Australian Government

Attorney-General's Department

Telecommunications (Interception and Access) Act 1979

Annual Report 2012-13

ISBN 978-1-925118-06-3

© Commonwealth of Australia 2013
All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia licence (www.creativecommons.org/licenses).
For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 3.0 AU licence (www.creativecommons.org/licenses).

Use of the Coat of Arms
The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.itsanhonour.gov.au). 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

EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) Act 1979* Act Annual Report 2012-13 sets out how eligible Commonwealth, State and Territory government agencies have used the powers under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) between 1 July 2012 and 30 June 2013.

The TIA Act protects the privacy of individuals who use the Australian telecommunications system by prohibiting access to telecommunications content and data. There are exceptions to this prohibition, such as access under a warrant to support national security and law enforcement criminal investigations into serious crime and exceptions to support emergency services.

The powers contained in the TIA Act support law enforcement agencies in their identification of criminal networks, co-conspirators and organised crime associates and assists in establishing the methodology of criminal enterprises. They also play an important role in identifying child exploitation material, sexual slavery and terrorist organisations.

During 2012-2013, information obtained under interception and stored communications warrants were used in:

- 3,083 arrests
- 6,898 prosecutions
- 2,765 convictions

Telecommunications data is commonly an early source of important lead information for further investigations and plays an important role in identifying as well as narrowing a field of potential suspects. Telecommunications data is also lawfully accessible under the TIA Act to help locate missing persons. In 2012-2013, there were 895 cases in which telecommunications data was used in a missing person's case.

This year, the TIA Act was amended to include the Victorian Independent Broad-based Anti-corruption Commission and the South Australian Independent Commissioner Against Corruption as interception agencies. Access to interception powers is vital to support investigations into corruption given the nature of corruption offences.

In addition, the Act was amended to support the introduction of the Victorian Public Interest Monitor (PIM) to support its role in overseeing applications for interception warrants in that State. This is the second PIM that has been introduced and the amendments enable the PIM to see and appear in applications for interception warrants.

The TIA Act was also amended to support Australia's accession to the Council of Europe's Convention on Cybercrime. Accession occurred on 1 March 2013 and supports Australia's commitment to prevent, detect and prosecute cybercrime offences. Accession strengthens international investigations, enabling Australia to interact on a global level by supporting access to and the sharing of information in these investigations.

The TIA Act can be found online at: http://www.comlaw.gov.au/Series/C2004A02124

CHAPTER 1 – TELECOMMUNICATIONS INTERCEPTION

Key requirements of the TIA Act

The primary function of the TIA Act is to protect the privacy of the communications of people who use the Australian telecommunications network. Under the TIA Act, communications cannot be intercepted while they are passing over the Australian telecommunications system, except as authorised in the circumstances set out in the TIA Act.

The TIA Act provides for several separate warrants for law enforcement agencies to access the content of a communication, including warrants relating to accessing real-time content (for example, a phone call while the parties are talking with each other) and a warrant to access 'stored communications' (including emails and text messages accessed from the telecommunications carrier after they have been sent).

This Chapter focuses on reporting about real-time interception warrants. Stored communications are the subject of Chapter 2. Information on Telecommunications Data is contained in Chapter 3.

During the reporting period interception warrants were only available to 17 Commonwealth and State and Territory agencies including:

- ACC, ACLEI and AFP
- State and Territory Police, and
- State anti-corruption agencies.

A full list of the agencies able to get interception warrants is at Appendix B.

An interception warrant may only be issued by an eligible Judge or a nominated Administrative Appeals Tribunal member. 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 Circuit Court (formerly the Federal Magistrates Court).

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

Before issuing an interception warrant the authority must be satisfied that:

- the agency is investigating a serious offence
- the gravity of the offence warrants the intrusion into privacy, and
- the interception is likely to support the investigation.

Serious offences generally carry a penalty of at least seven years' imprisonment. Serious offences for which interception can be obtained under the TIA Act include:

- murder
- kidnapping
- serious drug offences
- terrorism
- offences punishable by at least seven years imprisonment that involve conduct such as inflicting loss of life, serious personal injury, arson, drug trafficking, fraud, bribery and other serious conduct
- people smuggling, slavery, sexual servitude, deceptive recruiting and trafficking in persons
- sexual offences against children and offences involving child pornography
- money laundering, cybercrime and serious cartel offences
- offences involving organised crime.

The TIA Act requires this report to set out information in relation to agencies' use of powers under the Act. Use of Commonwealth, and State and Territory Department and Agency titles throughout this report are reflective of their titles during the reporting period. Where changes to titles have accorded during the reporting period, an explanatory note has been provided.

CASE STUDY: ADMINISTRATIVE APPEALS TRIBUNAL

The Administrative Appeals Tribunal's (AAT) Annual Report 2012-13 indicates that in a proportion of applications nominated AAT members issued a warrant or authorisation only after further information was provided at the request of the authorised member. A small number of warrant applications were refused, others granted only after conditions were imposed (including conditions in relation to privacy) and, in some instances, a warrant was issued for a lesser period of time than that sought by the law enforcement agency.

In recognition of the importance of the functions performed by authorised members, the Tribunal hosted a one-day seminar in October 2012 which included sessions dealing with the interception and surveillance application process, how the 'product' from the use of warrant/surveillance devices is used in the prosecution process and with what effect, and the legislative and community context in which telephone interception and other surveillance is taking place (including the role of Public Interest Monitors in Queensland and Victoria).

The Tribunal also updated its guidelines which contain practical information for authorised members about the exercise of these functions, and continued to liaise with the Attorney-General's Department about legislative and administrative reforms.

Key Legislative Developments 2012-2013

Amendments to meet Australia's Cybercrime Obligations

Council of Europe Convention on Cybercrime

On 1 March 2013, Australia formally joined 38 other nations as a party to the world's first leading international treaty on crimes committed via the internet. Cybercrime is a growing threat to Australian consumers, business and government; with the international nature of cybercrime no nation can effectively combat the problem alone. Australia's accession to the Convention, and the implementation of amendments to the TIA Act and other legislation to support this will lead to a strong ability for law enforcement agencies to combat this growing problem.

With the Convention now in effect, Australia's investigative agencies are able to use new powers introduced by the *Cybercrime Legislation Amendment Act 2012* to work with cybercrime investigators around the globe. The Act also amended computer offences in the *Criminal Code Act 1995* (Cth) to provide Commonwealth jurisdiction in relation to all computers and enabled the ability of Australian agencies to access and share information relating to international investigations. The Act also introduced new privacy protections, safeguards and reporting requirements for the exercise of new and existing powers.

The Cybercrime Convention can be found online at:
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

New authorities under the TIA Act

The *Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012* (the TI State Bodies Act) amended the TIA Act to add three new State government authorities as 'eligible authorities' under the TIA Act:

- the Independent Broad-based Anti-corruption Commission (Victoria) (the IBAC)
- the Victorian Inspectorate, and
- the Independent Commissioner Against Corruption (South Australia) (the SA ICAC)

Under the TIA Act eligible authorities can access information obtained under telecommunications interception warrants to support their investigations and prosecutions. The Commonwealth Attorney-General may declare an eligible authority to be an interception agency, subject to meeting requirements outlined in section 35 of the TIA Act. Once declared to be an interception agency, an agency can apply for interception warrants.[1]

The IBAC became an interception agency on 10 February 2013, when it replaced the Victorian Office of Police Integrity. Consistent with powers for other State oversight bodies, the Victorian Inspectorate was not declared an interception agency in its own right.

[1] TIA Act, s34. The State eligible authority must meet the requirements in s35 TIA Act to be declared an interception agency.

State legislation implementing the SA ICAC came into effect on 1 September 2013. The Declaration declaring the SA ICAC to be an interception agency came into force on that date. As this occurred after the current reporting year, SA ICAC has no interception warrants to report in this Annual Report.

The TI State Bodies Act also amended the TIA Act to introduce the Victorian Public Interest Monitor (PIM) into the Act. The amendments allow the Victorian PIM to:

- be advised at early the stages of the intention of a Victorian agency to apply for an interception warrant
- appear in applications for interception warrants by Victorian agencies, and
- provide submissions to issuing authorities.

Key Policy Developments 2012 - 2013

PJCIS Inquiry into Potential Reforms of National Security Legislation

On 4 May 2012 the former Government asked the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to consider possible reforms to security-related legislation. This included possible reforms to the interception regime aimed at ensuring the regime is keeping pace with rapid changes in the telecommunications environment.

The PJCIS accepted that new, emerging and future technologies impact on the ability of national security and law enforcement agencies to access communications to collect intelligence and to effectively detect and prosecute crimes. The pace of change in the last decade has meant the TIA Act has required frequent amendment. This has resulted in additional complexity in the Act and an increased number of exceptions to the general prohibition on interception.

Current powers, checks, balances and limitations on the operation of interception powers under the TIA Act were reviewed by the PJCIS to ensure that national security and law enforcement agencies can continue to perform their statutory roles while appropriately reflecting the privacy needs of contemporary communications users.

The Committee received submissions from government and national security agencies, law enforcement, community organisations and interested individuals.

The Committee tabled its Report in Parliament on 24 June 2013. Among its findings the Committee recommended:

- a comprehensive rewrite of the TIA Act to provide clear direction on the protections and powers available under the legislation;
- the introduction of a security framework for the telecommunications sector through amendments to the Telecommunications Act; and
- support for the majority of the proposed measures to modernise and improve laws relating to Australian intelligence agencies.

The PJCIS report can be found online at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm.

Further information about telecommunications, interception and privacy law can be found at:

- Attorney-General's Department: http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/default.aspx
- Department of Broadband, Communications and the Digital Economy: http://www.dbcde.gov.au/
- Commonwealth Ombudsman: http://www.ombudsman.gov.au/
- Office of the Australian Information Commissioner: http://oaic.gov.au/
- Telecommunications Industry Ombudsman: http://www.tio.com.au/
- Australian Communications and Media Authority: http://www.acma.gov.au/

Integrity testing

The *Law Enforcement Integrity Legislation Amendment Act 2012* amended the TIA Act and other relevant legislation to introduce targeted integrity testing for staff members of the AFP, ACC, and Customs suspected of corrupt conduct.

The amendments to the TIA essentially allow an interception agency to provide intercepted information to Customs, AFP, ACC or ACLEI for integrity testing purposes.

The amendments came into force on 13 December 2012.

Eligible Judges and nominated AAT members

An eligible Judge or nominated AAT member may issue a telecommunications interception warrant on application by an agency.

The next two tables set out information about the number of eligible Judges and nominated AAT members and the agencies to which they issued warrants.

Table 1: Availability of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT Members to issue telecommunications interception warrants – section 103(ab)

ISSUING AUTHORITY	NUMBER ELIGIBLE
FEDERAL COURT JUDGES	11
FAMILY COURT JUDGES	8
FEDERAL CIRCUIT COURT JUDGES	34
NOMINATED AAT MEMBERS	37

Table 2: Number of telecommunications interception warrants issued by Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT members - section 103(ab)

AGENCY	ISSUING AUTHORITY			
	FAMILY COURT JUDGES	FEDERAL COURT JUDGES	FEDERAL CIRCUIT COURT JUDGES	NOMINATED AAT MEMBERS
ACC	-	-	1	194
ACLEI	2	-	5	3
AFP	15	2	62	555
CCC WA	-	1	-	16
CMC QLD	-	-	2	24
ICAC	-	-	-	5
NSW CC	-	-	4	412
NSW POLICE	-	-	318	1,521
NT POLICE	-	-	48	22
PIC	-	-	-	70
QLD POLICE	-	-	157	135
SA POLICE	-	121	-	-
TAS POLICE	-	-	-	23
VIC POLICE	-	-	-	232
WA POLICE	158	-	-	118
TOTAL	**175**	**124**	**597**	**3,330**

Table 3: Applications for telecommunications interception warrants, telephone interception warrants, and renewal applications - sections 100(1)(a)-(c), and 100(2)(a)-(c)

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR WARRANTS		TELEPHONE APPLICATIONS FOR WARRANTS[2]		RENEWAL APPLICATIONS[3]	
		11/12	12/13	11/12	12/13	11/12	12/13
ACC	Made	143	195	-	-	34	36
	Refused/withdrawn	-	-	-	-	-	-
	Issued	143	195	-	-	34	36
ACLEI	Made	9	10	-	-	5	3
	Refused/withdrawn	-	-	-	-	-	-
	Issued	9	10	-	-	5	3
AFP	Made	541	640	1	-	135	149
	Refused/withdrawn	1	6	-	-	-	-
	Issued	540	634	1	-	135	149
CCC WA	Made	34	17	-	-	5	-
	Refused/withdrawn	2	-	-	-	-	-
	Issued	32	17	-	-	5	-
CMC QLD	Made	41	26	-	-	8	2
	Refused/withdrawn	-	-	-	-	-	-
	Issued	41	26	-	-	8	2
ICAC	Made	24	5	-	-	2	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	24	5	-	-	2	1
NSW CC	Made	348	417	-	-	75	105
	Refused/withdrawn	2	1	-	-	-	-
	Issued	346	416	-	-	75	105
NSW POLICE	Made	1,574	1,846	86	70	155	182
	Refused/withdrawn	4	7	-	1	-	-
	Issued	1,570	1,839	86	69	155	182
NT POLICE	Made	54	71	-	-	2	2
	Refused/withdrawn	-	-	-	-	-	-
	Issued	54	71	-	-	2	2
OPI	Made	12	-	-	-	5	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	12	-	-	-	5	-
PIC	Made	62	70	-	-	14	35
	Refused/withdrawn	-	-	-	-	-	-
	Issued	62	70	-	-	14	35
QLD POLICE	Made	218	292	-	-	21	36
	Refused/withdrawn	-	-	-	-	-	-
	Issued	218	292	-	-	21	36
SA POLICE	Made	102	126	-	-	10	6
	Refused/withdrawn	-	-	-	-	-	-
	Issued	102	126	-	-	10	6
TAS POLICE	Made	33	23	3	-	1	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	33	23	3	-	1	1
VIC POLICE	Made	293	233	16	19	26	21
	Refused/withdrawn	-	1	-	-	-	-
	Issued	293	232	16	19	26	21
WA POLICE	Made	276	276	5	1	15	28
	Refused/withdrawn	-	-	-	-	-	-
	Issued	276	276	5	1	15	28
TOTAL	**Made**	**3,764**	**4,247**	**111**	**90**	**513**	**607**
	Refused/withdrawn	**9**	**15**	**-**	**1**	**-**	**-**
	Issued	**3,755**	**4,232**	**111**	**89**	**513**	**607**

An issuing authority can in exceptional circumstances issue an interception warrant that authorises entry on premises to carry out telecommunications interception. An issuing authority

[2] Telephone applications are part of the total application of warrants.

[3] A renewal is a warrant that is issued for an existing warrant that is still in force

can only issue such a warrant if satisfied that it would be impracticable or inappropriate to intercept communications by less intrusive means.

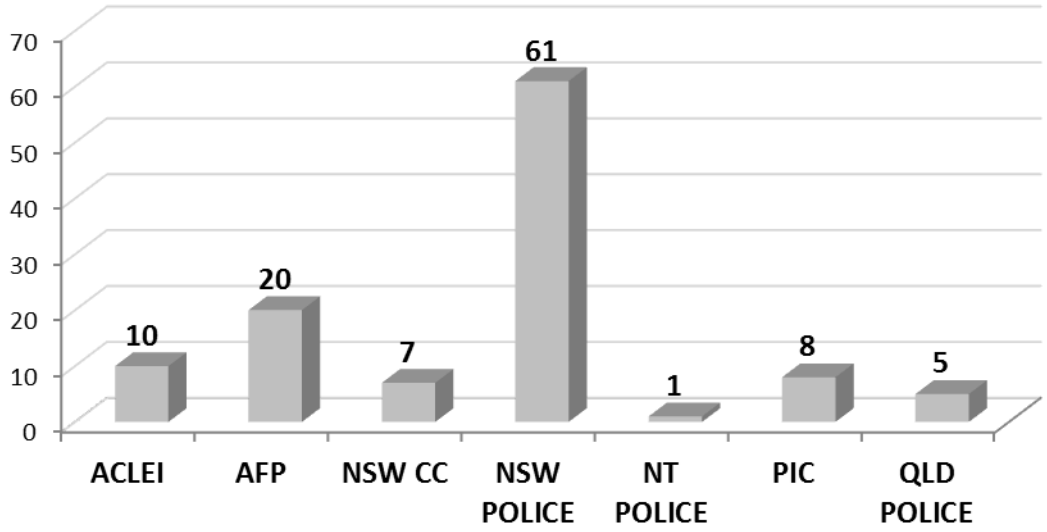
The following table sets out statistics about the use of entry on premises telecommunications interception warrants.

Table 4: Applications for telecommunications interception warrants authorising entry on premises - sections 100(1)(d), and 100(2)(d)

AGENCY	RELEVANT STATISTICS	WARRANTS AUTHORISING ENTRY ON PREMISES
AFP	Made Refused/withdrawn Issued	11 - 11
CCC WA	Made Refused/withdrawn Issued	1 - 1
NSW CC	Made Refused/withdrawn Issued	1 - 1
TOTAL	**Made** **Refused/withdrawn** **Issued**	**13** **-** **13**

An issuing authority can place conditions or restrictions on an interception warrant.
The following figure provides statistics on the use of warrants issued with conditions or restrictions.

Figure 1: Telecommunications interception warrants issued with specific conditions or restrictions - sections 100(1)(e), and 100(2)(e)



Named person warrants

An issuing authority is able to issue an interception warrant in relation to a named person.
A named person warrant can authorise the interception of telecommunications services (such as a landline or mobile service) and in certain circumstances telecommunications devices (such as a mobile handset).

Before issuing a named person warrant an issuing authority must take into account:

- how much the privacy of any person would be likely to be interfered with,
- the gravity of the offence,
- whether the interception will assist in the investigation, and
- the extent to which methods other than using a named person warrant are available to the agency.

The following two tables and figures provide information on the use of named person warrants.

Table 5: Original applications for named person warrants, telephone applications for named warrants, and renewal applications **-** sections 100(1)(ea) and 100(2)(ea)

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR NAMED PERSON WARRANTS		APPLICATIONS FOR TELEPHONE WARRANTS		APPLICATIONS FOR RENEWAL WARRANTS	
		11/12	12/13	11/12	12/13	11/12	12/13
ACC	Made	100	124	-	-	28	30
	Refused/withdrawn	-	-	-	-	-	-
	Issued	100	124	-	-	28	30
ACLEI	Made	3	3	-	-	2	2
	Refused/withdrawn	-	-	-	-	-	-
	Issued	3	3	-	-	2	2
AFP	Made	209	290	-	-	61	96
	Refused/withdrawn	1	5	-	-	-	-
	Issued	208	285	-	-	61	96
CCC WA	Made	-	3	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	-	3	-	-	-	-
CMC QLD	Made	8	9	-	-	1	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	8	9	-	-	1	1
NSW CC	Made	100	96	-	-	28	19
	Refused/withdrawn	-	-	-	-	-	-
	Issued	100	96	-	-	28	19
NSW POLICE	Made	97	132	3	-	18	27
	Refused/withdrawn	-	-	-	-	-	-
	Issued	97	132	3	-	18	27
NT POLICE	Made	1	2	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	1	2	-	-	-	-
OPI	Made	3	-	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	3	-	-	-	-	-
PIC	Made	2	3	-	-	1	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	2	3	-	-	1	1
QLD POLICE	Made	30	42	-	-	4	7
	Refused/withdrawn	-	-	-	-	-	-
	Issued	30	42	-	-	4	7
SA POLICE	Made	22	32	-	-	1	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	22	32	-	-	1	1
TAS POLICE	Made	2	1	-	-	-	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	2	1	-	-	-	1
VIC POLICE	Made	71	69	-	1	12	8
	Refused/withdrawn	-	-	-	-	-	-
	Issued	71	69	-	1	12	8
WA POLICE	Made	54	94	1	-	4	15
	Refused/withdrawn	-	-	-	-	-	-
	Issued	54	94	1	-	4	15
TOTAL	**Made**	**702**	**900**	**4**	**1**	**160**	**208**
	Refused/withdrawn	**1**	**5**	**-**	**-**	**-**	**-**
	Issued	**701**	**895**	**4**	**1**	**160**	**208**

Figure 2: Named person warrants issued with conditions or restrictions - sections 100(1)(ea) and 100(2)(ea)

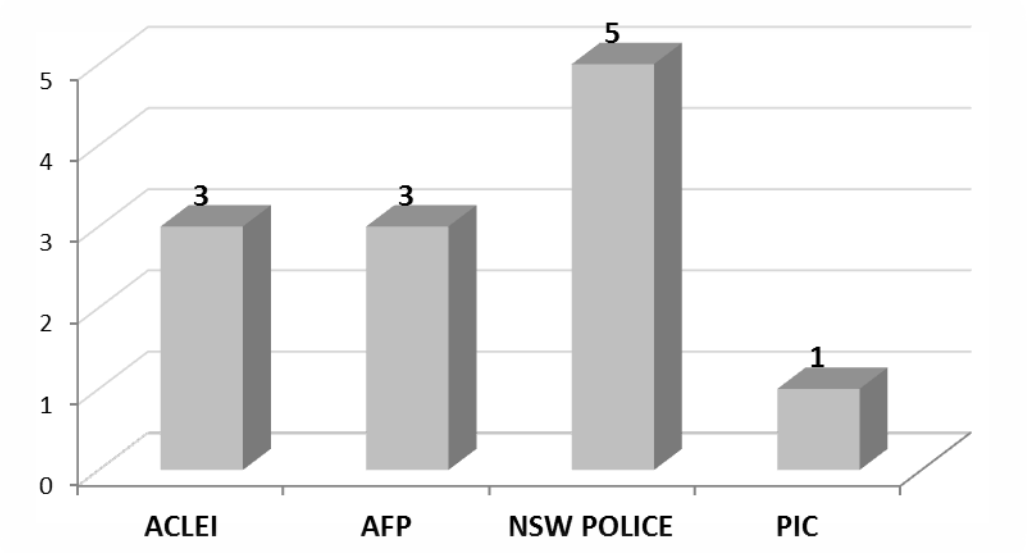


Table 6: Number of services intercepted under named person warrants - sections 100(1)(eb), and 100(2)(eb)

AGENCY	RELEVANT STATISTICS			
	1 service only	2 – 5 services	6 – 10 services	10+ services
ACC	31	63	20	6
ACLEI	-	3	-	-
AFP	61	133	27	7
CCC WA	-	1	1	1
CMC QLD	1	8	-	-
NSW CC	34	57	2	3
NSW POLICE	31	64	11	-
NT POLICE	-	1	1	-
PIC	-	-	-	3
QLD POLICE	8	29	3	2
SA POLICE	5	22	7	-
TAS POLICE	-	-	-	1
VIC POLICE	11	54	4	-
WA POLICE	20	66	8	-
TOTAL	**202**	**501**	**84**	**23**

Figure 3: Total number of services intercepted under service based named person warrants - sections 100(1)(ec), and 100(2)(ec)

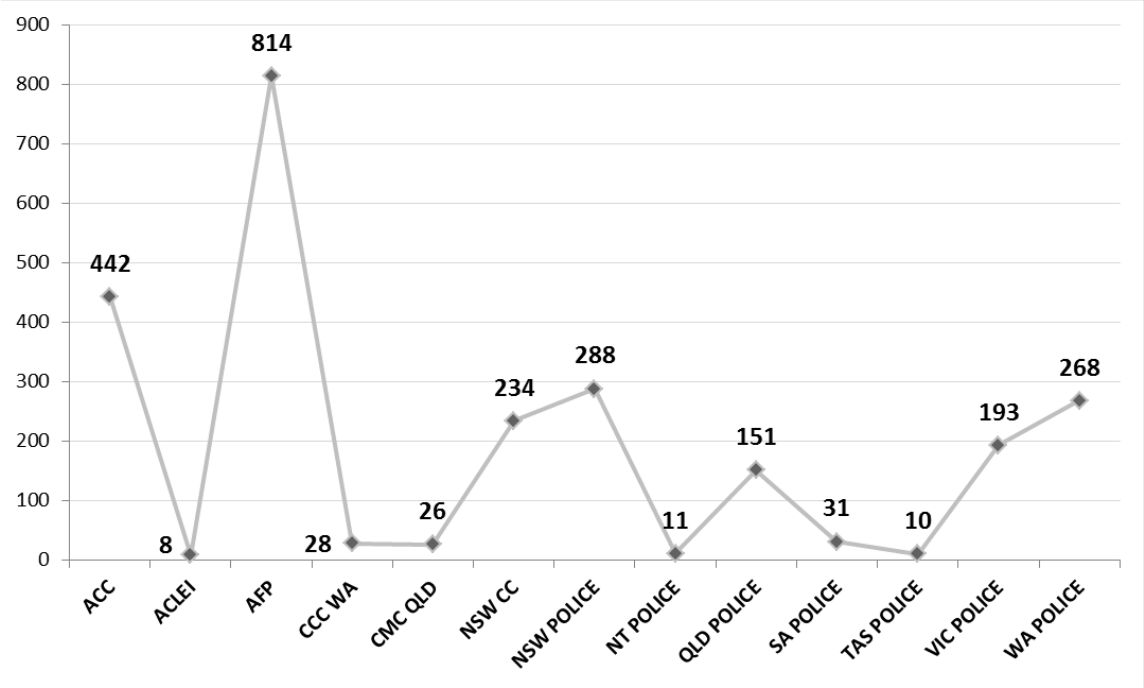


Table 7: Total number of services and devices intercepted under device based named person warrants - sections 100(1)(ec) and 100(2)(ec)

AGENCY	SERVICES	DEVICES
	12/13	12/13
ACC	-	17
AFP	-	66
NSW CC	-	2
NSW POLICE	32	26
TOTAL	32	111

B-Party warrants

An issuing authority can issue an interception warrant in which an interception agency intercepts the communications of a person who is communicating with a person suspected of involvement in a serious offence. This is known as a B-Party warrant.

A B-Party warrant can only be issued if there are no other practicable methods of identifying the telecommunications services of the person involved in the offences or interception of communications from that person's telecommunications services would not otherwise be possible.

The following two tables provide information about the use of B-Party warrants.

Table 8: Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications **-** sections 100(1)(ed), and 100(1)(ed)

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR B-PARTY WARRANTS		TELEPHONE APPLICATIONS FOR B-PARTY WARRANTS		RENEWAL APPLICATIONS FOR B-PARTY WARRANTS	
		11/12	12/13	11/12	12/13	11/12	12/13
ACC	Made	1	1	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	1	1	-	-	-	-
ACLEI	Made	1	2	-	-	-	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	1	2	-	-	-	1
AFP	Made	47	34	1	-	26	21
	Refused/withdrawn	-	-	-	-	-	-
	Issued	47	34	1	-	26	21
CCC WA	Made	-	3	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	-	3	-	-	-	-
NSW CC	Made	19	1	-	-	4	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	19	1	-	-	4	-
NSW POLICE	Made	66	71	13	20	2	4
	Refused/withdrawn	-	1	-	1	-	-
	Issued	66	70	13	19	2	4
OPI	Made	1	-	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	1	-	-	-	-	-
QLD POLICE	Made	-	6	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	-	6	-	-	-	-
VIC POLICE	Made	14	2	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	14	2	-	-	-	-
WA POLICE	Made	-	1	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	-	1	-	-	-	-
TOTAL	**Made**	**149**	**121**	**14**	**20**	**32**	**26**
	Refused/withdrawn	**-**	**1**	**-**	**1**	**-**	**-**
	Issued	**149**	**120**	**14**	**19**	**32**	**26**

Table 9: B-Party warrants issued with conditions or restrictions **-** sections 100(1)(ed) and 100(2)(ed)

AGENCY	APPLICATIONS FOR B-PARTY WARRANTS	
	11/12	12/13
ACLEI	1	2
AFP	-	3
NSW POLICE	2	1
TOTAL	**3**	**6**

Serious offences

The TIA Act gives law enforcement agencies across Australia valuable tools for detecting, investigating and prosecuting serious crime.

The ACC, in its 2013 report *Organised Crime in Australia*, assessed the overall threat to Australia from organised crime as high.[4] Organised crime such as identity crime, money laundering, fraud, cybercrime, drug trafficking, people smuggling and a range of other crimes is estimated to cost Australia $15 billion per year.[5]

The statistics provided in the next table demonstrate that telecommunications interception has been significant in investigating serious crimes. For example, in 2012-13 interception warrants listed the following serious offences:

- 388 for murder
- 274 for organised crime, and
- 2,063 for serious drug trafficking

The below table provides information on the number of serious offences investigated using telecommunications interception warrants. Further information on serious offences described under the TIA Act is provided at Appendix D.

[4] ACC, *Organised Crime in Australia 2013*, http://www.crimecommission.gov.au/sites/default/files/files/ACC%20OCA%202013.pdf, p. 12

[5] ACC, *Organised Crime in Australia 2013*, p. 6.

Table 10: Categories of serious offences specified in telecommunications interception warrants - sections 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

CATEGORIES OF OFFENCES	ACC	ACLEI	AFP	CCC WA	CMC QLD	ICAC	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
ACC SPECIAL INVESTIGATIONS	183	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**184**
ADMINISTRATION OF JUSTICE	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
ASSISTING A PERSON TO ESCAPE OR DISPOSE OF PROCEEDS	-	-	-	-	-	-	26	18	-	-	5	1	-	-	-	**50**
BRIBERY OR CORRUPTION; OFFENCES AGAINST SS 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 OF THE CRIMINAL CODE	-	8	31	15	1	5	-	7	-	38	1	-	-	15	-	**121**
CARTEL OFFENCES	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
CHILD PORNOGRAPHY OFFENCES	-	-	5	-	-	-	-	3	-	-	-	-	-	-	1	**9**
CONSPIRE / AID / ABET SERIOUS OFFENCE	6	-	-	-	-	-	95	46	10	-	-	1	-	4	-	**162**
CYBERCRIME OFFENCES	-	-	17	2	-	-	-	-	-	-	-	-	-	-	-	**19**
KIDNAPPING	-	-	1	-	-	-	5	17	1	-	-	-	-	14	1	**39**
LOSS OF LIFE OR PERSONAL INJURY	-	-	58	-	-	-	72	533	2	-	24	4	3	73	22	**791**
MONEY LAUNDERING	1		104	-	-	-	10	17	-	6		6		2	-	**146**
MURDER	-	-	2	-	-	-	44	177	5	-	46	14	4	41	55	**388**
ORGANISED OFFENCES AND/OR CRIMINAL ORGANISATIONS	-	-	33	-	-	-	12	205	-	-	1	-	-	2	21	**274**
PEOPLE SMUGGLING AND RELATED	-	-	22	-	-	-	-	-	-	2	-	-	-	-	-	**24**
SERIOUS DAMAGE TO PROPERTY AND/OR SERIOUS ARSON	-	-	-	-	-	-	-	62	1	-	3	6	-	3	13	**88**
SERIOUS DRUG OFFENCES AND/OR TRAFFICKING	4	2	500	-	24	-	220	661	52	7	211	129	16	77	160	**2,063**
SERIOUS FRAUD AND/OR REVENUE LOSS	-	-	16	-	1	-	1	54	-	19	1	-	-	-	3	**95**
TELECOMMUNICATIONS OFFENCES	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
TERRORISM OFFENCES	-	-	76	-	-	-	-	39	-	-	-	-	-	1	-	**116**
TOTAL	**194**	**10**	**865**	**17**	**26**	**5**	**485**	**1,839**	**71**	**72**	**292**	**161**	**23**	**232**	**276**	**4,569**

Duration of warrants

Under the TIA Act, a telecommunications interception warrant other than a B-Party warrant can be in force for up to 90 days. Under section 57, the chief executive of an agency may revoke a warrant at any time and must revoke a warrant if they are satisfied that the conditions for issuing the warrant no longer exist. The next table sets out the average length of time that interception warrants, including renewals but not including B-Party warrants, were issued for and the average length of time for which they were in force.

Table 11: Duration of original and renewal telecommunications interception warrants - sections 101(1)(a)-(d) and 101(2)(a)-(d)

AGENCY	DURATION OF ORIGINAL TELECOMMUNICATIONS INTERCEPTION WARRANTS		DURATION OF RENEWAL OF TELECOMMUNICATIONS INTERCEPTION WARRANTS	
	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)
ACC	88	51	90	66
ACLEI	79	67	75	75
AFP	68	52	82	71
CCC WA	71	59	-	-
CMC QLD	80	64	90	22
ICAC	90	81	45	45
NSW CC	84	35	84	80
NSW POLICE	73	51	77	67
NT POLICE	79	40	90	5
PIC	76	71	88	87
QLD POLICE	60	55	61	51
SA POLICE	78	66	89	-
TAS POLICE	71	42	60	-[6]
VIC POLICE	57	49	67	64
WA POLICE	77	53	90	67
AVERAGE	**75**	**56**	**78**	**58**

[6] Tasmania Police have advised that a renewal warrant spaned multiple reporting years. As such the average period in force will be reported in the follow reporting period.

Under the TIA Act, a B-Party warrant can be in force for up to 45 days. The following table sets out the average length of time for which B-Party warrants and renewals of those warrants were issued and the average length of time in force.

Table 12: Duration of original and renewal B-Party warrants - sections 101(1)(da) and 101(2)(da)

AGENCY	DURATION OF ORIGINAL TELECOMMUNICATIONS B-PARTY WARRANTS		DURATION OF RENEWAL OF TELECOMMUNICATIONS B-PARTY WARRANTS	
	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)	AVERAGE PERIOD SPECIFIED IN WARRANTS (DAYS)	AVERAGE PERIOD WARRANTS IN FORCE (DAYS)
ACC	45	37	-	-
ACLEI	45	-	45	45
AFP	39	26	45	39
CCC WA	45	45	-	-
NSW CC	20	8	-	-
NSW POLICE	32	22	37	34
OPI	-	-	-	-
QLD POLICE	8	8	-	-
VIC POLICE	45	45	-	-
WA POLICE	14	14	-	-
AVERAGE	**32**	**26**	**42**	**39**

A final renewal means a telecommunications interception warrant that is the last renewal of an original warrant. It is recorded as the number of days after the issue of the original warrant that the last renewal of the warrant ceases to be in force.

The categories of final renewals are:

- 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.

The following table provides information on the number of final renewals used by the agencies.

Table 13: Number of final renewals **-** sections 101(1)(e) and 101(2)(e)

AGENCY	90 DAYS	150 DAYS	180 DAYS
ACC	23	7	6
ACLEI	-	-	1
AFP	22	4	28
CMC QLD	1	1	-
ICAC	1	-	-
NSW CC	5	19	24
NSW POLICE	72	25	14
PIC	-	28	-
QLD POLICE	14	12	1
SA POLICE	2	-	-
VIC POLICE	8	-	-
WA POLICE	9	17	1
TOTAL	**157**	**113**	**75**

Effectiveness of telecommunications interception

Telecommunications interception is a powerful tool for law enforcement and security agencies to effectively assist with the investigation and prosecution of serious and organised crime, serious offences and serious contraventions and reduce the risk of threats to national security.

The effectiveness of telecommunications interception is set out in this Annual Report. The Annual Report shows there were 2951 arrests, 6746 prosecutions and 2700 convictions based on lawfully intercepted material.

Telecommunications interception, access to stored communications and access to telecommunications data assists agencies in a number of ways, including:

- Building a picture of a suspect and a network of contacts
- Providing evidence in criminal prosecutions
- Deterring criminals from using telecommunications services to plan or commit crimes
- Protecting the public, including people in emergency situations and victims or potential victims of crime
- Exculpating innocent persons or excluding persons from an investigation
- For telecommunications data, providing information that enables lawful interception or access of content.

CASE STUDY: AUSTRALIAN FEDERAL POLICE

The AFP carries out long-term investigations into the activities of global money laundering syndicates that operate across Europe, the Americas, Asia, Africa, and Australia on behalf of many of the world's largest organised crime groups including South American cocaine cartels, Asian Triad organisations, the Italian Mafia and Balkan organised crime groups.

AFP money laundering investigations are aimed at identifying and disrupting the organised crime groups using money laundering services in Australia.

The AFP uses the powers under the TIA Act to assist in drawing links between suspects and their activities. The AFP notes that people involved in crimes such as money laundering employ a number of tactics in their attempt to avoid detection, for example, using multiple mobiles phones and SIM cards, and employing new internet based communications.

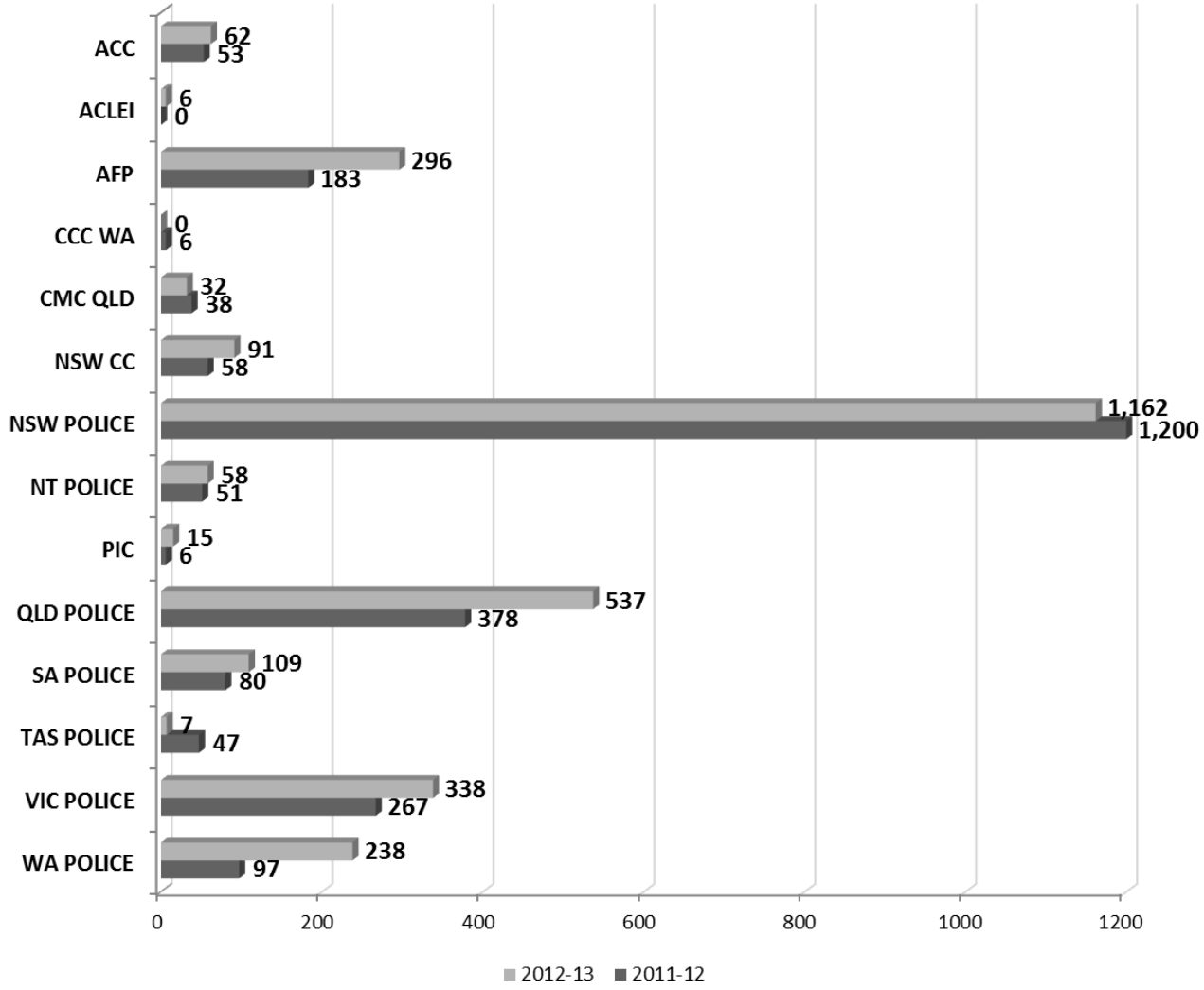
The value of funds exchanging hands globally is enormous. In an 18 month period, one money laundering investigation alone has seen the AFP:

- Arrest 35 offenders
- Seize 421 kilograms of drugs, and
- Seize over $8,000,000 in cash

In this environment the TIA Act is essential for the AFP to ensure it can conduct lawful interception and successfully stop these crimes.

The following Figure shows the number of arrests on the basis of lawfully intercepted information by all of the law enforcement agencies over the past two years.

Figure 4: Arrests on the basis of lawfully intercepted information **-** sections 102(1)(a) and 102(2)(a)



The following two tables show the number of prosecutions and convictions in which lawfully intercepted information was given in evidence by each of the law enforcement agencies. More information outlining types of offences listed in these tables is provided at Appendix D.

CATEGORIES OF OFFENCES	ACC	ACLEI	AFP	CCC WA	CMC QLD	ICAC	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
ACC SPECIAL INVESTIGATIONS	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ADMINISTRATION OF JUSTICE	-						4									4
ASSISTING A PERSON TO ESCAPE OR DISPOSE OF PROCEEDS	-	-	-	-	-	-	1	-	-	-	4	-	-	-	-	5
BRIBERY OR CORRUPTION; OFFENCES AGAINST SS131.1, 135.1, 142.1, 142.2, 148.2, 268.112 OF THE CRIMINAL CODE	-	2	26	8	-	2	24	-	2	-	-	-	-	3	-	67
CARTEL OFFENCES	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-
CHILD PORNOGRAPHY OFFENCES	-	-	7	-	-	-	-	18	-	-	-	-	-	-	-	25
CONSPIRE / AID / ABET SERIOUS OFFENCE	-	-	-	-	-	-	2	80	-	-	-	-	-	5	-	87
CYBERCRIME OFFENCES	-	-	25	-	-	-	-	-	-	-	-	-	-	1	-	26
KIDNAPPING	-	-	-	-	-	-	-	47	-	-	-	-	-	11	-	58
LOSS OF LIFE OR PERSONAL INJURY	-	-	-	-	-	-	-	867	-	-	5	3	-	162	12	1,049
MONEY LAUNDERING	2	-	36	-	-	-	14	43		-			-	26	-	121
MURDER	-	-	-	-	-	-	19	52	2	-	3	3	-	11	7	97
ORGANISED OFFENCES AND/OR CRIMINAL ORGANISATIONS	-	-	-	-	-	-	47	-	-	-	2	-	-	-	4	53
PEOPLE SMUGGLING AND RELATED	-	-	5	-	-	-	-	616	-	-	-	-	-	-	-	621
SERIOUS DAMAGE TO PROPERTY AND/OR SERIOUS ARSON	-	-	-	-	-	-	1	26	1	-	-	-	-	-	6	34
SERIOUS DRUG OFFENCES AND/OR TRAFFICKING	10	2	311	-	12	-	157	2,090	53		148	77	1	202	443	3,506
SERIOUS FRAUD AND/OR REVENUE LOSS	-	-	-	-	-	-	-	118	-	-	3	-	-	3	4	128
TELECOMMUNICATIONS OFFENCES	-	-	6	-	-	-	-	6	-	-	-	-	-	-	-	12
TERRORISM OFFENCES	-	-	1	-	-	-	4	-	-	-	-	-	-	-	-	5
OTHER SERIOUS OFFENCES	1	1	84	4	10	1	-	385	-	1	115		1	245	-	848
TOTAL	**13**	**5**	**501**	**12**	**22**	**3**	**273**	**4,348**	**58**	**1**	**280**	**83**	**2**	**669**	**476**	**6,746**

Table 14: Prosecutions in which lawfully intercepted information was given in evidence

CATEGORIES OF OFFENCES	ACC	ACLEI	AFP	CCC WA	CMC QLD	ICAC	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
ACC SPECIAL INVESTIGATIONS	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ADMINISTRATION OF JUSTICE	-	-	-	-	-	-	4	-	-	1	-	-	-	-	-	5
ASSISTING A PERSON TO ESCAPE OR DISPOSE OF PROCEEDS	-		-	-	-	-	2	-	-	-	4	-	-	-	-	6
BRIBERY OR CORRUPTION; OFFENCES AGAINST SS131.1, 135.1, 142.1, 142.2. 148.2, 268.112 OF THE CRIMINAL CODE	-	2	-	8	-	1	5	57	-	-	-	-	-	3	-	76
CARTEL OFFENCES	-	-	-	-	-	-	-	-	-	-	-	-	-		-	-
CHILD PORNOGRAPHY OFFENCES	-	-	6	-	-	-	-	5	-	-	-	-	-		-	11
CONSPIRE / AID / ABET SERIOUS OFFENCE	-	-	-	-	-	-	-	31	-	-	-	-	-	5	-	36
CYBERCRIME OFFENCES	-	-	21	-	-	-	-	-	-	-	-	-	-	1	-	22
KIDNAPPING	-	-	-	-	-	-	-	42	-	-	-	-	-	11	-	53
LOSS OF LIFE OR PERSONAL INJURY	-	-	-	-	-	-	-	162	-	-	5	-	-	162	7	336
MONEY LAUNDERING	-	-	7	-	-	-	9	-	-	-	-	-	-	25	-	41
MURDER	-	-	-	-	-	-	-	28	-	-	-	-	-	8	6	42
ORGANISED OFFENCES AND/OR CRIMINAL ORGANISATIONS	-	-	-	-	-	-	29	117	-	-	2	-	-	-	2	150
PEOPLE SMUGGLING AND RELATED	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	5
SERIOUS DAMAGE TO PROPERTY AND/OR SERIOUS ARSON	-	-	-	-	-	-	1	12	-	-	-	-	-	-	4	17
SERIOUS DRUG OFFENCES AND/OR TRAFFICKING	1	2	110	-	1	-	97	500	8	-	143	14	1	192	297	1,366
SERIOUS FRAUD AND/OR REVENUE LOSS	-	-	-	-	-	-	10	7	-	-	3	-	-	3	2	25
TELECOMMUNICATIONS OFFENCES	-	-	5	-	-	-	-	2	-	-	-	-	-	-	-	7
TERRORISM OFFENCES	-	-		-	-	-	4	-	-	-	-	-	-	-	-	4
OTHER SERIOUS OFFENCES	1	1	46	3		1		91	-	1	109	-	1	244	-	498
TOTAL	**2**	**5**	**200**	**11**	**1**	**2**	**161**	**1,054**	**8**	**2**	**266**	**14**	**2**	**654**	**318**	**2,700**

Table 15: Convictions in which lawfully intercepted information was given in evidence

CASE STUDY: SOUTH AUSTRALIA POLICE

During the reporting period the South Australia Police secured a conviction against an Adelaide man for the large scale manufacturing of methamphetamine. The man was arrested in March 2010 when police raided a warehouse in Adelaide's north where the man was preparing to sell the drugs in a multi-million dollar deal.

At the time of the arrest, one Forensic Chemist called the warehouse a 'Super Lab', with the ability to produce multiple large quantities of methamphetamines. During the raid police located 8 kgs of pseudoephedrine and close to 100 grams of high grade methamphetamines. Further investigation also showed that the man, who was on pre-release home detention for other drug offences, was intricately involved in the operation which was producing the drugs for a number of organised crime groups in South Australia.

South Australia Police have advised that the use of evidence obtained through the interception of telecommunications under the TIA Act was crucial in obtaining the conviction. The man was found guilty of *Manufacturing a Large Commercial Quantity of a Controlled Drug* and received a sentence of 17 years' jail.

Eligible Warrants

Under the TIA Act the annual 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 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.

Table 16 indicates what percentage of each agency's total warrants in force during the reporting period were eligible warrants.

Table 16: Percentage of eligible warrants - sections 102(3) and 102(4)

AGENCY	TOTAL NUMBER OF WARRANTS	NUMBER OF ELIGIBLE WARRANTS	%
ACC	180	55	31
ACLEI	13	3	23
AFP	712	534	75
CCC WA	17	9	53
CMC QLD	27	22	81
ICAC	7	4	57
NSW CC	489	368	75
NSW POLICE	2,069	1,584	77
NT POLICE	61	38	62
PIC	79	36	46
QLD POLICE	334	314	94
SA POLICE	126	126	100
TAS POLICE	23	16	70
VIC POLICE	271	142	52
WA POLICE	317	138	44
TOTAL	**4,725**	**3,389**	**72**

Interception without a warrant

The TIA Act enables agencies to undertake interception without a warrant in limited prescribed circumstances, such as where there is a need to intercept communications due to a serious threat to life or the possibility of serious injury. The following table demonstrates the occasions on which such interception has occurred during the reporting period.

Table 17: Interception without a warrant – section 102A

AGENCY	CONSENT WHERE PERSON LIKELY TO RECEIVE COMMUNICATION FROM PERSON WHO HAS:			
	COMMITEED AN ACT THAT HAS OR MAY RESULT IN LOSS OF LIFE OR SERIOUS PERSONAL INJURY	THREATENED TO KILL OR SERIOUSLY INJURE ANOTHER	THREATENED TO CAUSE SERIOUS DAMAGE TO PROPERTY	THREATENED TO TAKE, ENDANGER, OR CREATE SERIOUS THREAT TO OWN LIFE/SAFETY
AFP	-	1	-	-
TOTAL	**-**	**1**	**-**	**-**

No information on mutual assistance interception requests, section 102B, was provided by agencies for the reporting period.

Number of interceptions carried out on behalf of other agencies

The TIA Act supports interception agencies ability to cooperate and work collaboratively with by enabling one interception agency to carry out interception on behalf of other agencies. The main circumstance in which this type of function will occur is where a larger agency assists a smaller agency to intercept to reduce the costs of the smaller agency.

Table 18: Number of interceptions carried out on behalf of other agencies – section 103(ac)

INTERCEPTION CARRIED OUT BY:	INTERCEPTION CARRIED OUT ON BEHALF OF:	NUMBER OF INTERCEPTIONS:
ACC	**ACLEI**	2
ACC	**CMC QLD**	42
AFP	**ACLEI**	8
NSW CC	**NSW POLICE**	2
VIC POLICE	**TAS POLICE**	144
TOTAL		**198**

Telecommunications interception expenditure

The below figures and table show the *Total* and *Average* information on expenditure by agencies related to telecommunications interception.

Figure 5: Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants – section 103(a)

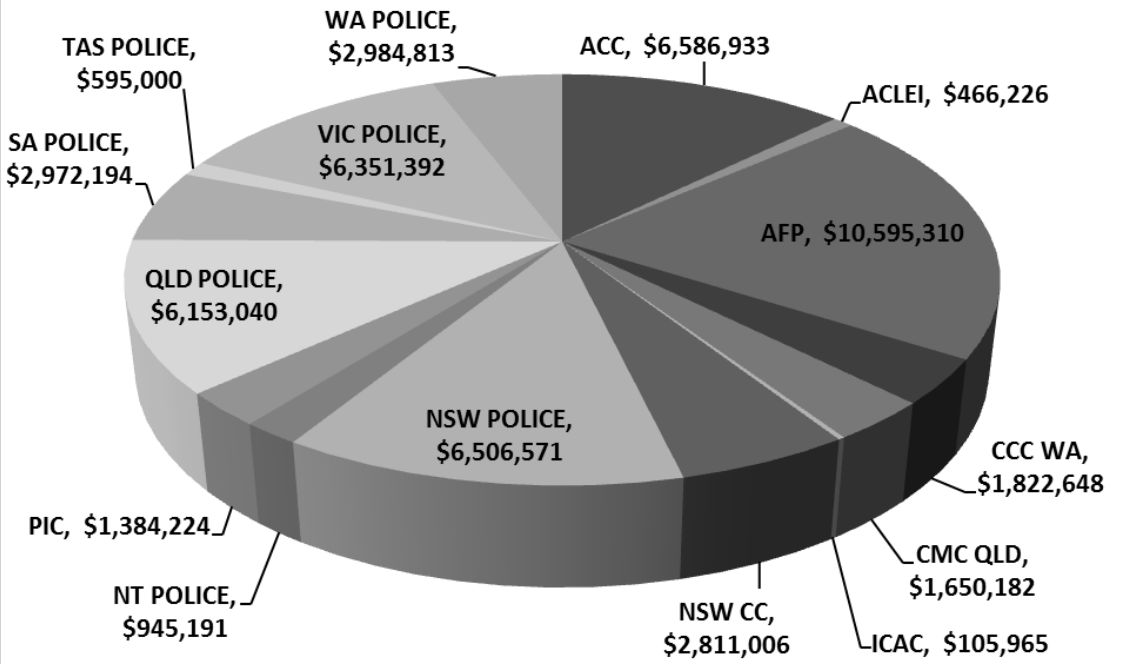


Table 19: Average expenditure per telecommunications interception warrant – section 103(aa)

AGENCY	Amount ($)
ACC	33,779
ACLEI	46,623
AFP	16,712
CCC WA	107,215
CMC QLD	63,469
ICAC	21,193
NSW CC	6,757
NSW POLICE	3,538
NT POLICE	13,313
PIC	19,775
QLD POLICE	21,072
SA POLICE	23,589
TAS POLICE	25,870
VIC POLICE	27,377
WA POLICE	10,815

Table 20: Recurrent costs of interceptions per agency

AGENCY	SALARIES	ADMINISTRATIVE SUPPORT	CAPITAL EXPENDITURE	INTERCEPTION COSTS	TOTAL ($)
ACC	5,471,862	62,325	-	1,052,746	**6,586,933**
ACLEI	360,965	55,271	14,000	35,990	**466,226**
AFP	6,916,948	135,827	2,765,681	776,854	**10,595,310**
CCC WA	1,186,598	12,021	546,984	77,045	**1,822,648**
CMC QLD	955,879	250,535	6,396	437,372	**1,650,182**
ICAC	44,051	3,340	54,516	4,058	**105,965**
NSW CC	1,816,489	95,304	41,247	857,966	**2,811,006**
NSW POLICE	4,446,221	730,213	-	1,330,137	**6,506,571**
NT POLICE	657,929	-	166,000	121,262	**945,191**
PIC	1,122,939	-	-	261,285	**1,384,224**
QLD POLICE	3,603,429	147,561	1,415,796	986,252	**6,153,038**
SA POLICE	2,087,951	255,534	87,555	103,447	**2,534,487**
TAS POLICE	465,000	-	50,000	80,000	**595,000**
VIC POLICE	5,217,640	275,188	57,571	800,993	**6,351,392**
WA POLICE	2,651,816	108,063	-	224,934	**2,984,813**

Emergency service facilities

The following table sets out the number of places that have been declared under the TIA Act to be emergency service facilities.

Table 21: 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	6	-	10
WESTERN AUSTRALIA	1	-	1	2	3
SOUTH AUSTRALIA	1	2	1	-	1
TASMANIA	1	2	1	-	2
AUSTRALIAN CAPITAL TERRITORY	3	-	-	-	3
NORTHERN TERRITORY	2	-	1	1	3
TOTAL	**55**	**114**	**46**	**6**	**47**

Safeguards, controls and reporting requirements

The TIA Act contains a number of safeguards, controls and reporting requirements in relation to interception, access to stored communications and disclosure of telecommunications data including:

- The heads of Interception agencies provide the Secretary of the Attorney-General's Department (AGD) a copy of each telecommunications interception warrant;
- Interception agencies report to the Attorney-General, within three months of a warrant ceasing to be in force, detailing the use made of information obtained by the interception;
- The Secretary of the AGD maintains a General Register detailing the particulars of all telecommunications interception warrants. The Secretary of the AGD must provide the General Register to the Attorney-General for inspection every three months;
- The Secretary of the AGD also maintains a Special Register recording the details of telecommunications interception warrants that do not lead to a prosecution within three months of the warrant expiring. The Special Register is also given to the Attorney-General to inspect; and
- The managing director of a telecommunications carrier reports to the Attorney-General within three months of the warrant ceasing to be in force, detailing the acts done by the carrier's employees to effect and discontinue interception.

Law enforcement agencies' use of interception powers under the TIA Act is independently oversighted by the Commonwealth Ombudsman and equivalent State bodies.

At least twice a year the Commonwealth Ombudsman must inspect the records kept by the ACC, ACLEI and the AFP relating to interceptions and the use, dissemination and destruction of intercepted information.

The Commonwealth Ombudsman is required under the TIA Act to report to the Attorney-General about these inspections, including information about any deficiencies identified and remedial action.

State and Territory legislation imposes similar requirements on State and Territory interception agencies regarding their use of interception powers.

While the Commonwealth Ombudsman is responsible for inspecting the records of the ACC, ACLEI and the AFP in relation to interception, the relevant State or Territory Ombudsman generally undertakes this function for State and Territory agencies. 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.

The Commonwealth Ombudsman must also conduct regular inspections of records in relation to access by enforcement agencies (including both Commonwealth and State agencies) to stored communications and report to the Attorney-General on the results of those inspections.

Commonwealth Ombudsman – Inspection of telecommunications interception records

During the reporting period the Commonwealth Ombudsman conducted six inspections of the interception records of the ACC, ACLEI and the AFP (two inspections for each agency).

The Ombudsman found that there continued to be a high level of compliance with the telecommunications interception provisions of the TIA Act and that agencies were cooperative with inspections and receptive to suggestions for improvement.

Overall, the Ombudsman considered that agencies demonstrated a good understanding of the Act's requirements, with all agencies found to be compliant with the majority of the Ombudsman's inspection criteria. The Ombudsman's inspection criteria (see Figures 6 and 7) are:

- Were restricted records properly destroyed (s79)?
- Were the requisite documents in connection with the issue of warrants kept (s80)?
- Were warrants in the correct form (s49)?
- Were the requisite records in connection with interceptions kept (s81)?
- Were interceptions conducted in accordance with the warrants (s7) and was any unlawfully intercepted information properly dealt with (s63)?

Commonwealth Ombudsman's Summary of Findings

Table 22: Summary of findings from the two inspections conducted at each agency during the reporting period

CRITERIA	ACC	ACLEI	AFP
Ss7 and 63 – Interceptions conducted in accordance with warrant, any unlawful information properly dealt with	Nothing to indicate otherwise, with exceptions noted[7]	Nothing to indicate otherwise	Nothing to indicate otherwise
S49 – Warrants in the correct form	Compliant except for issues noted[8]	Compliant	Compliant except for issues noted[9]
S79 – Restricted records properly destroyed	Compliant	Not assessed as no records destroyed	Compliant
S80 – Requisite records kept in connection with issue of warrant	Compliant	Compliant	Compliant
S81 – Requisite records kept in connection with interceptions	Compliant	Compliant except for issues noted[10]	Compliant

[7] The Ombudsman was unable to confirm whether internet data was intercepted in accordance with two warrants. Also, a carrier provided the ACC with stored communications that did not appear to be sent to or by the telecommunications service identified on the warrant.

[8] The ACC self-disclosed that three warrants had minor errors and one warrant stated the incorrect expiry date, which was voluntarily revoked.

[9] One record was not compliant with s49 and two warrants listed different offences from the affidavits.

[10] Some inaccuracies were noted in reports to the Minister. ACLEI advised that it sent amended reports after the Ombudsman identified this issue.

The further information on the Commonwealth Ombudsman's telecommunications interception inspection criteria is outlined in Figure 6 and 7 below.

Commonwealth Ombudsman's Findings for Individual Agency

ACC

No recommendations were made as a result of either of the two inspections of the ACC.

The Ombudsman could not determine whether internet data was intercepted in accordance with two warrants. This was due to the internet service provider not providing the ACC with the information necessary to make this assessment. The Ombudsman noted that the ACC is working with this internet service provider to address the issue.

The Ombudsman also noted that a carrier had provided the ACC with stored communications that did not appear to be sent to or from the telecommunications service related to the warrant. The ACC quarantined the stored communications once the Ombudsman identified the issue.

The Ombudsman acknowledged the ACC's frank disclosure of issues relevant to the inspection criteria and the provision of information regarding the ACC's processes and how it applies the TIA Act.

ACLEI

No recommendations were made as a result of either of the two inspections of ACLEI.

Section 49(2) of the Act enables a warrant to specify conditions or restrictions relating to interceptions undertaken under the warrant. The Ombudsman noted that it was unable to determine compliance with conditions specified in warrants. This was due to the Ombudsman's practice not to look at the content of interceptions due to its sensitivity. However, the Ombudsman noted that ACLEI has procedures in place to assist in adhering to conditions placed on warrants.

AFP

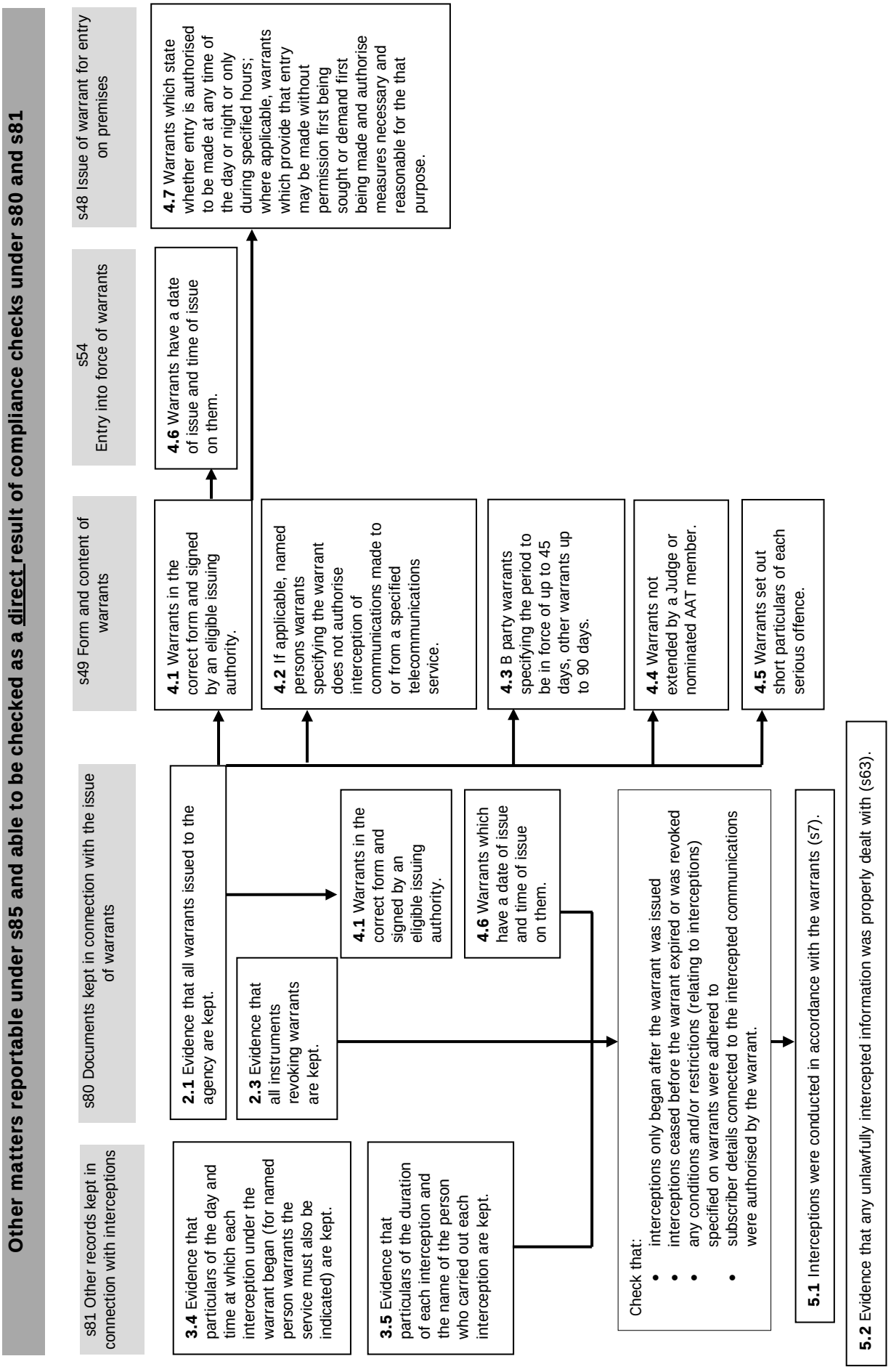
No recommendations were made as a result of either of the two inspections of the AFP.

Objective: to assess agencies' compliance with the record keeping and destruction requirements of the telecommunications interception provisions of the Telecommunications (Interception and Access) Act 1979

s79 Destruction of restricted records	s80 Documents kept in connection with the issue of warrants	s81 Other records kept in connection with interceptions (Warrant details, lawfully intercepted information (LII) records, use and communication records)
1.1 Evidence that the chief officer was satisfied that the restricted records destroyed were not likely to be required for a permitted purpose and were subsequently destroyed forthwith.	**2.1** Evidence that all warrants issued to the agency are kept.	**3.1** Evidence that each telephone application for a part 2-5 warrant is kept.
1.2 Evidence that the restricted records destroyed were not destroyed before the Attorney-General had inspected the warrants under which the restricted records were obtained.	**2.2** Evidence that each notification under s59A(2) are kept (notifications to the Secretary of AGD).	**3.2** Evidence that statements as to whether applications were withdrawn, refused or issued on the application are kept.
	2.3 Evidence that all instruments revoking warrants are kept.	**3.3** Evidence that all warrants whose authority is exercised by the agency are kept.
	2.4 Evidence that each certificate issued under s61(4) is kept (evidentiary certificates).	**3.4** Evidence that particulars of the day and time at which each interception under the warrant began (for named person warrants the service must also be indicated) are kept.
	2.5 Evidence that each authorisation by the chief officer under s66 (2) is kept (authorisation to receive information obtained under warrants).	**3.5** Evidence that particulars of the duration of each interception and the name of the person who carried out each interception are kept.
		3.6 Evidence that particulars of each named person warrant including each service to or from which communications have been intercepted under the warrants are kept.
		3.7 Evidence that each warrant issued to the agency is kept (that relates to restricted records that have at any time been in the agency's possession).
		3.8 Evidence that particulars of each occasion when the restricted record came to be in the agency's possession are kept.
		3.9 Evidence that particulars of each occasion when the restricted record ceased to be in the agency's possession are kept.
		3.10 Evidence that particulars of each other agency from or to which or other person from or to whom the agency received or supplied the restricted record are kept.
		3.11 Evidence that particulars of each use made by the agency of LII are kept.
		3.12 Evidence that particulars of each communication of LII by an officer of the agency to a person or body other than such an officer are kept.
		3.13 Evidence that particulars of when LII was given in evidence in a relevant proceeding in relation to the agency are kept.

Figure 6: Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria

Figure 7: Other matters reportable under s85



CHAPTER 2—STORED COMMUNICATIONS

The TIA Act enables an enforcement agency to apply for a stored communications warrant to assist in the investigation of a serious contravention. Stored communications include communications such as e-mail, SMS or voice messages stored on a carrier's network.

Enforcement agencies that have used stored communications warrants in the reporting year include interception agencies and other regulatory bodies such as:

- ACCC
- ASIC, and
- Customs

Stored communications warrants obtained for a serious contravention include:

- a serious offence (being an offence for which a telecommunications interception warrant may be obtained)
- an offence punishable imprisonment for at least three years, or
- an offence punishable by a fine of least 180 penalty units (currently $30,600) for individuals or 900 penalty units (currently $153,000) for non-individuals such as corporations.

The TIA Act requires this report to set out information in relation to agencies' use of stored communication powers. The required information is set out below in the rest of this Chapter.

Table 23: Applications and telephone applications for stored communications warrants – section 162(1)(a)-(b), and 162(2)(a)-(b)

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR STORED COMMUNICATIONS WARRANTS		TELEPHONE APPLICATIONS FOR STORED COMMUNICATIONS WARRANTS	
		11/12	12/13	11/12	12/13
ACC	Made	8	10	-	-
	Refused/withdrawn	-	-	-	-
	Issued	8	10	-	-
ACCC	Made	3	-	-	-
	Refused/withdrawn	1	-	-	-
	Issued	2	-	-	-
AFP	Made	76	44	-	-
	Refused/withdrawn	-	-	-	-
	Issued	76	44	-	-
ASIC	Made	3	-	-	-
	Refused/withdrawn	-	-	-	-
	Issued	3	-	-	-
CCC WA	Made	2	-	-	-
	Refused/withdrawn	-	-	-	-
	Issued	2	-	-	-
CMC QLD	Made	-	1	-	-
	Refused/withdrawn	-	-	-	-
	Issued	-	1	-	-
CUSTOMS	Made	5	8	-	-
	Refused/withdrawn	-	-	-	-
	Issued	5	8	-	-
NSW CC	Made	6	3	-	-
	Refused/withdrawn	-	-	-	-
	Issued	6	3	-	-
NSW POLICE	Made	181	233	-	-
	Refused/withdrawn	-	-	-	-
	Issued	181	233	-	-
NT POLICE	Made	12	15	-	-
	Refused/withdrawn	-	-	-	-
	Issued	12	15	-	-
PIC	Made	10	4	-	-
	Refused/withdrawn	-	-	-	-
	Issued	10	4	-	-
QLD POLICE	Made	63	101	-	-
	Refused/withdrawn	-	-	-	-
	Issued	63	101	-	-
SA POLICE	Made	12	11	-	-
	Refused/withdrawn	-	-	-	-
	Issued	12	11	-	-
TAS POLICE	Made	32	47	-	-
	Refused/withdrawn	1	-	-	-
	Issued	31	47	-	-
VIC POLICE	Made	9	26	-	-
	Refused/withdrawn	-	-	-	-
	Issued	9	26	-	-
WA POLICE	Made	63	59	-	1
	Refused/withdrawn	-	1	-	-
	Issued	63	58	-	1
TOTAL	**Made**	**485**	**562**	**-**	**1**
	Refused/withdrawn	**2**	**1**	**-**	**-**
	Issued	**483**	**561**	**-**	**1**

Table 24: Stored communications subject to conditions or restrictions – sections 162(2)(d)

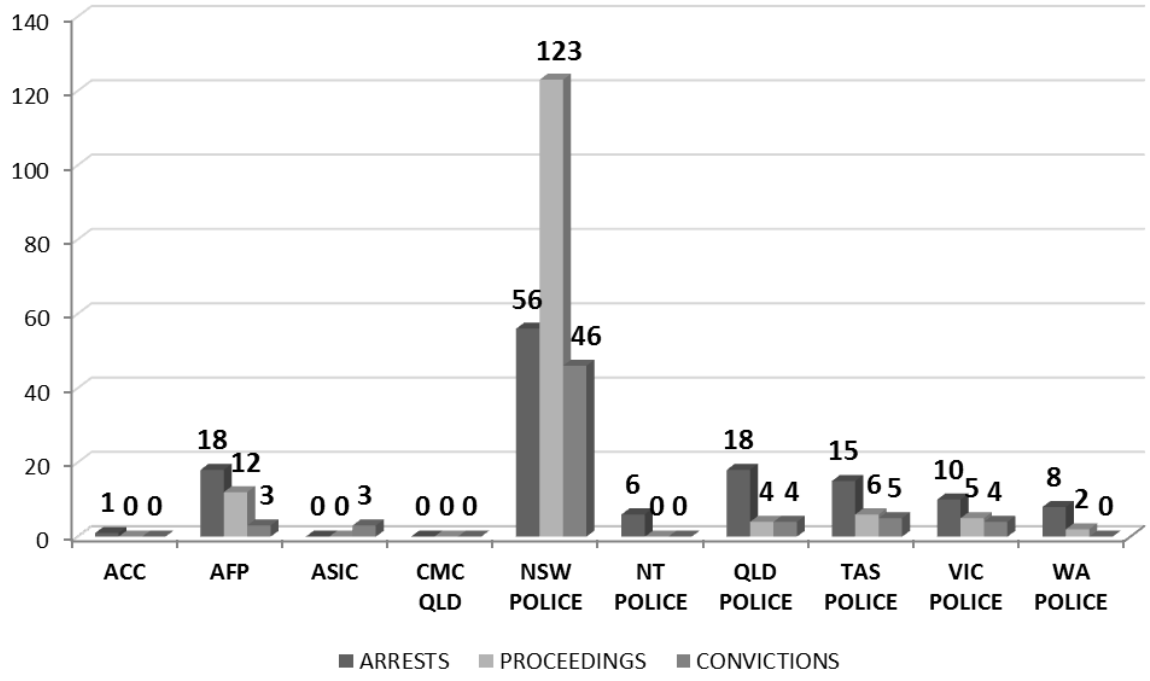
AGENCY	APPLICATIONS FOR WARRANTS	
	11/12	12/13
AFP	9	10
NSW CC	-	1
NSW POLICE	-	14
SA POLICE	12	11
QLD POLICE	2	1
VIC POLICE	-	3
TOTAL	23	40

Effectiveness of stored communications warrants

The below figure provides statistics regarding the effectiveness of stored communications warrants. This includes information about the number of arrests, prosecutions and convictions obtained using stored communications warrants respectively as a suspect arrested in a reporting period may be prosecuted in different reporting period.

Law enforcement agencies were able to make 132 arrests, 152 prosecutions and obtain 65 convictions based on evidence obtained under stored communications warrants.

Figure 8: Number of arrests, proceedings and convictions made on the basis of lawfully accessed information – section 163(a)-(b)



Mutual assistance

The *Cybercrime Legislation Amendment Act 2012* along with the *Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012* inserted new reporting requirements into the TIA Act about mutual assistance requests. These requirements have been included in this Annual Report.

Table 25: Mutual assistance of stored communications warrant applications – section 162(1)(c)

AGENCY	NUMBER OF STORED COMMUNICATIONS WARRANTS MADE AS A RESULT OF MUTUAL ASSISTANCE	NUMBER OF STORED COMMUNICATIONS WARRANTS REFUSED	NUMBER OF STORED COMMUNICATIONS WARRANTS ISSUED AS A RESULT OF MUTUAL ASSISTANCE
AFP	6	-	6
TOTAL	**6**	**-**	**6**

Paragraph 162(1)(d) of the TIA Act provides that the Annual Report must list, for each offence against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual assistance application made by the agency during the year - the offence under a law of the Commonwealth, or of a State or Territory, that is of the same nature as, or substantially similar to, the foreign offence. The AFP advised that the offences related to:

- An offence against section 372.1 of the *Criminal Code Act 1995* (Dealing in identification information)
- An offence against part 10.8 of the *Criminal Code Act 1995* (Dishonestly obtaining or dealing in personal financial information)
- An offence against section 474.14 of *Criminal Code Act 1995* (Using a telecommunications network with intention to commit a serious offence)
- An offence against section134.2 of *Criminal Code Act 1995* (Obtaining a financial advantage by deception)
- An offence against part 10.2 of the *Criminal Code Act 1995* (Money laundering)
- An offence against section 400.8 of the *Criminal Code Act 199*5 (Dealing in proceeds of crime), and
- An offence against section 135.4 of the *Criminal Code Act 1995* (Conspiracy to defraud)

Section 163A of the TIA Act provides that the Annual Report must also provide information regarding the number of occasions on which lawfully accessed information or stored communications warrant information was provided to a foreign country. The AFP responded that this occurred on 6 occasions.

Commonwealth Ombudsman – Inspection of stored communications access records

During the reporting period the Ombudsman inspected 16 enforcement agencies and assessed the records relating to 480 stored communications warrants issued to enforcement agencies in 2011-2012.

The Ombudsman found that there was an overall high level of agency compliance with the stored communications access provisions of the TIA Act.

The Ombudsman also noted that most agencies have implemented the Ombudsman's previous suggestions and recommendations, updating relevant policies and procedures to help staff to comply with the TIA Act.

The Ombudsman's inspection criteria (see Figure 9) are:

- Were destructions properly conducted (ss150 and 151(e))?
- Were records properly kept (s151)?
- Were warrants compliant with the Act (ss116(1)(d), 6B, 5E, 118, 6DB and 119(5))?
- Were conditions and restrictions on warrants adhered to (where applicable) (s117)?
- Was lawfully accessed information only communicated to authorised officers (ss135(1) and (2))?
- Were stored communications warrants validly executed (ss108, 117 and 119) and was any unlawfully obtained product properly dealt with (s133)?

Further information on the Ombudsman's inspection criteria is provided in the diagram below.

Record keeping compliance

The Ombudsman is required to inspect the records of enforcement agencies to ascertain their compliance with sections 150 and 151 of the TIA Act.

The Ombudsman reported that all agencies were compliant with s151 of the TIA Act, which sets out the record keeping requirements relating to stored communications warrants. However, one agency was not able to produce a record at the time of inspection and this issue will be reviewed at the next inspection.

The Ombudsman noted that 10 agencies destroyed records under s150 of the TIA Act. Six agencies were assessed as not compliant with certain provisions under s150. Issues arose from reports not being submitted to the Attorney-General or destructions not occurring in accordance with the TIA Act. In response to these findings, agencies advised that where applicable, reports would be provided, destruction undertaken and procedures implemented or updated to improve compliance.

Issues

As a result of assessing compliance with record keeping requirements, the Ombudsman also assesses compliance with the stored communication access provisions in the TIA Act more generally. Issues that were identified are outlined below.

Operation of legislation

The Ombudsman noted difficulties for enforcement agencies in complying with legislation due to the ambiguities involved in interpreting 'access' to stored communications when a warrant is 'first executed'. The Attorney-General's Department has worked with agencies and carriers to provide guidance on this issue, and the regime was the subject of a review that was put before the

Parliamentary Joint Committee on Intelligence and Security during the reporting period.

Applying for warrants

The Ombudsman noted that two agencies had approached persons who were not authorised to issue warrants under section 6DB of the TIA Act. One of the agencies amended their procedures to address this issue and advised that the obtained stored communications were destroyed. The other agency advised that it was reviewing its procedures and taking other action.

The Ombudsman identified that two agencies applied for warrants in respect of multiple entities. One agency advised that after obtaining advice from the Attorney-General's Department, the stored communications obtained under the warrant would be quarantined and destroyed. The Ombudsman advised the other agency to quarantine the stored communications until they are destroyed.

Determining the date of access

The Ombudsman noted that there were issues relating to determining the date a carrier accessed stored communications under a warrant. This made it difficult to ascertain compliance with the five day limit in s108 of the TIA Act, which only allows access to stored communications within five days after the day on which the warrant was issued. However the Ombudsman noted that, based on the inspections conducted, most carriers were now successfully completing the cover sheet prepared by the Attorney-General's Department in response to previous Ombudsman reports. In instances where carriers did not complete the cover sheet or did not provide clear information, the Ombudsman advised agencies to seek clarification from carriers and quarantine any accessed stored communications until it could be determined that they were accessed lawfully (within the five day limit).

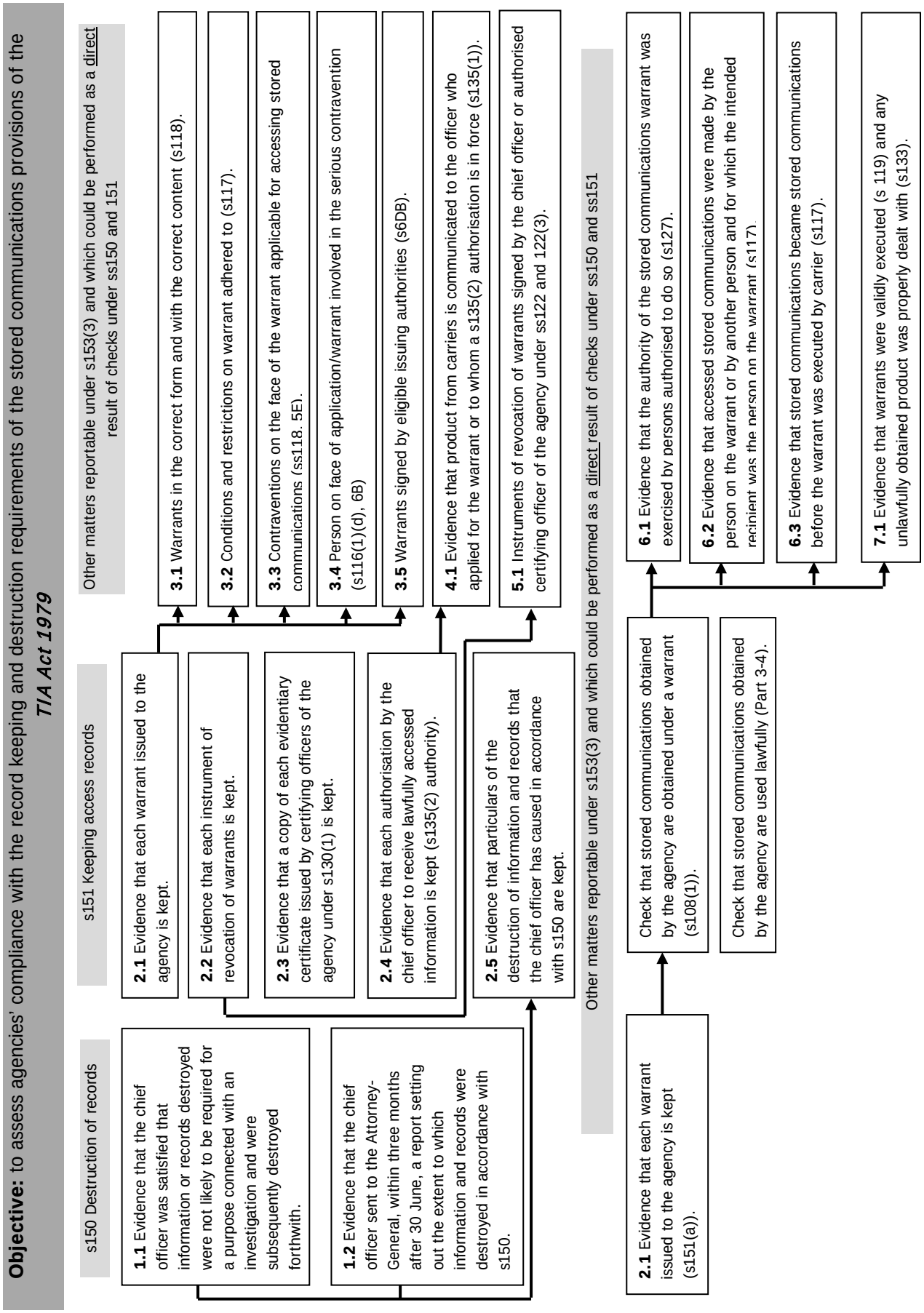
Stored communications accessed outside the authority of warrants

The Ombudsman identified a number of instances where, based on the advice provided by carriers, it appeared that stored communications were accessed after the five day limit. The Ombudsman advised the relevant agencies to quarantine these stored communications. The Ombudsman noted that agencies have implemented suggestions from previous reports to "screen" all stored communications received from carriers and quarantine communications that are not related to the relevant warrant. Despite having procedures in place, the Ombudsman identified that a number of agencies had not identified and quarantined such stored communications, and advised the agencies to take appropriate action.

Adhering to warrant restrictions

The Ombudsman identified that one agency had not fully adhered to warrant restrictions. The agency advised that its normal practice was not followed and that the restriction was not clearly articulated in the warrant. The agency advised that it has updated its procedures to ensure that this issue does not arise in the future and advised that the stored communications obtained would be destroyed.

Figure 9: Commonwealth Ombudsman Stored Communications Access Inspection Criteria



CHAPTER 3—TELECOMMUNICATIONS DATA

Part 4-1 of the TIA Act enables enforcement agencies to authorise the disclosure of telecommunications data by telecommunications carriers or carriage service providers in certain circumstances. Enforcement agencies under the TIA Act include:

- AFP, ACLEI and ACC
- Customs
- CrimTrac
- State and Territory police forces
- State anti-corruption agencies
- A body whose functions include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.

The category of pecuniary penalty and public revenue enforcement agencies includes a range of bodies such as:

- ACCC
- ASIC
- Australian Taxation Office
- Department of Human Services
- Department of Immigration and Citizenship, and
- Local councils

Telecommunications data, also referred to as metadata, communications data and communications associated data, is information about the process of a communication, as distinct from its content. The term includes information about the identity of the sending and receiving parties and related subscriber details, and involves account identifying information collected by the telecommunications carrier or internet service provider to establish the account and information such as the time and date of the communication, its duration, location area and type of communication.

Data authorisations are significant in assisting agencies to safeguard national security, enforce criminal and other laws and to protect the public revenue. Data authorisations are also vital for agencies to obtain the information necessary to apply for telecommunications interception or stored communications warrants.

Under the TIA Act, all enforcement agencies can access historical data and criminal law enforcement agencies can also access prospective data.

Historical Data

Historical data, also known as existing data, is information that is already in existence when an authorisation for disclosure is received by a telecommunications carrier or carriage service provider.

An enforcement agency may authorise a telecommunications carrier to disclose historical data when access to the data is reasonably necessary to:

- enforce a criminal law
- enforce a law imposing a pecuniary penalty, or
- protect the public revenue.

The data access provisions in the TIA Act also allow the AFP and State and Territory Police to issue authorisations for the disclosure of historical data to help locate missing persons.

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

- the head of the agency
- a deputy head of the agency, or
- a person in a senior position in the agency authorised by the head of the agency.

Before making an authorisation for the disclosure of telecommunications data, the authorised officer must weigh the interference with the privacy of any person against the likely usefulness of the information and the reason for the proposed disclosure.

Prospective Data

Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force. Only agencies recognised under the Act as being a 'criminal law enforcement agency' can authorise the disclosure of prospective data. During the current reporting period, a 'criminal law enforcement agency' meant all interception agencies and Customs.

A criminal law enforcement agency can only authorise the disclosure of prospective data when disclosure is considered to be reasonably necessary for the investigation of an offence punishable by imprisonment for at least three years.

A prospective data authorisation comes into force once the relevant telecommunications service provider receives the request. Authorisations can only be in force for 45 days or less.

CASE STUDY: AUSTRALIAN CRIME COMMISSION

In February 2013, the ACC received information indicating a person was processing illicit funds and potentially involved in money laundering. Enquiries revealed that this person had not previously come to the attention of law enforcement.

A check of the person's mobile telephone number conducted by the ACC revealed that it belonged to a second person know to the ACC. The second person is currently suspected of arranging the importation and distribution of large quantities of illicit drugs in Australia.

Analysis of relevant information obtained under the TIA Act showed a relationship between the two people. The ACC assessed that illicit funds being managed by the first person were likely derived from illicit drug sales conducted by the second person. Intelligence regarding this matter has been referred to a Task Force for further investigation.

ACC has related that without the ability to conduct checks under the TIA Act, it is unlikely to have detected—or have the ability to investigate—such relationships.

Existing Data – Enforcement of a Criminal Law

During the reporting period the Victorian Government announced that the Department of Environment and Sustainability, and the Department of Primary Industries would be integrated into the new Department of Environment and Primary Industries.

Further, the New South Wales Office of Environment & Heritage advised that during the reporting period they and Environment Protection Authority separated. The figure provided for 2012-13 includes both agencies as they continue to share administration resources.

Finally, the former Victorian Taxi Directorate has changed its name to Taxi Services Commission.

The following tables provide information on agency use of existing data authorisations in the enforcement of a criminal law.

Table 26: Number of authorisations made by a Law Enforcement Agency for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)

AGENCY	AUTHORISATIONS	
	11/12	12/13
ACC	3,593[11]	3,789
ACLEI	99	2,594
AFP	22,900	25,582
CCC WA	1,305	1,538
CMC QLD	7,040	7,646
IBAC	-	20
ICAC	594	575
NSW CC	3,649	3,120
NSW POLICE	103,824	119,705
NT POLICE	2,828	3,308
OPI	307	71
PIC	1,470	1,771
QLD POLICE	36,531	41,120
SA POLICE	8,025	9,119
TAS POLICE	9,342	8,701
VIC POLICE	67,173	64,458
WA POLICE	12,293	19,812
TOTAL	**280,973**	**312,929**

[11] This figure has been revised following advice from the ACC.

Table 27: Number of authorisations made by a Commonwealth Enforcement Agency for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)

AGENCY	AUTHORISATIONS	
	11/12	12/13
ACCC	77	134
AUSTRALIAN FISHERIES MANAGEMENT AUTHORITY	1	2
ASIC	1,587	1,336
AUSTRALIAN TAXATION OFFICE	654	493
CIVIL AVIATION SAFETY AUTHORITY	-	4
CUSTOMS	5,197	3,902
DEPT. OF AGRICULTURE, FISHERIES AND FORESTRY	76	84
DEPT. OF DEFENCE	10	14
DEPT. OF FAMILIES, HOUSING, COMMUNITY SERVICES AND INDIGENOUS AFFAIRS	-	4
DEPT. OF FOREIGN AFFAIRS AND TRADE	3	84
DEPT. OF HEALTH AND AGEING	52	76
DEPT. OF HUMAN SERVICES	-	1
DEPT. OF SUSTAINABILITY, ENVIRONMENT, WATER, POPULATION AND COMMUNITIES	28	9
INSOLVENCY AND TRUSTEE SERVICE AUSTRALIA	181	111
TOTAL	**7,866**	**6,254**

Table 28: Number of authorisations made by a State or Territory Enforcement Agency for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)

AGENCY	AUTHORISATIONS	
	11/12	12/13
BANKSTOWN CITY COUNCIL	-	5
CORRECTIVE SERVICES NSW	108	69
CORRECTIONS VICTORIA	131	-
DEPT. OF COMMERCE (WA)	458	116
DEPT. OF ENVIRONMENT AND PRIMARY INDUSTRIES (VIC)	-	349
DEPT. OF ENVIRONMENT AND HERITAGE PROTECTION (QLD)	4	-
DEPT. OF PRIMARY INDUSTRIES (VIC)	590	-
JUVENILE JUSTICE NSW	-	-
OFFICE OF ENVIRONMENT & HERITAGE (NSW)	156	106
RSPCA QUEENSLAND	27	8
RSPCA TASMANIA INC.	1	-
RSPCA VICTORIA	35	23
TRANSPORT ACCIDENT COMMISSION (VIC)	9	1
WORKSAFE VICTORIA	-	14
TOTAL	**1,519**	**691**

Table 29: Total number of authorisations made for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)

AGENCY	AUTHORISATIONS	
	11/12	12/13
No. of authorisations made by a Law Enforcement Agency	280,973	312,929
No. of authorisations made by a Commonwealth Agency	7,866	6,254
No. of authorisations made by a State or Territory Agency	1,519	691
TOTAL	**290,358**	**319,874**

Existing Data – Enforcement of a Law Imposing a Pecuniary Penalty or the Protection of the Public Revenue

During the previous reporting period CentreLink, Child Support Program, and Medicare were free standing agencies and reported independently from the Department of Human Services. Following restructuring, all three agencies have been incorporated into the Department, as such from 2012-13 all reporting figures are listed under the Department of Human Services.

Further, in April 2013 the Victorian Government announced that the Department of Environment and Sustainability, and the Department of Primary Industries would be integrated into the new Department of Environment and Primary Industries.

The following tables provide information on agency use of historical data authorisations in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue.

Table 30: Number of authorisations made by a Law Enforcement Agency for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue – section 186(1)(b)

AGENCY	AUTHORISATIONS	
	11/12	12/13
AFP	101	99
NSW POLICE	5464	6,300
NT POLICE	-	2
QLD POLICE	144	110
TAS POLICE	534	67
TOTAL	**6,243**	**6,578**

Table 31: Number of authorisations made by a Commonwealth Enforcement Agency for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue – section 186(1)(b)

AGENCY	AUTHORISATIONS	
	11/12	12/13
ACCC	89	155
AUSTRALIAN HEALTH PRACTITIONER REGULATION AGENCY	4	20
ASIC	179	114
AUSTRALIAN TAXATION OFFICE	177	138
AUSTRALIA POST	251	375
CENTRELINK	1,181	-
CHILD SUPPORT PROGRAM	23	-
CIVIL AVIATION SAFETY AUTHORITY	-	3
CLEAN ENERGY REGULATOR	-	1
CUSTOMS	116	120
DEPT. OF AGRICULTURE, FISHERIES AND FORESTRY	-	8
DEPT. OF DEFENCE	279	127
DEPT. OF FOREIGN AFFAIRS AND TRADE	-	67
DEPT. OF HEALTH AND AGEING	1	1
DEPT. OF HUMAN SERVICES	-	628
DEPT. OF IMMIGRATION AND CITIZENSHIP	-	14
DEPT. OF SUSTAINABILITY, ENVIRONMENT, WATER, POPULATION AND COMMUNITIES	5	-
MEDICARE AUSTRALIA	58	-
FAIR WORK BUILDING & CONSTRUCTION	7	1
TAX PRACTITIONERS BOARD	12	61
TOTAL	**2,382**	**1,833**

Table 32: Number of authorisations made by a State or Territory Enforcement Agency for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue – section 186(1)(b)

AGENCY	AUTHORISATIONS	
	11/12	12/13
ACT REVENUE OFFICE	4	6
BANKSTOWN CITY COUNCIL	4	5
CONSUMER AFFAIRS VICTORIA	230	187
CONSUMER AND BUSINESS SERVICES (SA)	141	209
CORRECTIONS VICTORIA	-	-
DEPT. OF AGRICULTURE, FISHERIES AND FORESTRY (QLD)	33	33
DEPT. OF COMMERCE (WA)	57	84
DEPT. OF ENVIRONMENT AND CONSERVATION (WA)	34	87
DEPT OF ENVIRONMENT AND HERITAGE PROTECTION (QLD)	26	55
DEPT. OF ENVIRONMENT & PRIMARY INDUSTRIES (VIC)	-	51
DEPT. OF ENVIRONMENT AND SUSTAINABILITY (VIC)	23	-
DEPT. OF FISHERIES (WA)	71	101
DEPT. OF JUSTICE AND ATTORNEY-GENERAL (QLD)	309	257
DEPT. OF PRIMARY INDUSTRIES (NSW)	100	197
HARNESS RACING NEW SOUTH WALES	-	12
HEALTH CARE COMPLAINTS COMMISSION (NSW)	39	15
IPSWICH CITY COUNCIL	-	6
JUVENILE JUSTICE NSW	2	-
KNOX CITY COUNCIL	-	5
NSW FAIR TRADING	1,003	740
OFFICE OF LIQUOR AND GAMING REGULATION (QLD)	2	2
OFFICE OF STATE REVENUE (NSW)	127	137
OFFICE OF STATE REVENUE (QLD)	10	5
OFFICE OF THE RACING INTEGRITY COMMISSIONER (VIC)	-	15
RACING AND WAGERING WESTERN AUSTRALIA	-	10
RACING NSW	-	14
RACING QUEENSLAND	-	28
REVENUE SA	26	18
ROADS AND MARITIME SERVICES (NSW)	-	4
RSPCA SOUTH AUSTRALIA	-	1
STATE REVENUE OFFICE VICTORIA	45	40
TASMANIA PRISON SERVICE	7	15
WORKCOVER NSW	-	1
WORKSAFE VICTORIA	7	-
WYNDHAM CITY COUNCIL	11	15
TOTAL	**2,311**	**2,355**

Table 33: Total 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 – section 186(1)(b)

AGENCY	AUTHORISATIONS	
	11/12	12/13
No. of authorisations made by a Law Enforcement Agency	6,243	6,578
No. of authorisations made by a Commonwealth Agency	2,382	1,833
No. of authorisations made by a State or Territory Agency	2,311	2,355
TOTAL	**10,936**	**10,766**

CASE STUDY: Wyndham City Council

In July 2012, Wyndham City received a report of an elderly man who had been attacked by a dog and required hospital treatment for his injuries. Following the attack, the female owner of the dog phoned paramedics and then left the scene without providing her details. Wyndham City contacted Ambulance Victoria, requesting her phone number.

Wyndham City made numerous attempts to contact the dog's owner including requests that she come in and discuss the matter. On each occasion she was evasive and uncooperative. Wyndham City felt that given the circumstances it was important to identify the dog's owner and take appropriate action to ensure the safety of the community.

As a last resort, Wyndham City sought authorisation under the TIA Act to determine her name and address. Wyndham City had advised that they only approve a small number of authorisations under the TIA Act for cases where the information is deemed to be essential in helping to identify a person or persons that have breached the law and strictly for cases that are in the public interest.

The information Wyndham City obtained on the dog's owner led to her identification and allowed Wyndham City to eventually successfully prosecute her in Court.

Prospective data authorisations

The next two tables set out statistics about the use of prospective data authorisations during the reporting year.

Table 34: Prospective data authorisations – sections 186(1)(c)

AGENCY	NUMBER OF AUTHORISATIONS MADE	DAYS SPECIFIED IN FORCE	ACTUAL DAYS IN FORCE	AUTHORISATIONS DISCOUNTED
ACC	915	32,417	21,951	-
AFP	683	22,063	16,709	59
IBAC	5	221	-	5
CCC WA	30	1,238	970	2
CMC QLD	124	22,964	2,409	6
CUSTOMS	167	194	189	4
ICAC	32	1,394	1,065	-
NSW CC	837	30,501	26,155	11
NSW POLICE	667	25,209	15,977	21
NT POLICE	432	19,437	16,651	34
OPI	6	264	264	-
PIC	162	6,575	5,560	12
QLD POLICE	1,643	64,812	46,182	206
SA POLICE	427	17,614	15,184	-
TAS POLICE	197	8,865	5,249	15
VIC POLICE	629	24,763	16,164	50
WA POLICE	576	25,920	16,128	39
TOTAL	**7,532**	**304,451**	**206,807**	**464**

Table 35: Average specified and actual time in force of data authorisations

AGENCY	AVERAGE PERIOD SPECIFIED		AVERAGE PERIOD ACTUAL	
	11/12	12/13	11/12	12/13
ACC	38[12]	35	30[13]	24
AFP	36	32	32	27
CCC WA	40	41	38	35
CMC QLD	12	24	10	20
CUSTOMS	33	1	10	1
IBAC	-	44	-	-
ICAC	45	44	23	33
NSW CC	34	36	28	32
NSW POLICE	38	38	23	25
NT POLICE	45	45	45	42
OPI	32	44	24	44
PIC	43	41	38	37
QLD POLICE	30	39	24	32
SA POLICE	37	41	28	36
TAS POLICE	45	45	24	29
VIC POLICE	38[14]	39	27[15]	28
WA POLICE	45	45	26	30
AVERAGE	**37**	**37**	**27**	**30**

Data authorisations to locate missing persons

Table 36: The number of authorisations made for access to existing information or documents for the location of missing persons – section 178A

AGENCY	AUTHORISATIONS
AFP	45
NSW POLICE	570
NT POLICE	17
QLD POLICE	263
TOTAL	**895**

Foreign law enforcement

The TIA Act also requires the AFP to report on data authorisations made in relation to foreign law enforcement. The AFP advised that 4 data authorisations were made for access to historical data and 1 data authorisation was made for access to prospective data in the reporting period.

[12] This figure has been revised following advice from the ACC.
[13] As above, this report reflects the accurate figure.
[14] This figure has been revised following advice from the Victoria Police.
[15] As above, this report reflects the accurate figure.

CHAPTER 4—FURTHER INFORMATION

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

More information about telecommunications interception and access and telecommunications data access can be found at http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/default.aspx.

Previous copies of the *Telecommunications (Interception and Access) Act 1979* Annual Report can be accessed online at http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx.

APPENDIX A - LIST OF TABLES AND FIGURES

Tables

Figures

APPENDIX B - INTERCEPTION AGENCIES UNDER THE TIA ACT

Commonwealth Agency or State Eligible Authority	Date of s34 declaration
Australian Commission for Law Enforcement Integrity	Not applicable
Australian Crime Commission	Not applicable
Australian Federal Police	Not applicable
Corruption and Crime Commission (Western Australia)	26 March 2004
Crime and Misconduct Commission (Queensland)	7 July 2009
Independent Broad-based Anti-corruption Commission (Victoria)	18 December 2012 (came into force 10 February 2013)
Independent Commission Against Corruption (New South Wales)	6 June 1990
New South Wales Crime Commission	30 January 1989
New South Wales Police Force	30 January 1989
Northern Territory Police	25 October 2006
Office of Police Integrity (Victoria)	18 December 2006 (repealed 10 February 2013)
Police Integrity Commission (New South Wales)	14 July 1998
Queensland Police Service	8 July 2009
South Australian ICAC	17 June 2013 (came into force 1 September 2013)
South Australia Police	10 July 1991
Tasmania Police	5 February 2005
Victoria Police	28 October 1988
Western Australia Police	15 July 1997

APPENDIX C – ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AGD	Attorney-General's Department
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
CAC	Communications Access Co-ordinator
CCC WA	Corruption and Crime Commission - Western Australia
CMC QLD	Crime and Misconduct Commission
Customs	Australian Customs and Border Protection Service
DIAC	Department of Immigration and Citizenship
IBAC	Independent Broad-based Anti-corruption Commission (Victoria)
NSW CC	New South Wales Crime Commission
NSW ICAC	Independent Commission Against Corruption (New South Wales)
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)
PIM	Public Interest Monitor
PJCIS	Parliamentary Joint Committee on Intelligence and Security
QLD Police	Queensland Police Service
ICAC	Independent Commissioner Against Corruption (New South Wales)
SA Police	South Australia Police
TAS Police	Tasmania Police
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
VIC Police	Victoria Police
WA Police	Western Australia Police

APPENDIX D – Categories of serious offences

Serious Offence Category	Offences Covered
ACC special investigation	TIA Act, s5D(1)(f): ACC special investigation
Administration of justice	TIA Act, s5D(8)(b): offences against ss35, 36, 36A, 37, 39, 41, 42, 43, 46 or 47 of the Crimes Act 1914
Assist escape punishment / dispose of proceeds	TIA Act, s5D(7): assisting a person to escape punishment or to dispose of the proceeds of a serious offence
Bribery or corruption; offences against ss131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code	TIA Act, s5D(2)(vii), bribery or corruption; TIA Act, s5D(8)(a): offences against ss131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the Criminal Code Act 1995
Cartel offences	TIA Act, s5D(5B): cartel offences
Child pornography offences	TIA Act, s5D(3B): child pornography offences
Conspire / aid / abet serious offence	TIA Act, s5D(6): conspiring to commit or aiding or abetting the commission of a serious offence
Cybercrime offences	TIA Act, s5D(5): cybercrime offences
Kidnapping	TIA Act, s5D(1)(b): kidnapping
Loss of life or personal injury	TIA Act, s5D(2)(b)(i) and (ii): serious personal injury, loss of life
Money laundering	TIA Act, s5D(4): money laundering
Murder	TIA Act, s5D(1)(a): murder
Organised offences and/or criminal organisations	TIA Act, s5D(3): offences involving planning and organisation; s5D(8A) and (9), criminal organisations
People smuggling and related	TIA Act, s5D(3A): people smuggling, slavery, sexual servitude, deceptive recruiting, trafficking in persons
Serious damage to property and/or serious arson	TIA Act, s5D(2)(b)(iii) and (iiia): serious damage to property, arson
Serious drug offences and/or trafficking	TIA Act, s5D(5A); s5D(2)(b)(iv): serious drug offences, drug trafficking; TIA Act, s5D(1)(c): import or export border controlled drugs
Serious fraud and/or revenue loss	TIA Act, s5D(2)(v) and (vi): serious fraud, serious revenue loss
Telecommunications offences	TIA Act, s5D(5)(a): telecommunications offence
Terrorism offences	TIA Act, s5D(1)(d), 5D(1)(e): terrorism offences