14,030	18,305	16,003
OPI	56,523	27,662	107,754
PIC	23,788	19,825	20,782
QLD POLICE	19,311	29,555	28,225
SA POLICE	24,049	25,124	26,637
TAS POLICE	20,800	18,614	17,587
VIC POLICE	14,225	18,158	18,718
WA POLICE	9,590	14,159	11,810

Availability of eligible judges and nominated AAT members

4.66 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

[14] ACC advised that the information supplied for the 09/10 and 10/11 periods was inaccurate, and this report reflects the accurate figure.

extent to which nominated AAT members have been used for that purpose. This information is set out in Tables 47 and 48.

Table 47—Availability of Federal Court Judges, Family Court Judges, Federal Magistrates and nominated AAT Members to issue telecommunications interception warrants[15]

ISSUING AUTHORITY	NUMBER ELIGIBLE
FEDERAL COURT JUDGES	12
FAMILY COURT JUDGES	4
FEDERAL MAGISTRATES	34
NOMINATED AAT MEMBERS	39

4.67 During the reporting period, approximately 82.7% of telecommunications interception warrants were issued by AAT members, 11.4% by Federal Magistrates, 5.4% by Family Court Judges and 0.4% by Federal Court Judges. The number of warrants issued by authorities is influenced by an agency's operational needs and the availability of an issuing authority at the time of application.

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

AGENCY	ISSUING AUTHORITY			
	FEDERAL COURT JUDGES	FAMILY COURT JUDGES	FEDERAL MAGISTRATES	NOMINATED AAT MEMBERS
ACC	-	-	-	151
ACLEI	-	-	5	4
AFP	10	16	56	459
CCC WA	-	-	-	32
CMC QLD	-	-	-	41
ICAC	-	-	-	24
NSW CC	-	-	3	343
NSW POLICE	-	-	201	1,549
NT POLICE	-	-	29	25
OPI	-	-	-	12
PIC	7	-	-	55
QLD POLICE	-	-	155	63
SA POLICE	-	-	-	102
TAS POLICE	-	-	-	33
VIC POLICE	-	-	-	295
WA POLICE	-	199	-	77
TOTAL	**17**	**215**	**449**	**3,265**

Interceptions on behalf of other agencies

4.68 Paragraph 103(ac) of the TIA Act provides that the report must set out the number (if any) of interceptions carried out by each agency on behalf of other agencies. Table 49 sets

[15] 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.

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

4.69 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.

4.70 During the reporting period there were 114 interceptions carried out on behalf of other agencies, a decrease of 61.6% from the 297 carried out in the previous reporting period.

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

INTERCEPTION CARRIED OUT BY:	INTERCEPTION CARRIED OUT ON BEHALF OF:	No. OF INTERCEPTIONS
ACC	ACLEI	4
ACC	CMC QLD	53
ACC	QLD POLICE	11
AFP	ACLEI	6
AFP	NSW CC	6
AFP	NSW POLICE	1
VIC POLICE	TAS POLICE	33
TOTAL		114

Resources devoted to telecommunications interception

4.71 In addition to the total expenditure figures provided in Table 45, the figures in Table 50 below were supplied by each agency and provide a breakdown of the total recurrent costs of interception over the reporting period. However, as agencies do not necessarily treat particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

Table 50—Recurrent costs of interceptions per agency

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL ($)
ACC	5,213,764	1,016,207	94,586	100,796	**6,425,353**
ACLEI	583,817	-	-	14,282	**598,099**
AFP	6,796,311	129,546	953,598	2,722,932	**10,602,387**
CCC WA	732,253	94,910	465,210	80,372	**1,372,745**
CMC QLD	806,354	126,804	283,125	350,517	**1,566,800**
ICAC	41,108	11,777	406,700	14,356	**473,941**
NSW CC	1,926,175	41,854	577,974	872,022	**3,418,025**
NSW POLICE	3,520,567	609,584	-	326,539	**4,456,690**
NT POLICE	683,554	5,854	-	174,752	**864,160**
OPI	1,109,759	121,157	-	62,125	**1,293,041**
PIC	1175,818	-	-	112,451	**1,288,269**
QLD POLICE	3,603,430	147,562	1,415,796	986,253	**6,153,041**
SA POLICE	2,176,357	237,979	192,573	110,082	**2,716,991**
TAS POLICE	456,069	-	117,525	6,784	**580,378**

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL ($)
VIC POLICE	4,316,232	320,606	297,735	549,707	**5,484,280**
WA POLICE	3,145,923	194,910	-	113,696	**3,454,529**

Emergency services facility declarations

4.72 Paragraph 103(ad) of the TIA Act provides that the report must include the number and type of premises for each State and Territory that have been declared by the Attorney-General to be emergency services facilities pursuant to subsection 6(2A) of the TIA Act during the reporting period. The declarations enable such facilities to record incoming and outgoing calls without a telecommunications interception warrant. Table 51 provides the required information.

Table 51—Emergency service facility declarations

STATE/TERRITORY	POLICE	FIRE BRIGADE	AMBULANCE	EMERGENCY SERVICES AUTHORITY	DESPATCHING
NEW SOUTH WALES	8	97	6	-	3
VICTORIA	18	-	30	3	22
QUEENSLAND	21	13[16]	6		10
WESTERN AUSTRALIA	1	-	1	2	3
SOUTH AUSTRALIA	1	2	1	-	1
TASMANIA	1	2	1	-	2
AUSTRALIAN CAPITAL TERRITORY	3	-	-	1	1
NORTHERN TERRITORY	2	-	1	1	3
TOTAL	**55**	**114**	**46**	**7**	**45**

Reports by Commonwealth Ombudsman

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

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

[16] The Queensland Government has advised that three of the facilities also cater to Queensland Ambulance Service.

ACLEI

4.74 The Ombudsman conducted two inspections of ACLEI's telecommunications interception records during the reporting period. The inspections were conducted on 12 October 2011 and again on 15 February 2012. During the reporting period six telecommunications interception warrants issued to ACLEI either expired or were revoked, all of which were assessed by the Ombudsman.

4.75 ACLEI was assessed as compliant with the record keeping requirements connected with the issues of warrants under section 80 of the TIA Act and compliant with the other record keeping requirements in connection with interceptions under section 81 of the TIA Act.

4.76 The Ombudsman noted that apart from some minor administrative errors, no contraventions of the TIA Act were found. The Ombudsman did however note that ACLEI is yet to implement a formalised standard operating procedures to provide guidance to its staff on the telecommunications interception record keeping and revocation requirements of the TIA Act.

4.77 The Ombudsman raised this issue with ACLEI on 12 October 2011 and was advised on 15 February 2012 that it intended to finalise these procedures as soon as possible. The Ombudsman noted that ACLEI has provided informal guidance to staff on the procedures involved in maintaining accurate records and revoking telecommunications interception warrants.

The ACC

4.78 The Ombudsman conducted two inspections of the ACC's telecommunications interception records during the reporting period. The inspections were conducted from 5 to 7 December 2011 and again from 21 to 23 May 2012. Of the 175 telecommunications warrants issued to the ACC which had expired or were revoked during 2011, a sample of 116 was selected for inspection, and of the 144 reported destroyed warrants, a sample of 43 was selected for inspection.

4.79 The ACC was assessed as compliant with the destruction requirements under section 79 of the TIA Act, compliant with the record keeping requirements connected with the issue of warrants under section 80 of the TIA Act and compliant with the other record keeping requirements in connection with interceptions under section 81 of the TIA Act.

4.80 The Ombudsman noted that the ACC continues to manage its interception activities effectively, and that the ACC seeks to continuously improve its administrative processes and procedures. The Ombudsman also noted that the ACC remains cooperative during inspections and is receptive to feedback and suggestions for improvement.

4.81 The Ombudsman has noted in their report that one administrative issue was present regarding the form of warrants issued. Under section 80(a) of the TIA Act, warrants must comply with the form prescribed by the *Telecommunications (Interception and Access) Regulations 1987*. Six warrants issued to the ACC were identified as not being in the prescribed form. The ACC has responded to this issue, and at the second inspection, they self-disclosed all warrants identified as not being in the prescribed form. The ACC has

advised the Ombudsman that it will take appropriate staff training measures to rectify this issue.

The AFP

4.82 The Ombudsman conducted two inspections of the AFP's telecommunications interception records during the reporting period. The inspections were conducted from 25 to 27 October 2011 and again from 8 to 10 February 2012. Of the 515 telecommunications warrants issued to the AFP which had expired or revoked during 2011, a sample of 113 was selected for inspection, and of the 307 reported destroyed warrants, a sample of 69 was selected for inspection.

4.83 The AFP was assessed as compliant with the destruction requirements under section 79 of the TIA Act, compliant with the record keeping requirements connected with the issue of warrants under section 80 of the TIA Act and compliant with the other record keeping requirements in connection with interceptions under section 81 of the TIA Act.

4.84 During their inspection under section 85 of the TIA Act, the Ombudsman noted two compliance issues.

4.85 The first issue noted by the Ombudsman was that, for two inspected warrants, the Ombudsman was unable to determine if all interceptions were conducted in accordance with the warrants. On inspection, a connection between the lines of the communications that were intercepted and the details listed in the warrants could not be established. This has been attributed to the relevant carrier failing to provide the AFP with sufficient information to establish the connection. In response to this finding, the AFP has advised the Ombudsman that is has begun working with the relevant carrier to rectify this issue and anticipates that the carrier should be able to provide this information in the near future.

4.86 The second issue was that the AFP had applied for one warrant in respect of a natural person, but the warrant was issued in respect of a company. Further investigation by the Ombudsman found that the warrant was in relation to an unidentified individual using a device that was subscribed to by a company and that the warrant was issued to the subscriber company rather than the individual.

4.87 The Ombudsman has noted that as the warrant was issued in respect of a company, theoretically the warrant would allow the AFP to obtain any communications made to or by other persons working for the company and using the service identified on the warrant. The Ombudsman noted however that the warrant was issued in relation to a mobile phone service and therefore the risk may have been mitigated in this instance.

Other information

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

Stored communications

4.89 The Ombudsman inspected the records of 15 enforcement agencies pursuant to the stored communications provisions of the TIA Act and provided the reports to the Attorney-General under section 153(1) of the TIA Act. The agencies inspected were the Australian Competition and Consumer Commission, ACC, ACBPS, AFP, CMC Queensland,

NSW CC, NSW Police, NT Police, OPI, PIC, Queensland Police Service, SA Police, Tasmania Police, Victoria Police, WA Police.

4.90 The Ombudsman has reported that all agencies were assessed as compliant with the record keeping requirements relating to the issue of stored communications warrants under section 151 of the TIA Act.

4.91 The Ombudsman reported that five agencies destroyed records under section 150 of the TIA Act during 2010-11. Of these, two agencies were assessed as non-compliant. The Ombudsman has noted that one of the agencies took immediate remedial action to address the relevant issues and has advised that they have implemented procedures to address these issues. The other agency has since implemented appropriate procedures and practices to ensure compliance.

4.92 The Ombudsman noted that an overall improvement in agency compliance was seen, with fewer recommendations needed than last year. The Ombudsman also noted that most agencies have updated relevant policies and procedures to assist their staff to better comply with the TIA Act, and have implemented measures to assure themselves that they are only dealing with lawfully obtained stored communications.

Access to stored communications

4.93 During the course of the Ombudsman's assessment of agencies, an issue was identified which highlighted the ambiguity that arises when attempting to interpret what constitutes 'access' to stored communications under section 6AA and 'first executed' under section 119 of the TIA Act. It was noted that this ambiguity poses a risk to all agencies that use the legislative provisions and prevents the Ombudsman from making conclusive assessments of whether or not stored communications warrants are lawfully executed.

4.94 The Ombudsman notes that for a carrier to access a stored communication under an agency's warrant, it would perform a number of tasks that would meet the criteria for accessing such as preserving, downloading or recording. However, carriers can perform these tasks over a number of days, creating ambiguity as to what date 'access' occurred and therefore when the warrant was first executed.

4.95 The Ombudsman stated that these ambiguities have created uncertainty for agencies that have applied the relevant provisions with the intention of meeting their statutory obligations. The Ombudsman is also concerned that, as agencies are left to rely on their own risk assessments and any court decisions, this may diminish the effectiveness of their oversight role.

4.96 In the Ombudsman's view, in order to ensure that stored communications are accessed with appropriate controls and that it can provide effective oversight, there needs to be clarity regarding what constitutes 'access' of stored communications and 'execution' of a warrant. These definitions also need to accommodate the practicalities involved for carriers when they execute stored communications warrants and assist agencies in their law enforcement activities.

Accessing stored communications other than those permitted by the TIA Act

4.97 The Ombudsman noted that during their inspections they identified some instances where it appeared that stored communications, other than those permitted by the TIA Act, were accessed by carriers and provided to agencies.

4.98 The Ombudsman has recommended to agencies that they screen all stored communications they receive from carriers to ensure that the communications were sent to, or by the person, listed on the warrant. Further, the Ombudsman requests that in instances where communications are received that are outside the authority of the warrant, the communications be quarantined.

CHAPTER 5—STORED COMMUNICATIONS INFORMATION REQUIRED UNDER THE ACT

The information required

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

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

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

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

Which agencies may seek stored communications warrants?

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

- ACBPS
- ASIC

- Australian Competition and Consumer Commission
- Australian Taxation Office
- Centrelink, and
- Department of Immigration and Citizenship

Applications for stored communications warrants

5.5 Paragraphs 162(1)(a) and (2)(a) of the TIA Act provide that the report must set out how many applications for stored communications warrants were made, how many applications were withdrawn or refused and the number of warrants issued during the reporting year for each agency and in total. This information is presented in Table 52. Only those enforcement agencies that applied for stored communications warrants during the past three reporting periods are included in the table.

5.6 Stored communications warrants continue to be a valuable tool for agencies, with the number of warrants issued increasing each year. There were 61% more store communications warrants issued during 2011-12 than in the previous reporting year.

Table 52—Applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
ACBPS	Made Refused/withdrawn Issued	7 - 7	7 - 7	5 - 5
ACC	Made Refused/withdrawn Issued	55 - 55	27 - 27	8 - 8
AFP	Made Refused/withdrawn Issued	39 - 39	25 - 25	76 - 76
ASIC	Made Refused/withdrawn Issued	10 - 10	- - -	3 - 3
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	Made Refused/withdrawn Issued	- - -	5 - 5	3 1 2
CCC WA	Made Refused/withdrawn Issued	1 - 1	- - -	2 - 2
CMC QLD	Made Refused/withdrawn Issued	9 - 9[17]	2 - 2	- - -
NSW CC	Made Refused/withdrawn Issued	1 - 1	- - -	6 - 6
NSW POLICE	Made Refused/withdrawn Issued	22 - 22	90 1 89	181 - 181
NT POLICE	Made Refused/withdrawn Issued	2 - 2	11 - 11	12 - 12

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

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
OPI	Made	2	2	-
	Refused/withdrawn	-	-	-
	Issued	2	2	-
PIC	Made	-	8	10
	Refused/withdrawn	-	-	-
	Issued	-	8	10
QLD POLICE	Made	66	48	63
	Refused/withdrawn	-	-	-
	Issued	66	48	63
SA POLICE	Made	5	5	12
	Refused/withdrawn	-	-	-
	Issued	5	5	12
TAS POLICE	Made	46	45	32
	Refused/withdrawn	-	1	1
	Issued	46	44	31
VIC POLICE	Made	6	11	9
	Refused/withdrawn	-	-	-
	Issued	6	11	9
WA POLICE	Made	14	14	63
	Refused/withdrawn	-	-	-
	Issued	14	14	63
TOTAL [paragraph 162(2)(a)]	**Made**	**285**	**300**	**485**
	Refused/withdrawn	**-**	**2**	**2**
	Issued	**285**	**298**	**483**

Telephone applications for stored communications warrants

5.7 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.

5.8 During the reporting period there were no telephone applications for stored communications warrants made. This particular method of application is seldom used and has steadily decreased in usage over previous reporting periods.

5.9 This information is presented in Table 53.

Table 53—Telephone applications for stored communications warrants

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
NSW POLICE	Made	3	3	-
	Refused/withdrawn	-	-	-
	Issued	3	3	-
VIC POLICE	Made	2	-	-
	Refused/withdrawn	-	-	-
	Issued	2	-	-

Renewal applications for stored communications warrants

5.10 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.

5.11 There were no renewal applications for stored communications warrants made during the reporting period.

Stored communications warrants subject to conditions or restrictions

5.12 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.

5.13 There has been an increase in the number stored communications warrants issued subject to conditions and restrictions as a proportion of the total, although in absolute terms the numbers remain small. This information is presented in Table 54.

Table 54—Stored communications warrants subject to conditions or restrictions

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		
		09/10	10/11	11/12
AFP	Made	1	-	9
	Refused/withdrawn	-	-	-
	Issued	1	-	9
CMC QLD	Made	-	2	-
	Refused/withdrawn	-	-	-
	Issued	-	2	-
SA POLICE	Made	-	4	12
	Refused/withdrawn	-	-	-
	Issued	-	4	12
QLD POLICE	Made	1	2	2
	Refused/withdrawn	-	-	-
	Issued	1	2	2
TOTAL	**Made**	**2**	**8**	**23**
	Refused/withdrawn	**-**	**-**	**-**
	Issued	**2**	**8**	**23**

Effectiveness of stored communications warrants

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

5.14 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 55. The table also includes the number of convictions recorded based on lawfully accessed information.

5.15 As the table below illustrates, there has been an increase in all categories, with a 109.1% increase in convictions from lawfully accessed information from the previous reporting period.

Table 55—Number of arrests, proceedings and convictions made on the basis of lawfully accessed information

AGENCY	ARRESTS			PROCEEDINGS			CONVICTIONS		
	09/10	10/11	11/12	09/10	10/11	11/12	09/10	10/11	11/12
ACC	10	8	20	-	-	9	-	-	3
AFP	1	2	5	1	2	4	-	2	8
ACBPS	3	-	-	1	-	2	-	1	2
ASIC	-	-	-	-	-	-	-	-	1[18]
CMC QLD	15	1	1	-	2	-	-	2	1
NSW CC	-	-	5	-	-	-	-	-	-
NSW POLICE	10	25	47	22	3	172	20	2	48
NT POLICE	1	-	3	-	-	-	-	-	-
QLD POLICE	47	35	12	12	14	2	12	14	4
SA POLICE	-	1	-	2	1	1	2	1	1
TAS POLICE	25	16	4	7	11	-	8	11	-
VIC POLICE	1	3	9	3	-	1	7	-	1
TOTAL	**113**	**91**	**106**	**48**	**33**	**191**	**49**	**33**	**69**

Interpretative note relating to prosecutions and convictions statistics

5.16 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.

5.17 Additionally, the information in Table 56 should be interpreted with caution. Due to operational priorities, an arrest recorded in one reporting period may not result in a prosecution/committal (if at all) until a later reporting period and any resulting conviction may be recorded in that or an even later reporting period. Additionally, the number of arrests may not equate to the number of charges laid as an arrested person may be prosecuted and convicted for a number of offences, some or all of which may be prosecuted at a later time.

[18] This conviction relates to an investigation that began in October 2009, with the suspect pleading guilty in December 2010.

CHAPTER 6—TELECOMMUNICATIONS DATA - INFORMATION REQUIRED UNDER THE ACT

The information required

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

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

Which agencies may authorise the disclosure of telecommunications data

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

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

Authorisations granted

6.4 The number of authorisations made for access to existing information or documents in the enforcement of the criminal law is given at Table 56. 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 57.

Table 56—Number of authorisations made for access to existing information or documents in the enforcement of the criminal law

AGENCY	AUTHORISATIONS		
	09/10	10/11	11/12
ACC	12,467	12,467	6,764
ACLEI	65	160	99
AFP	20,869	22,992	22,900
AUSTRALIAN COMPETITION & CONSUMER COMMISSION	35	25	77
ACBPS	4,157	4,017	5,197
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	2	4	1
ASIC	2,874	1,602	1,587
AUSTRALIAN TAXATION OFFICE	610	724	654
CCC WA	506	357	1,305
CMC QLD	9,577[19]	8,395	7,040
CORRECTIVE SERVICES NSW	37	63	108
CORRECTIONS VICTORIA	-	82	131
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY	89	22	76
DEPARTMENT OF COMMERCE (WA)	184	314	458
DEPARTMENT OF DEFENCE	30	20	10
DEPARTMENT OF ENVIRONMENT AND HERITAGE PROTECTION (QLD)[20]	-	-	4
DEPARTMENT OF ENVIRONMENT AND RESOURCE MANAGEMENT (QLD)	-	8	-[21]
DEPARTMENT OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFIARS	7	23	-
DEPARTMENT OF FOREIGN AFFAIRS AND TRADE[22]	-	-	3
DEPARTMENT OF HEALTH AND AGEING	22[23]	47	52
DEPARTMENT OF IMMIGRATION AND CITIZENSHIP	86	180	24
DEPARTMENT OF PRIMARY INDUSTRIES (VIC)	464	469	590
DEPARTMENT OF SUSTAINABILITY, ENVIRONMENT, WATER, POPULATION AND COMMUNITIES[24]	22	12	28

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

[20] Previously reported as the Department of Environment and Resource Management (Qld).

[21] On 30 March 2012 the Queensland Government announced machinery-of-government change that has seen the Department of Environment and Resource Management (Qld) cease operations.

[22] The Department of Foreign Affairs and Trade was not an 'enforcement agency' in previous reporting periods.

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

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

AGENCY	AUTHORISATIONS		
	09/10	10/11	11/12
ICAC	450	596	594
INSOLVENCY AND TRUSTEE SERVICE AUSTRALIA	211	135	181
JUVENILE JUSTICE NSW	-	3	-
NSW CC	3,602	2,915	3,649
NSW POLICE	115,343	41,340	103,824
NT POLICE	1,834	3,695	2,828
OFFICE OF ENVIRONMENT & HERITAGE (NSW)[25]	119	192	156[26]
OPI	2,235	5,246	307
PIC	1,242	1,731	1,470
QLD POLICE	10,223	30,896[27]	36,531
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS QUEENSLAND	46	52	27
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS TASMANIA INC.	-	-	1
ROYAL SOCIETY FOR THE PREVENTION OF CRUELTY TO ANIMALS VICTORIA	16	31	35
SA POLICE	11,631	7,094	8,025
TAS POLICE	6,689	9,845	9,342
TRANSPORT ACCIDENT COMMISSION (VIC)	2	4	9
VIC POLICE	50,234	65,703[28]	67,173
VICTORIAN TAXI DIRECTORATE	3	18	-
WA POLICE	26,234	22,152	12,293
TOTAL	**282,195**	**243,631**	**293,501**

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

[26] The Office of Environment & Heritage advised that during the reporting period they and Environment Protection Authority separated. The figure includes both agencies as they continue to share administration resources.

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

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

Table 57—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		
	09/10	10/11	11/12
ACT REVENUE OFFICE	-	-	4
AFP	267	359	101
AUSTRALIAN COMPETITION AND CONSUMER COMMISSION	10	66	89[29]
ACBPS	225	173	116
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	4	-	-
AUSTRALIAN HEALTH PRACTITIONER REGULATION AGENCY[30]	-	-	4
ASIC	123	209	179
AUSTRALIAN TAXATION OFFICE	504	249	177
AUSTRALIA POST	361	160	251
BANKSTOWN CITY COUNCIL	-	-	4[31]
CENTRELINK	2,579	2,127	1,181
CHILD SUPPORT PROGRAM[32]	74	67	23
CMC QLD	1	-	-
CONSUMER AFFAIRS VICTORIA	235	269	230
CONSUMER AND BUSINESS SERVICES (SA)[33]	201	178	141
CORRECTIONS VICTORIA	52	67	-
DEPARTMENT OF AGRICULTURE, FISHERIES AND FORESTRY (QLD)[34]	-	-	33
DEPARTMENT OF COMMERCE (WA)	20	99	57
DEPARTMENT OF DEFENCE	129[35]	104[36]	279
DEPARTMENT OF ENVIRONMENT AND CONSERVATION (WA)	18	39	34
DEPARTMENT OF ENVIRONMENT AND HERITAGE PROTECTION (QLD)[37]	3	1	26

[29] The Australian Competition and Consumer Commission has advised that the increase in requests is in large part a reflection of the introduction of the Australian Consumer Law carrying civil pecuniary penalties as remedies for civil pecuniary matters.

[30] Australian Health Practitioner Regulation Agency was not an 'enforcement agency' in previous reporting periods.

[31] Bankstown City Council was not an enforcement agency in previous reporting periods.

[32] Previously known as Child Support Agency.

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

[34] Queensland Boating and Fisheries Patrol was previously part of the Department of Employment, Economic Development and Innovation until 1 September 2011, at which point the area was moved to the Department of Transport and Main Roads. Another move in 7 April 2011 saw the formation of the Department of Agriculture, Fisheries and Forestry.

[35] Department of Defence advised that the information supplied for the 09/10 period was inaccurate, this report reflects the accurate figure.

[36] Department of Defence advised that the information supplied for the 10/11 period was inaccurate, this report reflects the accurate figure.

[37] Previously known as the Department of Environment and Resource Management (Qld).

AGENCY	AUTHORISATIONS		
	09/10	10/11	11/12
DEPARTMENT OF EMPLOYMENT, ECONOMIC DEVELOPMENT AND INNOVATION (QLD)	21	41	-[38]
DEPARTMENT OF FISHERIES (WA)	-	-	71
DEPARTMENT OF HEALTH AND AGEING[39]	4[40]	6	1
DEPARTMENT OF IMMIGRATION AND CITIZENSHIP	204	76	-
DEPARTMENT OF JUSTICE (NT)	2	-	-
DEPARTMENT OF JUSTICE AND ATTORNEY-GENERAL (QLD)	-	-	309
DEPARTMENT OF PRIMARY INDUSTRIES (NSW)[41]	108	65	100
DEPARTMENT OF PRIMARY INDUSTRIES (VIC)	1	3	-
DEPARTMENT OF SUSTAINABILITY AND ENVIRONMENT (VIC)	75	108	23
DEPARTMENT OF SUSTAINABILITY, ENVIRONMENT, WATER, POPULATION AND COMMUNITIES (DSEWPC)[42]	-	-	5
HEALTH CARE COMPLAINTS COMMISSION (NSW)	8	30	39
ICAC	24	-	-
JUVENILE JUSTICE NSW	1	2	2
MEDICARE AUSTRALIA	10[43]	21	58
NSW FAIR TRADING	1,012	935	1,003
NSW POLICE	-	2,076	5464
OFFICE OF LIQUOR AND GAMING REGULATION (QLD)	-	-	2
OFFICE OF LIQUOR, GAMING AND RACING (NSW)	-[44]	2	-
OFFICE OF STATE REVENUE (NSW)	132	224	127
OFFICE OF STATE REVENUE (QLD)	27	20	10
OFFICE OF THE AUSTRALIAN BUILDING AND CONSTRUCTION COMMISSIONER[45]	12	31	7
QLD POLICE	-	56	144

[38] Following the 2012 Queensland election, the Department of Employment, Economic Development and Innovation ceased and its functions distributed to other agencies: http://www.deedi.qld.gov.au/.

[39] Department of Health and Ageing includes those of the Therapeutic Goods Administration.

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

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

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

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

[44] The Office of Liquor, Gaming and Racing was not an enforcement agency in previous reporting periods

[45] The Office of the Australian Building and Construction Commissioner conclude operations on 1 June 2012. A new specialist regulator for the building and construction industry, the Fair Work Building & Construction (FWBC), has now commenced operations.

AGENCY	AUTHORISATIONS		
	09/10	10/11	11/12
REVENUE SA	77	90	26
SA POLICE	-	1	-
STATE REVENUE OFFICE VICTORIA	130	106	45
TASMANIA PRISON SERVICE	3	5	7
TAS POLICE	-	-	534
TAX PRACTITIONERS BOARD	-	-	12[46]
VICTORIAN TAXI DIRECTORATE	3	4	-
WORKCOVER QUEENSLAND	4	-	-
WORKSAFE VICTORIA	27	13	7
WYNDHAM CITY COUNCIL	-[47]	20	11
TOTAL	**6,704**	**8,102**	**10,936**

6.5 The number of authorisations made by a criminal law-enforcement agency for access to specified information or documents that come into existence during the period for which the authorisations is in force is given in Table 58. 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.

[46] The Tax Practitioners Board was not an 'enforcement agency' in previous reporting periods.

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

Table 58—Prospective authorisations

AGENCY	NUMBER OF AUTHORISATIONS MADE			DAYS SPECIFIED IN FORCE			ACTUAL DAYS IN FORCE			AUTHORISATIONS DISCOUNTED		
	09/10	10/11	11/12	09/10	10/11	11/12	09/10	10/11	11/12	09/10	10/11	11/12
ACC	114	422	529	4,461	17,229	17,643	2,884	15,851	17,643	-	29	-
AFP	3	86	194	46	3,830	308	46	3,055	226	-	10	2
ACBPS	148	683	487	4,577	6,643	17,609	3,714	4,697	14,155	7	23	44
CCC WA	67	51	29	2,502	1,817	1,160	1,840	1,273	1,015	6	5	2
CMC QLD	174	86	268	6,927	3,830	3,102	6,919	3,055	2,628	20	10	4
ICAC	2	-	35	3	-	1,565	3	-	649	-	-	7
NSW CC	967	850	797	27,078	22,097	26,905	24,740	19,586	19,832	64	74	28
NSW POLICE	221	370	573	5,771	10,311	21,586	3,960	6,110	12,032	10	32	42
NT POLICE	322	435	285	14,448	15,975	12,765	12,234	13,936	12,511	20	36	10
OPI[48]	19	19	17	719	510	549	653	396	403	9	-	-
PIC	127	94	182	5,299	3,882	7,773	4,218	3,108	5,295	25	8	41
QLD POLICE	451	641	816	9,775	18,931	24,613	8,684	17,753	17,315	41	43	88
SA POLICE	83	181	311	2,953	6,426	11,538	1,755	4,057	8,330	6	10	9
TAS POLICE	40	110	127	1,800	4,950	5,715	1,007	2,332	2,826	-	11	11
VIC POLICE	797	547	787	25,335	20,789	30,298	18,357	13,896	20,050	32	30	31
WA POLICE[49]	272	347	374	12,240	15,615	16,830	6,989	7,783	8,779	33	35	41
TOTAL	**3,804**	**4,836**	**5,811**	**123,934**	**149,005**	**199,959**	**97,911**	**113,833**	**143,689**	**273**	**346**	**360**

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

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

6.6 Information is also given about the average number of days the authorisations were specified in force, and the average actual number of days they remained in force. This information is presented at Table 59.

Table 59—Average specified and actual time in forces

AGENCY	AVERAGE PERIOD SPECIFIED			AVERAGE PERIOD ACTUAL		
	09/10	10/11	11/12	09/10	10/11	11/12
ACC	39	41	33	25	40	33
AFP	31	10	36	26	7	32
ACBPS	15	-	33	15	-	33
CCC WA	37	36	40	30	28	38
CMC QLD	40	45	12	45	40	10
ICAC	2	-	45	2	-	23
NSW CC	28	26	34	27	25	28
NSW POLICE	26	28	38	19	18	23
NT POLICE	45	37	45	41	35	45
OPI[50]	38	27	32	33	21	24
PIC	42	41	43	41	36	38
QLD POLICE	22	30	30	21	30	24
SA POLICE	36	35	37	23	23	28
TAS POLICE	45	45	45	25	23	24
VIC POLICE	32	38	21	24	27	13
WA POLICE	45	45	45	29[51]	25	26
TOTAL	**33**	**34**	**36**	**30**	**27**	**28**

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

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

CHAPTER 7—FURTHER INFORMATION

7.1 Further information about the *Telecommunications (Interception and Access) Act 1979* can be obtained by contacting the Attorney-General's Department:

Telecommunications and Surveillance Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

(02) 6141 2900

7.2 Previous copies of the *Telecommunications (Interception and Access) Act 1979* Annual Report can be accessed online at: www.ag.gov.au