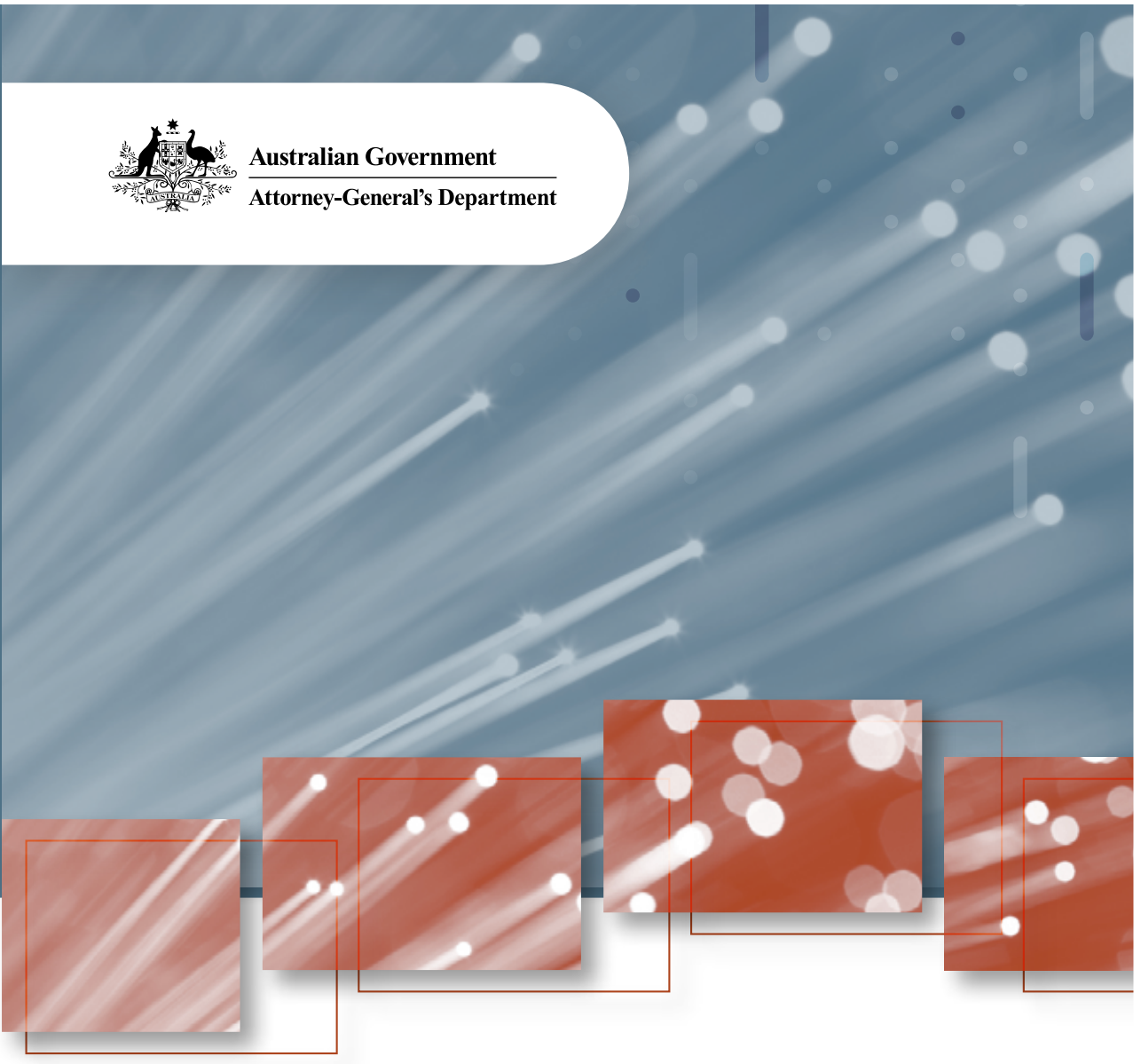


TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

Annual Report 2014–15

ISBN 978-1-925290-48-6 (Print)
ISBN 978-1-925290-49-3 (Online)

© Commonwealth of Australia 2015

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International 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 4.0 licence (www.creativecommons.org/licenses).

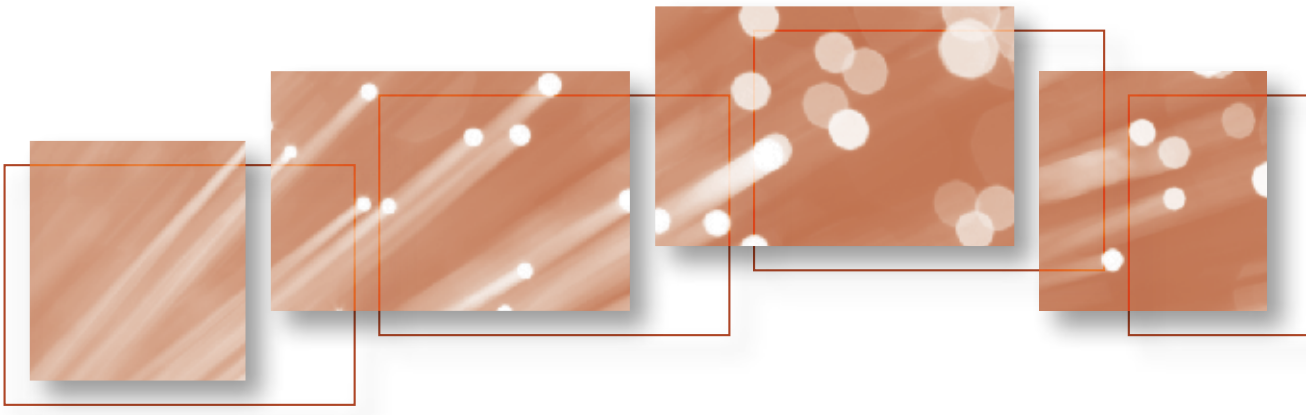
Use of the Coat of Arms

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:

Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Email: copyright@ag.gov.au



TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

Annual Report 2014–15

CONTENTS

EXECUTIVE SUMMARY

The *Telecommunications (Interception and Access) Act 1979 Act Annual Report 2014–15* sets out the extent and circumstances in which eligible Commonwealth, State and Territory government agencies have used the powers available under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) between 1 July 2014 and 30 June 2015.

The primary function of the TIA Act is to protect the privacy of the communications of people who use the Australian telecommunications network. Serious and organised criminals and persons seeking to harm Australia's national security routinely use telecommunications service providers and communications technology to plan and to carry out their activities. Some activities, including child pornography, are predominantly executed through communications devices such as phones and computers.

The TIA Act provides a legal framework for national security and law enforcement agencies to access the information held by communications providers that agencies need to investigate criminal offences and other activities that threaten safety and security. The access that may be sought under the TIA Act includes access to telecommunications data, stored communications that already exist or the interception of communications in real time in prescribed circumstances. Each of the powers available under the TIA Act is explained below.

The use of warrants to either intercept or access stored communications under the TIA Act is independently overseen by the Commonwealth Ombudsman and equivalent state bodies. From 13 October 2015, the number of agencies able to access stored communications was reduced to only criminal-law enforcement agencies and the independent oversight role of the Commonwealth Ombudsman was extended to agency use of telecommunications data under the TIA Act.

Legislative reforms

On 26 March 2015, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) was passed. The Data Retention Act imposed a new data retention obligation on carriers to retain specific information for a period of two years. In addition, the Data Retention Act significantly reduced the number of agencies that may access stored communications and telecommunications data under the TIA Act. It also introduces additional record-keeping and reporting obligations relating to the access to and use of telecommunications data by law enforcement agencies.

The obligations introduced by the Data Retention Act came into effect on 13 October 2015. Accordingly, the 2014-15 annual report does not contain the additional information that the Data Retention Act requires to be included in future reports. For example, future reports will include information relating to the offences for which telecommunications data has been sought and the number of requests for subscriber

data and traffic data. Further information about the record keeping obligations and future annual reporting on the access and use of telecommunications data by enforcement agencies is contained in Chapter 3.

Key judicial decisions

No significant judicial decisions relevant to the TIA Act occurred during the reporting period.

Review of policy developments

There were three inquiries or reviews relating to potential policy developments to the TIA Act during the 2014–15 reporting period:

The Senate Legal and Constitutional Affairs Committee Comprehensive Revision of the TIA Act Report

The Senate for Legal and Constitutional Affairs Committee agreed to inquire into the revision of the TIA Act on 12 December 2013. The Committee was required to comprehensively review the TIA Act having regard to recommendations made by the Australian Law Reform Commission and the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into Potential reforms of Australia's National Security Legislation in May 2013. The Senate Committee tabled its Report on 24 March 2015 recommending reform of the TIA Act. The Government had not responded to that inquiry at the end of the reporting period.

The Senate Committee's inquiry spanned 15 months, during which time, the Government introduced the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

The Data Retention Bill

The Data Retention Bill would require Australian telecommunications companies to keep a limited set of telecommunications data for two years and significantly reduce the number of agencies that may access telecommunications data under the TIA Act. The Bill passed the Parliament on 26 March 2015 as the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act).

The Government noted that telecommunications data is increasingly important to Australia's law enforcement and national security agencies. Access to telecommunications data is central to virtually every counter-terrorism, organised crime, counter-espionage and cyber-security investigation, as well as almost every serious criminal investigation, such as murder, rape and kidnapping by allowing prescribed agencies to determine how and with whom a person has been communicating. The Government indicated its intent to standardise the types of telecommunications data that service providers must retain under the TIA Act and the period of time that information must be held in order to assist investigations into particular offences, given telecommunications data has proven to be a critical tool for law enforcement and national security agencies, providing both intelligence and evidence when identifying and prosecuting alleged offenders.

The Data Retention Act also introduced additional record-keeping and reporting obligations relating to the access to and use of telecommunications data by enforcement agencies, and ensures that this access is subject to comprehensive oversight by the Commonwealth Ombudsman's Office.

The Data Retention Act does not increase or otherwise modify the powers of Australian agencies in relation to access to the content of communications.

Before the Bill passed Parliament, it was reviewed by the PJCIS and the Parliamentary Joint Committee on Human Rights (PJCHR).

The PJCIS inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

In its Report, the PJCIS concluded that data retention is a 'necessary, effective and proportionate response' to combat serious crime and threats to national security and recommended that the Bill be passed subject to recommendations designed to strengthen safeguards and oversight measures. The Committee also recommended that the department undertake a range of additional reviews on policy issues related to access to telecommunications data and telecommunications interception. The Government accepted all of the recommendations in passing the legislation.

The PJCHR review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

The PJCHR tabled its Report on 18 March 2015. The PJCHR examined the compatibility of the Government's Data Retention Bill with human rights. The role of the PJCHR is to consider whether a proposed Bill's limitation on the right to privacy will be permissible under international human rights law where it addresses a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective. The PJCHR was of the view that the Attorney-General generally established that the proposed scheme addresses a pressing and substantial concern which may be regarded as a legitimate objective under international human rights law. It also acknowledged the fundamental and legitimate interests of government in ensuring that there are adequate tools for law enforcement agencies to ensure 'public safety and the ability for victims of crime to have recourse to justice's a result of the PJCHR recommendations the Government introduced additional accountability and oversight arrangements to further protect privacy rights.

Key findings

- In 2014–15, issuing authorities issued 3,926 interception warrants, this is consistent with the 2013–14 period when 4,007 warrants were issued. Interception warrants are highly privacy intrusive and are only sought when operationally necessary and where statutory preconditions are met.
- During 2014–15, information obtained under interception warrants was used in:[1]
  - 3,100 arrests
  - 4,686 prosecutions
  - 1,912 convictions.

1 These figures provide an indication about the effectiveness of interception, rather than the full picture, as, for example, a conviction can be recorded without admitting intercepted information into evidence.

- In 2014–15, 83 enforcement agencies made 365,728 authorisations for the disclosure of historical telecommunications data. Of these, 354,841 authorisations were made to enforce a criminal law. This compares with 334,658 data authorisations made by 77 enforcement agencies in 2013–14, of which 324,260 authorisations were made to enforce a criminal law (a 9 per cent increase from 2013–14).
- In 2014–15, 102 B-Party warrants[2] were issued, around 15 per cent less than in 2013–14.
- In 2014–15, 1,000 named person warrants were issued. This is consistent with the 2013-14 reporting period during which 999 named person warrants were obtained.
- In 2014–15, consistent with the last reporting period, the majority of named person warrants were for the interception of between two to five telecommunications services.
- In 2014–15, law enforcement agencies made 377 arrests, conducted 335 prosecutions and obtained 198 convictions based on evidence obtained under stored communications warrants.[3]
- 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.

Access to the content of a communication

Accessing content, or the substance of a communication—for instance, the message written in an email, the discussion between two parties to a phone call, the subject line of an email or a private social media post—without the knowledge of the person making the communication is highly privacy intrusive. Under the TIA Act, access can only occur under an interception or stored communications warrant, or in certain limited circumstances, such as a life-threatening emergency. Accessing a person's communications is subject to significant limitations, oversight and reporting obligations and the annual report is an important part of this accountability framework.

The ability to access a person's communications is an effective investigative tool that supports and complements information obtained through other methods. In some cases, the weight of evidence obtained through either an interception or a stored communications warrant results in defendants entering guilty pleas, thereby eliminating the need for the intercepted information to be introduced into evidence.

2 A B-Party warrant is an interception warrant that enables an interception agency to intercept the communications of a person who is communicating with a person suspected of involvement in a serious offence.

3 These figures provide an indication about the effectiveness of interception, rather than the full picture, as, for example, a conviction can be recorded without admitting intercepted information into evidence.

Telecommunications data

A critical tool available under the TIA Act is access to telecommunications data.[4]

Telecommunications data is often the first source of lead information for further investigations, helping to eliminate potential suspects and to support applications for more privacy intrusive investigative tools including search warrants and interception warrants. For example, an examination of call charge records can show that a potential person of interest has had no contact with suspects being investigated.

Telecommunications data gives agencies a method for tracing telecommunications from end-to-end. It can also be used to demonstrate an association between people, or to prove that two or more people spoke with each other at a critical point in time (such as before the commission of an alleged offence).

Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits authorities or bodies that are an 'enforcement agency' under the TIA Act to authorise telecommunications carriers to disclose telecommunications data where that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue.[5]

During the reporting period all enforcement agencies could access historical data[6] and only criminal law-enforcement agencies could access prospective data to assist in the investigation of offences punishable by at least 3 years' imprisonment.[7] The Data Retention Act which was passed by the Parliament in March 2015 reduced the number of enforcement agencies that may access telecommunications data on an ongoing basis to 21 specified agencies. There is the ability for the Attorney-General to declare additional agencies in prescribed circumstances.

Format of Annual Report

This Annual Report is organised into three main chapters:

- Chapter 1—telecommunications interception,
- Chapter 2—stored communications; and
- Chapter 3—telecommunications data.

The TIA Act and associated amendments is available online at <www.comlaw.gov.au>.

4 Telecommunications data is information about a communication, such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent.

5 All interception agencies are also enforcement agencies as well as authorities or bodies whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.

6 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.

7 Prospective data is telecommunications data that comes into existence during a period of time in which an authorisation is in force.

More information

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

- Attorney-General's Department <www.ag.gov.au/>
- Department of Communications <www.communications.gov.au/>
- Commonwealth Ombudsman <www.ombudsman.gov.au/>
- Office of the Australian Information Commissioner <www.oaic.gov.au/>
- Telecommunications Industry Ombudsman <www.tio.com.au/>
- Australian Communications and Media Authority <www.acma.gov.au/>

CHAPTER 1

TELECOMMUNICATIONS INTERCEPTION

The primary function of the TIA Act is to protect the privacy of the communications of people who use the Australian telecommunications network by making it an offence to intercept communications, subject to limited lawful exceptions. 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.

Definition

The term 'interception agency' is defined in section 5 of the TIA Act. This is limited to agencies such as the Australian Federal Police and State and Territory police forces eligible to apply under Part 2–5 of the TIA Act for an interception warrant.

The TIA Act provides for several types of warrants which enable access to the content of a communication, including warrants allowing access to 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).

During the reporting period, interception warrants were available to 17 Commonwealth, 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 obtain an interception warrant is provided in Appendix B.

Serious offences

Interception warrants can only be obtained to investigate serious offences. 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 involving child pornography, money laundering, and offences involving organised crime.

The information provided in Table 1 illustrates the important role telecommunications interception plays in investigating serious crimes. Consistent with previous years, in 2014–15 agencies obtained the majority of warrants to assist with investigations into serious drug offences (1,901 warrants). Loss of life or personal injury offences were specified in 477 warrants and 420 warrants related to murder investigations. Organised crime was specified as an offence in 203 warrants. The total number of offences is typically larger than the total number of warrants issued as warrants can be issued to investigate more than one serious offence.

Information about the serious offences covered under each category of serious offence set out in the first column of Table 1 is provided in Appendix D.

Table 1: Categories of serious offences specified in telecommunications interception warrants—ss. 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	ACC	ACLEI	AFP	CCC (WA)	CCC (QLD)	IBAC	ICAC (NSW)	ICAC (SA)	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	TAS POL	VIC POL	WA POL	TOTAL
ACC Special Investigations	286	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	286
Administration of Justice	-	-	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4
Assisting a person to escape or dispose of proceeds	-	-	1	-	-	-	-	-	12	14	-	-	1	-	-	-	-	28
Bribery or corruption; offences against ss 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code	-	7	40	23	7	-	5	2	-	8	1	30	-	2	-	3	21	149
Cartel Offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Child Pornography Offences	2	-	3	-	-	-	-	-	-	5	-	-	-	-	-	-	-	10
Conspire/Aid/Abet Serious Offence	-	-	-	-	-	-	-	1	7	28	7	-	-	4	-	2	-	49
Cybercrime Offences	-	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Kidnapping	-	-	-	-	-	-	-	-	13	34	-	-	-	2	1	3	-	53
Loss Of Life Or Personal Injury	-	-	16	-	-	-	-	-	-	378	6	-	4	3	-	51	19	477
Money Laundering	1	-	148	-	-	-	-	-	27	-	-	8	1	-	-	-	12	197
Murder	-	-	24	-	-	-	-	-	56	204	15	-	27	8	9	39	38	420
Organised Offences and/or Criminal Organisations	-	-	4	-	-	-	-	-	-	172	-	-	1	5	-	6	15	203
People Smuggling And Related	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Serious Damage To Property and/or Serious Arson	-	-	7	-	-	-	-	-	-	40	-	-	-	2	-	9	5	63
Serious Drug Offences and/or Trafficking (9.1 Criminal Code)	-	-	588	-	30	4	-	-	90	583	25	10	236	62	14	61	198	1,901
Serious Fraud and/or Revenue Loss	-	-	67	-	7	14	-	-	-	66	-	-	1	-	-	-	10	165
Telecommunications Offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Terrorism Offences	-	-	121	-	-	-	-	-	-	-	-	-	-	-	-	-	-	121
Total	**289**	**7**	**1,024**	**23**	**44**	**18**	**5**	**3**	**205**	**1,532**	**54**	**48**	**271**	**88**	**24**	**174**	**318**	**4,127**

Eligibility to issue an interception warrant

An interception warrant may only be issued by an eligible Judge or a nominated Administrative Appeals Tribunal (AAT) member. Table 2 records that in 2014–15 there were 80 issuing authorities.

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.

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.

Table 2: Availability of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges and nominated AAT Members to issue telecommunications interception warrants—s. 103(ab)

Issuing authority	Number eligible
Federal Court judges	14
Family Court judges	4
Federal Circuit Court judges	33
Nominated AAT members	29

Before issuing an interception warrant the authority must take into account:

- the gravity of the conduct of the offence/s being investigated
- how much the interception would be likely to assist with the investigation, and
- the extent to which other methods of investigating the offence are available to the agency

Applications for and issue of telecommunications interception warrants

Table 3 sets out information about the number of eligible judges and nominated AAT members and the agencies to which they issued warrants. In 2014–15, issuing authorities issued 3,926 interception warrants, a decrease of around 2 per cent from 2013–14, when 4,007 warrants were issued. Interception warrants are highly privacy intrusive and are only sought when operationally necessary.

Table 3: Number of telecommunications interception warrants issued by Federal Court judges, Family Court judges, Federal Circuit Court judges and nominated AAT members—s. 103(ab)

Agency	Issuing authority			
	Family Court judges	Federal Court judges	Federal Circuit Court judges	Nominated AAT members
ACC	-	-	11	278
ACLEI	-	-	3	-
AFP	8	119	56	669
CCC (QLD)	-	-	5	39
CCC (WA)	5	-	-	18
IBAC	-	-	-	18
ICAC (NSW)	-	-	-	5
ICAC (SA)	-	-	-	3
NSW CC	-	-	-	185
NSW Police	-	118	-	1,414
NT Police	21	-	-	33
PIC	-	4	-	44
QLD Police	-	-	178	93
SA Police	-	-	5	80
TAS Police	-	-	-	24
VIC Police	-	-	-	172
WA Police	170	-	-	148
Total	**204**	**241**	**258**	**3,223**

Table 4: Applications for telecommunications interception warrants, telephone interception warrants, and renewal applications—ss. 100(1)(a)-(c) and 100(2)(a)-(c)

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants[8]		Renewal applications[9]	
		13/14	14/15	13/14	14/15	13/14	14/15
ACC	Made	253	290	-	-	25	27
	Refused/withdrawn	-	1	-	-	-	-
	Issued	253	289	-	-	25	27
ACLEI	Made	25	3	-	-	17	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	25	3	-	-	17	1
AFP	Made	690	856	-	3	143	243
	Refused/withdrawn	6	4	-	-	-	-
	Issued	684	852	-	3	143	243
CCC (QLD)	Made	38	44	-	-	7	13
	Refused/withdrawn	-	-	-	-	-	-
	Issued	38	44	-	-	7	13
CCC (WA)	Made	67	25	-	-	23	7
	Refused/withdrawn	3	2	-	-	-	-
	Issued	64	23	-	-	23	7
IBAC	Made	16	18	-	-	1	6
	Refused/withdrawn	-	-	-	-	-	-
	Issued	16	18	-	-	1	6
ICAC (NSW)	Made	21	5	-	-	8	2
	Refused/withdrawn	-	-	-	-	-	-
	Issued	21	5	-	-	8	2
ICAC (SA)	Made	6	3	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	6	3	-	-	-	-
NSW CC	Made	349	185	-	-	71	68
	Refused/withdrawn	-	-	-	-	-	-
	Issued	349	185	-	-	71	68
NSW Police	Made	1,519	1,532	57	40	197	252
	Refused/withdrawn	5	-	-	-	-	-
	Issued	1,514	1,532	57	40	197	252
NT Police	Made	43	54	-	-	4	9
	Refused/withdrawn	-	-	-	-	-	-
	Issued	43	54	-	-	4	9
PIC	Made	35	48	-	-	8	9
	Refused/withdrawn	-	-	-	-	-	-
	Issued	35	48	-	-	8	9
QLD Police	Made	308	271	-	-	33	42
	Refused/withdrawn	4	-	-	-	-	-
	Issued	304	271	-	-	33	42

Agency	Relevant statistics	Applications for warrants		Telephone applications for warrants[8]		Renewal applications[9]	
		13/14	14/15	13/14	14/15	13/14	14/15
SA Police	Made	132	85	3	-	9	3
	Refused/withdrawn	-	-	-	-	-	-
	Issued	132	85	3	-	9	3
TAS Police	Made	35	24	-	1	6	6
	Refused/withdrawn	-	-	-	-	-	-
	Issued	35	24	-	1	6	6
VIC Police	Made	188	174	15	1	7	9
	Refused/withdrawn	-	2	-	-	-	-
	Issued	188	172	15	1	7	9
WA Police	Made	300	318	-	-	44	53
	Refused/withdrawn	-	-	-	-	-	-
	Issued	300	318	-	-	44	53
Total	**Made**	**4,025**	**3,935**	**75**	**45**	**603**	**750**
	Refused/withdrawn	**18**	**9**	**-**	**-**	**-**	**-**
	Issued	**4,007**	**3,926**	**75**	**45**	**603**	**750**

The TIA Act provides that in exceptional circumstances, an issuing authority can issue an interception warrant that authorises entry on to premises to carry out telecommunications interception. An issuing authority can only issue such a warrant if satisfied that it would be impracticable or inappropriate to intercept communications otherwise than by use of equipment installed on those premises. Agencies only use this type of warrant on rare occasions.

Table 5: Applications for telecommunications interception warrants authorising entry on premises—ss. 100(1)(d) and 100(2)(d)

Agency	Relevant statistics	Warrants authorising entry on premises	
		13/14	14/15
AFP	Made	-	1
	Refused/withdrawn	-	-
	Issued	-	1
CCC (WA)	Made	1	2
	Refused/withdrawn	-	-
	Issued	1	2
Total	**Made**	**1**	**3**
	Refused/withdrawn	**-**	**-**
	Issued	**1**	**3**

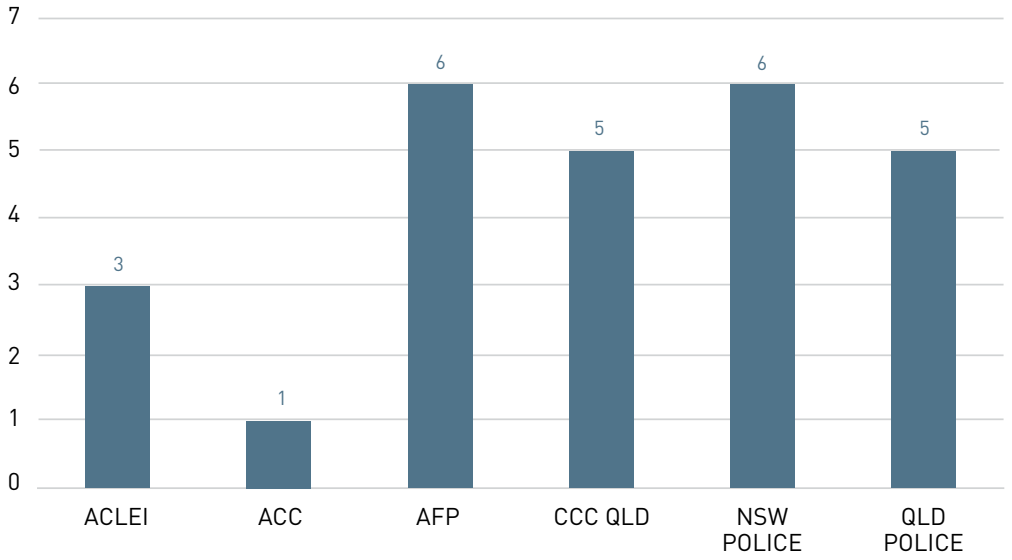
8 Telephone applications are part of the total application of warrants.

9 A renewal is a warrant that is issued for an existing warrant that is still in force

An issuing authority can place any conditions or restrictions on an interception warrant they consider necessary. For example, a condition or restriction may limit the ability for the agency to use or communicate the information obtained under the warrant, or restrict when interceptions may occur.

Figure 1 provides information about the use of warrants issued with conditions or restrictions. In 2014–15, 26 interception warrants were issued with a condition or a restriction.

Figure 1: Telecommunications interception warrants issued with specific conditions or restrictions—ss. 100(1)(e) and 100(2)(e)



Effectiveness of telecommunications interception warrants

The information provided in this section 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 until a later reporting period. Any resulting conviction could be recorded in that or a subsequent 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.

The tables may also 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 continue to report that telecommunications interception effectively enables investigators to identify persons involved in and the infrastructure of, organised criminal activities. In some cases, the weight of evidence obtained through telecommunications interception results in defendants entering guilty pleas, thereby eliminating the need for the intercepted information to be admitted into evidence.

In 2014–15 there were 3,100 arrests, 4,686 prosecutions and 1,912 convictions based on lawfully intercepted material. Tables 6, 7 and 8 provide this information.

Table 6: Arrests on the basis of lawfully intercepted information—ss. 102(1)(a) and 102(2)(a)[10]

Agency	Arrests	
	13/14	14/15
ACC	105	104
ACLEI	10	5
AFP	209	281
CCC (WA)	1	-
CCC (QLD)	10	46
NSW CC	139	102
NSW Police	1,181	1,171
NT Police	47	35
PIC	50	9
QLD Police	437	457
SA Police	121	159
TAS Police	57	31
VIC Police	254	329
WA Police	317	371
Total	**2,938**	**3,100**

10 The figures include statistics from agencies that do not have formal arrest powers and require the assistance of other law-enforcement agencies to execute an arrest. In these circumstances, an arrest figure may have been recorded in both the agency that obtained the warrant and the arresting agency.

Table 7: Prosecutions in which lawfully intercepted information was given in evidence

Categories of offences	ACC	ACLEI	AFP	CCC (WA)	CCC (QLD)	NSW CC	NSW POL	NT POL	PIC	QLD POL	SA POL	VIC POL	WA POL	TOTAL
ACC special investigations	3	-	-	-	-	-	-	-	-	-	-	-	-	**3**
Administration of Justice	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Assisting a person to escape or dispose of proceeds	-	-	-	-	-	2	12	-	-	-	-	3	-	**17**
Bribery or corruption; offences against ss 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code	-	-	13	-	-	-	1	1	1	-	-	1	5	**22**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Child pornography offences	-	-	1	-	-	-	-	-	-	1	-	-	-	**2**
Conspire/aid/abet serious offence	-	-	2	-	-	-	6	1	8	-	1	7	-	**25**
Cybercrime offences	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Kidnapping	-	-	-	-	-	-	20	-	-	-	8	13	-	**41**
Loss of life or personal injury	-	-	3	-	-	5	27	-	-	-	11	106	11	**163**
Money laundering	-	-	84	-	-	14	11	1	1	2	-	19	8	**140**
Murder	-	-	-	-	-	2	33	5	-	2	5	13	12	**72**
Organised offences and/or criminal organisations	-	-	6	-	-	41	95	-	-	1	7	1	211	**362**
People smuggling and related	-	-	21	-	-	-	-	-	-	-	11	-	-	**32**
Serious damage to property and/or serious arson	-	-	-	-	-	2	40	-	-	-	-	4	5	**51**
Serious drug offences and/or trafficking	-	3	209	-	4	197	1,530	12	-	200	116	322	524	**3,117**
Serious fraud and/or revenue loss	-	-	62	1	-	-	241	-	-	17	-	5	4	**330**
Telecommunications offences	-	-	-	-	-	-	15	-	-	-	-	-	-	**15**
Terrorism offences	-	-	14	-	-	-	-	-	-	-	-	-	-	**14**
Other serious offences	-	-	32	-	-	-	240	-	8	-	-	-	-	**280**
Total	**3**	**3**	**447**	**1**	**4**	**263**	**2,271**	**20**	**18**	**223**	**159**	**494**	**780**	**4,686**

Table 8: Convictions in which lawfully intercepted information was given in evidence

Categories of offences	ACC	ACLEI	AFP	CCC (WA)	CCC (QLD)	NSW CC	NSW POL	PIC	QLD POL	SA POL	VIC POL	WA POL	TOTAL
ACC special investigations	3	-	-	-	-	-	-	-	-	-	-	-	**3**
Administration of Justice	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Assisting a person to escape or dispose of proceeds	-	-	-	-	-	-	6	-	-	-	-	-	**6**
Bribery or corruption; offences against ss 131.1, 135.1, 142.1, 142.2, 148.2, 268.112 of the Criminal Code	-	2	8	-	-	-	3	-	-	-	1	2	**16**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Child pornography offences	-	-	-	-	-	-	17	-	1	-	-	-	**18**
Conspire/aid/abet serious offence	-	-	-	-	-	-	1	1	-	-	2	-	**4**
Cybercrime offences	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Kidnapping	-	-	-	-	-	-	8	-	-	-	6	-	**14**
Loss of life or personal injury	-	-	-	-	-	-	21	-	-	1	50	4	**76**
Money laundering	-	-	14	-	-	7	5	-	2	-	15	4	**47**
Murder	-	-	-	-	-	-	14	-	2	3	11	7	**37**
Organised offences and/or criminal organisations	-	-	2	-	-	25	53	-	1	-	1	169	**251**
People smuggling and related	-	-	4	-	-	-	-	-	-	-	-	-	**4**
Serious damage to property and/or serious arson	-	-	-	-	-	1	5	-	-	-	2	2	**10**
Serious drug offences and/or trafficking	-	4	92	-	4	86	318	-	197	9	204	347	**1,261**
Serious fraud and/or revenue loss	-	-	29	-	-	-	22	-	17	-	3	1	**72**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	**-**
Terrorism offences	-	-	2	-	-	-	-	-	-	-	-	-	**2**
Other serious offences	-	-	13	-	-	-	69	9	-	-	-	-	**91**
Total	**3**	**6**	**164**	**-**	**4**	**119**	**542**	**10**	**220**	**13**	**295**	**536**	**1,912**

Named person warrants

A named person warrant can authorise the interception of multiple telecommunications services (such as a landline or mobile service), or 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 tables and figures show that in 2014–15, 1,000 named person warrants were issued, this is comparable to the 2013–14 reporting period in which 999 named person warrants were issued.

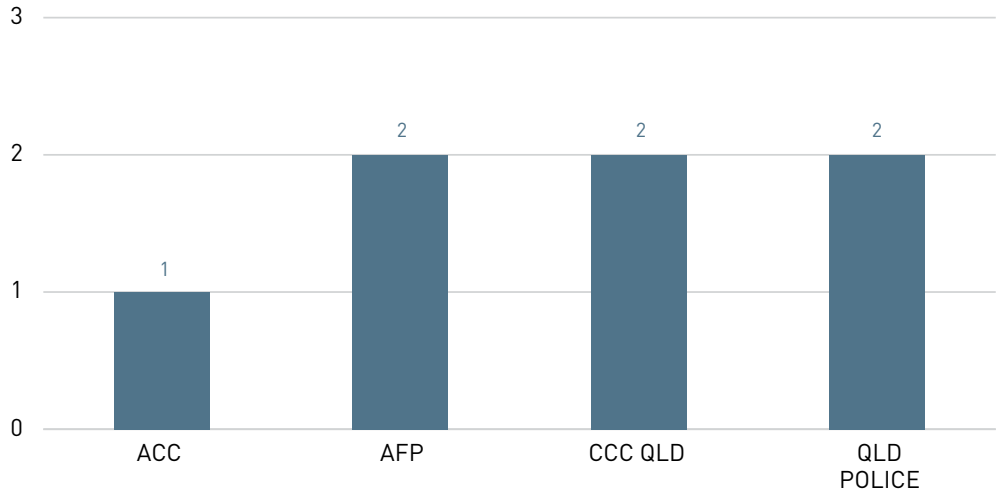
Table 9: Original applications for named person warrants, telephone applications for named person warrants, and renewal applications—ss. 100(1)(ea) and 100(2)(ea)

Agency	Relevant statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		13/14	14/15	13/14	14/15	13/14	14/15
ACC	Made	168	185	-	-	22	23
	Refused/withdrawn	-	-	-	-	-	-
	Issued	168	185	-	-	22	23
ACLEI	Made	4	-	-	-	1	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	4	-	-	-	1	-
AFP	Made	318	335	-	1	106	110
	Refused/withdrawn	3	2	-	-	-	-
	Issued	315	333	-	1	106	110
CCC (QLD)	Made	13	26	-	-	6	11
	Refused/withdrawn	-	-	-	-	-	-
	Issued	13	26	-	-	6	11
CCC (WA)	Made	2	2	-	-	1	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	2	2	-	-	1	-
IBAC	Made	8	2	-	-	1	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	8	2	-	-	1	1
NSW CC	Made	145	91	-	-	32	47
	Refused/withdrawn	-	-	-	-	-	-
	Issued	145	91	-	-	32	47

Agency	Relevant statistics	Applications for named person warrants		Telephone applications for named person warrants		Renewal applications for named person warrants	
		13/14	14/15	13/14	14/15	13/14	14/15
NSW Police	Made	105	144	-	2	25	39
	Refused/withdrawn	-	-	-	-	-	-
	Issued	105	144	-	2	25	39
NT Police	Made	3	-	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	3	-	-	-	-	-
QLD Police	Made	42	46	-	-	6	6
	Refused/withdrawn	1	-	-	-	-	-
	Issued	41	46	-	-	6	6
SA Police	Made	25	3	-	-	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	25	3	-	-	-	-
TAS Police	Made	9	5	-	-	4	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	9	5	-	-	4	1
VIC Police	Made	44	44	1	-	1	3
	Refused/withdrawn	-	-	-	-	-	-
	Issued	44	44	1	-	1	3
WA Police	Made	117	119	-	-	26	32
	Refused/withdrawn	-	-	-	-	-	-
	Issued	117	119	-	-	26	32
Total	**Made**	**1,003**	**1,002**	**1**	**3**	**231**	**273**
	Refused/withdrawn	**4**	**2**	**-**	**-**	**-**	**-**
	Issued	**999**	**1,000**	**1**	**3**	**231**	**273**

Under the TIA Act, issuing authorities can issue a warrant with conditions and restrictions about interceptions under the warrant. In 2014–15, 7 named person warrants were issued with a condition or restriction.

Figure 2: Named person warrants issued with conditions or restrictions—ss. 100(1)(ea) and 100(2)(ea)



Consistent with the last reporting period, in 2014–15 the majority of named person warrants were for the interception of between two to five telecommunications services.

Table 10: Number of services intercepted under named person warrants—ss. 100(1)(eb) and 100(2)(eb)

Agency	Relevant statistics							
	1 service only		2 –5 services		6–10 services		10+ services	
	13/14	14/15	13/14	14/15	13/14	14/15	13/14	14/15
ACC	47	50	106	123	12	18	-	8
ACLEI	2	-	2	-	-	-	-	-
AFP	44	104	195	205	23	21	2	1
CCC (QLD)	5	7	6	15	2	3	-	-
CCC (WA)	-	-	1	1	-	-	1	1
IBAC	-	-	6	1	2	1	-	-
NSW CC	51	36	82	47	8	6	1	1
NSW Police	29	33	59	95	11	10	-	-
NT Police	-	-	1	-	1	-	1	-
QLD Police	8	10	27	32	6	4	-	-
SA Police	4	-	18	3	2	-	-	-
TAS Police	-	-	7	4	2	2	-	-
VIC Police	8	10	32	28	4	2	-	1
WA Police	33	33	74	78	10	8	-	-
Total	**231**	**283**	**616**	**632**	**83**	**75**	**5**	**12**

Subsections 100(1)(ec)(i)-(iii) require the report to include the following information in relation to named person warrants the total number of:

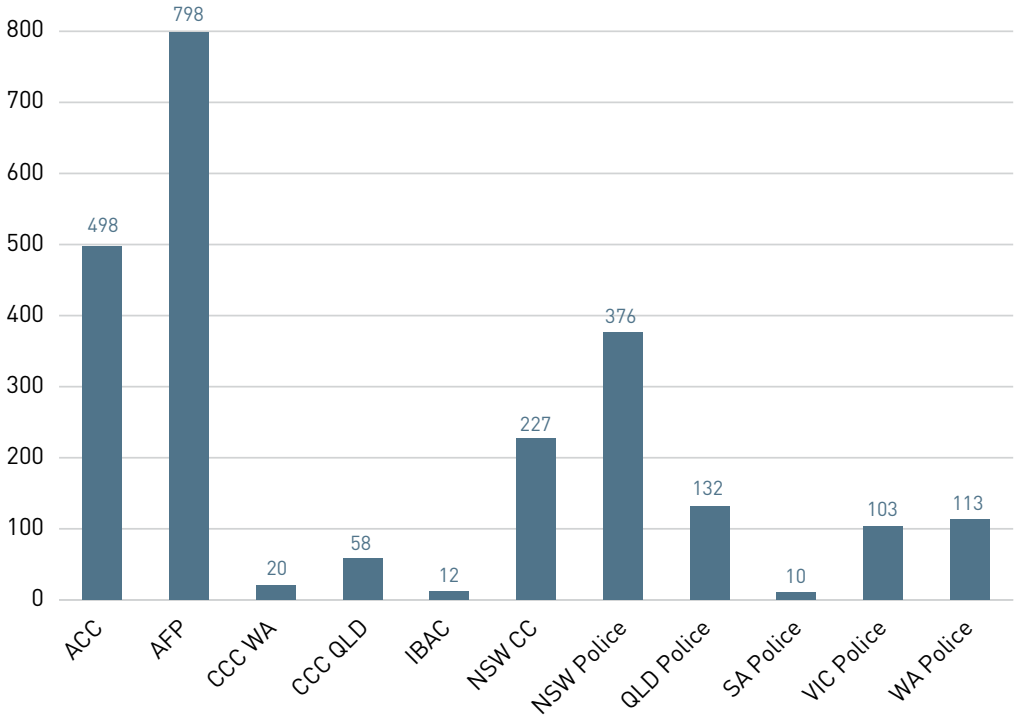
(i) services intercepted under service based named person warrants

(ii) services intercepted under device based named person warrants, and

(iii) telecommunications devices intercepted under device based named person warrants.

Figure 3 and Table 11 outline the number of services intercepted under the different types of named person warrants and should be read in conjunction with Table 9 which provides the total number of named person warrants issued.

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



Under the TIA Act, agencies can apply for a named person warrant in relation to telecommunications devices, where a device or devices of interest can be identified. Table 11 shows, consistent with previous years, that in 2014–15 device-based named person warrants were used by only a small number of agencies.

Table 11: Total number of services and devices intercepted under device-based named person warrants—ss. 100(1)(ec) and 100(2)(ec)

Agency	Services	Devices
ACC	79	63
AFP[11]	-	72
NSW CC	-	1
NSW Police	6	5
VIC Police	9	3
WA Police	6	-
Total	**100**	**144**

B-Party warrants

Definition

A 'B-Party warrant' is a warrant that enables an interception agency to intercept the communications of a person who is communicating with a person suspected of involvement in a serious offence.

An issuing authority can issue a B-Party warrant, but only if there are no other practicable methods of identifying the telecommunications services of the person involved in the offences, or if interception of communications from that person's telecommunications services would not otherwise be possible.

Table 12 shows that in 2014–15, 102 B-Party warrants were issued, around 26 per cent less than in 2013–14.

11 The number of services intercepted under device based warrants is unavailable for the AFP during the reporting period and will be updated in the next Annual Report.

Table 12: Applications for B-Party warrants, telephone applications for B-Party warrants, and renewal applications—ss. 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	
		13/14	14/15	13/14	14/15	13/14	14/15
ACC	Made	-	4	-	-	-	1
	Refused/withdrawn	-	-	-	-	-	-
	Issued	-	4	-	-	-	1
ACLEI	Made	11	-	-	-	10	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	11	-	-	-	10	-
AFP	Made	62	50	-	-	18	32
	Refused/withdrawn	-	-	-	-	-	-
	Issued	62	50	-	-	18	32
NSW CC	Made	6	7	-	-	1	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	6	7	-	-	1	-
NSW Police	Made	57	41	8	9	-	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	57	41	8	9	-	-
SA Police	Made	3	-	-	-	1	-
	Refused/withdrawn	-	-	-	-	-	-
	Issued	3	-	-	-	1	-
Total	**Made**	**139**	**102**	**8**	**9**	**30**	**33**
	Refused/withdrawn	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**139**	**102**	**8**	**9**	**30**	**33**

Table 13: B-Party warrants issued with conditions or restrictions—ss. 100(1)(ed) and 100(2)(ed)

Agency	Applications for B-Party warrants	
	13/14	14/15
ACLEI	11	-
AFP	-	2
NSW Police	2	1
Total	**13**	**3**

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. Table 14 sets out the average length of time for which interception warrants—including renewals, but not including B-Party warrants—were issued and the average length of time they were in force.

Table 14: Duration of original and renewal telecommunications interception warrants—ss. 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	89	51	86	70
ACLEI	90	82	90	50
AFP	84	61	82	70
CCC (QLD)	82	68	84	67
CCC (WA)	69	37	71	71
IBAC	90	89	90	90
ICAC (NSW)	90	89	90	40
ICAC (SA)	88	88	-	-
NSW CC	82	70	89	79
NSW Police	61	46	65	55
NT Police	90	53	90	50
PIC	82	70	90	88
QLD Police	74	56	68	60
SA Police	76	50	56	32
TAS Police	74	47	84	84
VIC Police	74	54	53	32
WA Police	89	55	87	66
Average	**81**	**63**	**80**	**63**

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 they were in force.

Table 15: Duration of original and renewal B-Party warrants—ss. 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	45	45	-
AFP	42	40	45	43
NSW CC	35	35	-	-
NSW Police	31	13	-	-
Average	**38**	**33**	**45**	**43**

A final renewal means a telecommunications interception warrant that is the last renewal of an original warrant. A final renewal 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.

Table 16 provides information on the number of final renewals used by agencies.

Table 16: Number of final renewals—ss. 101(1)(e) and 101(2)(e)

Agency	90 days		150 days		180 days	
	13/14	14/15	13/14	14/15	13/14	14/15
ACC	9	8	9	8	1	6
ACLEI	-	-	1	-	3	-
AFP	64	35	2	51	23	68
CCC (QLD)	-	2	-	8	2	-
CCC (WA)	6	1	1	6	2	-
IBAC	-	-	-	4	-	1
ICAC (NSW)	1	2	2	-	2	-
NSW CC	12	3	27	18	15	20
NSW Police	79	110	48	8	34	30
NT Police	-	-	1	3	-	2
PIC	4	3	-	-	3	-
QLD Police	14	13	4	12	3	4
SA Police	6	3	-	-	1	-
TAS Police	5	-	-	-	-	-
VIC Police	2	-	-	-	-	-
WA Police	-	11	30	23	1	12
Total	**202**	**191**	**125**	**141**	**90**	**143**

Eligible warrants

Definition

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

Table 17 sets out the number of eligible warrants issued to agencies during the reporting period and the percentage of warrants issued to agencies that were eligible warrants.

Table 17: Percentage of eligible warrants—ss. 102(3) and 102(4)

Agency	Total number of warrants	Number of eligible warrants	%
ACC	332	141	42
ACLEI	6	4	67
AFP	1,206	849	70
CCC (QLD)	55	35	64
CCC (WA)	34	19	56
IBAC	20	12	60
ICAC (NSW)	5	5	100
ICAC (SA)	3	2	67
NSW CC	251	234	93
NSW Police	1,529	1,176	77
NT Police	54	25	46
PIC	13	11	85
QLD Police	309	296	96
SA Police	85	60	71
TAS Police	26	20	77
VIC Police	205	142	69
WA Police	365	162	44
Total	**4,498**	**3,193**	**71**

Interception without a warrant

Under the TIA Act, agencies can undertake interception without a warrant in limited circumstances, for example, where there is a serious threat to life or the possibility of serious injury. Table 18a reports on interceptions under subsection 7(5) of the TIA Act, which relates to situations where the person to whom the communication is directed consents to the interception. Table 18b reports on subsection 7(4) of the TIA Act, which relates to situations where an officer of the agency undertaking the interception is a party to the communication.

Table 18a: Interception without a warrant—s. 102A

Agency	Consent where person likely to receive communication from person who has:							
	Committed 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	
	13/14	14/15	13/14	14/15	13/14	14/15	13/14	14/15
AFP	-	-	5	-	-	-	-	-
Total	**-**	**-**	**5**	**-**	**-**	**-**	**-**	**-**

Table 18b: Interception without a warrant—s. 102A

Agency	Agency is a party to the communication and has reasonable grounds for believing person likely to receive communication from person who has:							
	Committed 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	
	13/14	**14/15**	**13/14**	**14/15**	**13/14**	**14/15**	**13/14**	**14/15**
AFP	-	11	5	-	-	-	-	-
NSW Police	-	2	-	-	-	-	1	2
Total	**-**	**13**	**5**	**-**	**-**	**-**	**1**	**2**

Mutual assistance

Section 102B of the TIA Act requires that the annual report include information about the number of occasions on which lawfully intercepted information or interception warrant information was provided to a foreign country under subsection 68(1) or section 68A of the TIA Act in connection with an authorisation made under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*. One authorisation issued under section 13A included telecommunications interception material.

Number of interceptions carried out on behalf of other agencies

The TIA Act supports the ability of interception agencies to cooperate and to work collaboratively by enabling one interception agency to carry out interception on behalf of other agencies. Typically this occurs when a larger agency assists a smaller agency to intercept to reduce the costs of the smaller agency.

Table 19: Number of interceptions carried out on behalf of other agencies—s. 103(ac)

Interception carried out by:	Interception carried out on behalf of:	Number of interceptions:
ACC	CCC (QLD)	109
AFP	ACLEI	2
	ACC	2
CCC (WA)	WA POLICE	6
VIC Police	TAS POLICE	24
IBAC	ICAC (SA)	3
Total		**146**

Telecommunications interception expenditure

Table 20 below provides information about the total expenditure (including expenditure of a capital nature) by interception agencies on telecommunications interception warrants and the average expenditure (total warrant expenditure divided by the number of warrants issued) per warrant. The average cost per warrant is significantly affected by capital expenditure (which can vary significantly, for instance, due to a capital upgrade program) and the number of warrants issued, meaning that smaller interception agencies typically have higher average costs as they apply for fewer warrants. Care should be taken in comparing costs associated with average expenditure as interception agencies employ different interception models which may result in some instances costs associated with interception being delineated, and for other agencies, those same costs being included in their average expenditure.

Table 20: Total expenditure incurred by each agency in connection with the execution of telecommunications interception warrants and average expenditure per telecommunications interception warrant—ss. 103(a) and 103(aa)

Police	Total expenditure ($)	Average expenditure ($)
ACC	8,257,735	28,573
ACLEI	111,193	37,064
AFP	16,685,145	19,583
CCC (QLD)	1,939,070	44,069
CCC (WA)	1,189,101	51,700
IBAC	1,677,907	93,217
ICAC (NSW)	85,308	17,062
ICAC (SA)	119,978	39,993
NSW CC	2,851,845	15,415
NSW Police	6,154,535	4,017
NT Police	995,254	18,431

Police	Total expenditure ($)	Average expenditure ($)
PIC	1,344,327	28,006
QLD Police	4,654,842	17,176
SA Police	2,974,939	34,999
TAS Police	557,000	23,208
VIC Police	7,791,994	45,302
WA Police	3,972,509	12,492

Table 21 provides a breakdown of the total recurrent costs of interception over the reporting period. As agencies do not necessarily treat or record particular items of expenditure in the same way, caution should be exercised in comparing costs incurred by individual agencies.

Table 21: Recurrent costs of interceptions per agency

Agency	Salaries	Administrative support	Capital expenditure	Interception costs	Total ($)
ACC	6,170,150	88,595	636,116	1,362,874	**8,257,735**
ACLEI	100,089	5,099	-	6,005	**111,193**
AFP	8,221,757	220,701	5,583,084	2,659,603	**16,685,145**
CCC (QLD)	1,300,261	159,843	38,212	440,754	**1,939,070**
CCC (WA)	835,928	4,136	266,664	82,373	**1,189,101**
IBAC	1,470,728	52,563	-	154,616	**1,677,907**
ICAC (NSW)	50,928	-	-	34,380	**85,308**
ICAC (SA)	38,160	-	-	81,818	**119,978**
NSW CC	2,048,341	-	4,803	798,701	**2,851,845**
NSW Police	4,680,702	283,625	20,000	1,170,208	**6,154,535**
NT Police	794,098	-	120,809	80,347	**995,254**
PIC	1,127,312	-	-	217,015	**1,344,327**
QLD Police	3,258,736	490,147	85,540	820,419	**4,654,842**
SA Police	2,177,266	291,691	304,420	201,562	**2,974,939**
TAS Police	400,000	50,000	60,000	47,000	**557,000**
VIC Police	4,876,309	266,065	1,528,000	1,121,620	**7,791,994**
WA Police	3,318,407	490,635	-	163,467	**3,972,509**

Emergency service facilities

Table 22 sets out the number of places that have been declared under the TIA Act to be emergency service facilities. Under the TIA Act, listening to or recording calls to and from a facility declared by the Minister to be an emergency service facility is not interception. This exemption ensures that emergency services can assist emergency callers and respond to critical situations as quickly as possible, without the need to first obtain a caller's consent to recording of the call.

Table 22: Emergency service facility declarations

State/territory	Police	Fire brigade	Ambulance	Emergency services authority	Despatching
Australian Capital Territory	5	-	-	-	3
New South Wales	8	95	6	-	6
Northern Territory	2	-	1	1	4
Queensland	21	12	6	-	13
South Australia	1	2	1	-	3
Tasmania	1	2	1	-	2
Victoria	6	1	10	3	5
Western Australia	1	2	1	-	6
Total	**45**	**114**	**26**	**4**	**42**

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) with 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 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.

Law enforcement agencies' use of interception powers under the TIA Act is independently overseen 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 inspections are retrospective and on the basis of a full year, and for this reason, the Ombudsman inspected relevant telecommunications interception warrants that expired between 1 January and 31 December 2014.

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 provides a copy to the Commonwealth Attorney-General.

The Commonwealth Ombudsman also conducts regular inspections of records in relation to access by enforcement agencies (including both Commonwealth and state agencies) to stored communications and reports 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).

During its review of warrants that expired in the period 1 January to 31 December 2014, the Ombudsman noted that there continues to be a high level of compliance with the TIA Act, where agencies displayed a good understanding of the TIA Act's requirements. The Ombudsman particularly noted the cooperative and responsive approach towards inspection findings.

Overall, the Ombudsman did not identify any systemic issues or significant problems, with all agencies found to be compliant with the majority of the Ombudsman's inspection criteria. The Ombudsman's inspection criteria (see Figures 4 and 5) are:

1. Were restricted records properly destroyed (s 79)?
2. Were the requisite documents kept in connection with the issue of warrants (s 80)?
3. Were warrant applications properly made and warrants in the correct form (ss 39(1) and 49)?
4. Were the requisite records kept in connection with interceptions (s 81)?
5. Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)?

Commonwealth Ombudsman's summary of findings

Table 23a: Summary of findings from the two inspections conducted at each agency during the period 1 January to 30 June 2014

Criteria	ACC	ACLEI	AFP
Were restricted records properly destroyed (s 79)?	Not assessed—the ACC advised there were no destructions conducted in the inspection period.	Not assessed as no records destroyed.	Compliant for physical restricted records, not compliant for electronic restricted records.
Were the requisite documents kept in connection with the issue of warrants (s 80)?	Compliant.	Compliant with an exception relating to four warrants.	Compliant with the exception of one instance (self-disclosed).
Were warrants properly applied for and in the correct form (ss 39(1) and 49)?	Compliant.	Compliant.	Compliant with the exception of one instance.
Were requisite records kept in connection with interceptions (s 81)?	Compliant.	Compliant.	Compliant with the exception of two instances in relation to s 81(1)(e).
Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)?	Compliant.	Nothing to indicate otherwise, except in one instance.	Nothing to indicate otherwise except in two instances. Unable to determine in eight instances.

Table 23b: Summary of findings from the two inspections conducted at each agency during the period 1 July to 31 December 2014

Criteria	ACC	ACLEI	AFP
Were restricted records properly destroyed (s 79)?	Not assessed as no records destroyed.	Not assessed as no records destroyed.	Not compliant for physical restricted records, no electronic restricted records assessed.
Were the requisite documents kept in connection with the issue of warrants (s 80)?	Compliant.	Compliant.	Compliant.
Were warrants properly applied for and in the correct form (ss 39(1) and 49)?	Compliant except in two instances.	Compliant.	Compliant.
Were requisite records kept in connection with interceptions (s 81)?	Compliant.	Compliant.	Compliant.

Criteria	ACC	ACLEI	AFP
Were interceptions conducted in accordance with the warrants (s 7) and was any unlawfully intercepted information properly dealt with (s 63)?	Nothing to indicate otherwise.	Nothing to indicate otherwise.	Nothing to indicate otherwise except in 11 instances, unable to determine in two instances.

Commonwealth Ombudsman's findings for individual agency for warrants expiring between 1 January to 31 December 2014

ACC

No formal recommendations were made as a result of either of the two inspections of the ACC, nor were any deficiencies identified that impacted the integrity of the telecommunications interception regime. The Ombudsman noted the ACC had implemented effective monitoring and quarantining procedures for its interception of telecommunications.

ACLEI

No formal recommendations were made as a result of either of the two inspections of ACLEI. The Ombudsman noted that ACLEI did not provide proper notification of the services intercepted under four named person warrants and separately continued interceptions in matters where revocations had been issued to the Department, prior to notifying the carriers to disconnect the interception. ACLEI has updated its procedures to ensure that these errors do not occur in the future.

AFP

The Ombudsman made one formal recommendation for the AFP to update its procedures and processes to ensure compliance with section 79 of the TIA Act of which the AFP was responsive to the issue. The AFP accepted the recommendation and took appropriate remedial action.

The Ombudsman noted that subsection 7(4) of the TIA Act had been breached by the AFP when conducting emergency interceptions. To mitigate the effects of this, the AFP advised that it had implemented restrictive practices to quarantine any unauthorised information. The Ombudsman did not consider that these instances reflected significant problems with the AFP's processes and for ensuring interceptions were lawful.

The Ombudsman was unable to determine whether some intercepted lines obtained under 9 warrants were lawfully intercepted. As a result, the AFP investigated these issues and quarantined information obtained under one warrant and set in place new procedures. The Ombudsman noted the AFP's responsiveness to this issue.

Further information about the Commonwealth Ombudsman's telecommunications interception inspection criteria is outlined in Figure 4 and 5 below.

Figure 4: Commonwealth Ombudsman's Telecommunications Interception Inspection Criteria

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*

s 79 Destruction of restricted records

1.1 Evidence that the chief officer was satisfied that the destroyed restricted records were not likely to be required for a permitted purpose and were subsequently destroyed forthwith (s 79(1)).

1.2 Evidence that the destroyed restricted records were not destroyed before the Attorney-General had inspected the warrants under which the restricted records were obtained (s 79(2)).

s 80 Documents kept in connection with the issue of warrants

2.1 Evidence that all warrants issued to the agency are kept (s 80(a)).

2.2 Evidence that a copy of each notification under s 59A(2) is kept (notifications to the Secretary of AGD) (s 80(b)).

2.3 Evidence that all instruments revoking warrants are kept (s 80(c)).

2.4 Evidence that a copy of each certificate issued under s 61(4) is kept (*evidentiary certificates*) (s 80(d)).

2.5 Evidence that each authorisation by the chief officer under s 66 (2) is kept (*authorisation to receive information obtained under warrants*) (s 80(e)).

s 81 Other records kept in connection with interceptions (Warrant details, lawfully intercepted information (LII) records, use and communication)

3.1 Evidence that each telephone application for a part 2–5 warrant is kept (s 81(1)(a)).

3.2 Evidence that statements as to whether applications were withdrawn, refused or issued on the application are kept (s 81(1)(a)).

3.3 Evidence that the particulars of all warrants whose authority is exercised by the agency are kept (s 81(1)(c)(i)).

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 (ss 81(1)(c)(ii)) and 81(2)).

3.5 Evidence that particulars of the duration of each interception and the name of the person who carried out each interception are kept (ss 81(1)(c)(iii) and (iv)).

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 (s 81(1)(c)(v)).

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 (s 81(1)(d)(i)).

3.8 Evidence that particulars of each occasion when the restricted record came to be in the agency's possession are kept (s 81(1)(d)(ii)).

3.9 Evidence that particulars of each occasion when the restricted record ceased to be in the agency's possession are kept (s 81(1)(d)(iii)).

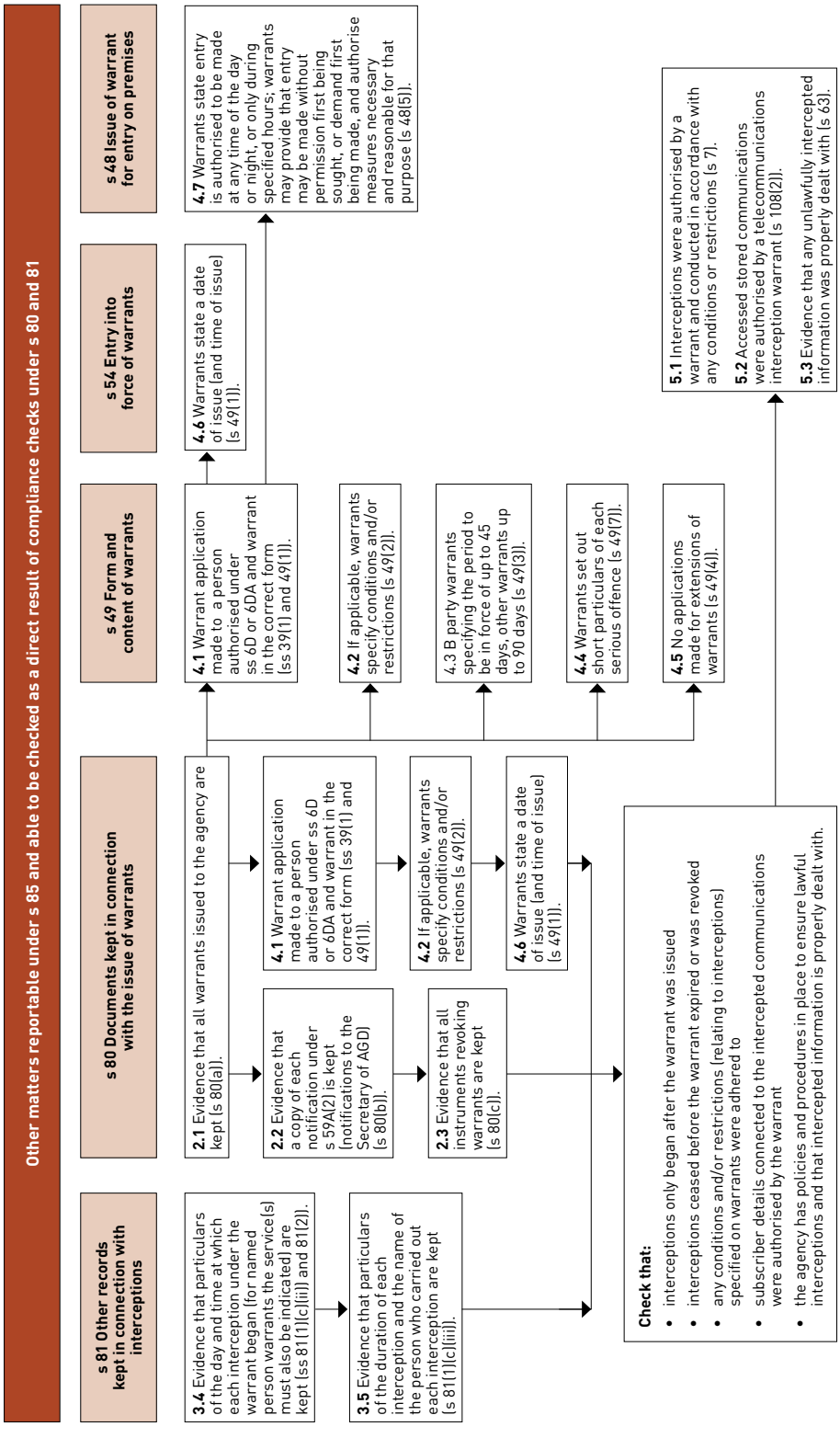
3.10 Evidence that particulars of each other agency from or to which or other person from or to whom the agency received or supplied the restricted record are kept (s 81(1)(d)(iv)).

3.11 Evidence that particulars of each use made by the agency of LII are kept (s 81(1)(e)).

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 (s 81(1)(f)).

3.13 Evidence that particulars of when LII was given in evidence in a relevant proceeding in relation to the agency are kept (s 81(1)(g)).

Figure 5: Other matters reportable under s.85



CHAPTER 2

STORED COMMUNICATIONS

Authorities and bodies that are 'enforcement agencies' under the TIA Act can apply to an independent issuing authority for a stored communications warrant to investigate a 'serious contravention' of the law.

Definition

An 'enforcement agency' is broadly defined to include all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.

Stored communications include communications such as email, SMS or voice messages stored on a carrier's network.

Definition

A 'serious contravention' includes:

- **serious offences (offences for which a telecommunications interception warrant can be obtained)**
- **offences punishable by imprisonment for a period of at least three years**
- **offences 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.**

Table 24: Applications and telephone applications for stored communications warrants—ss. 162(1)(a)-(b) and 162(2)(a)-(b)

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants	
		13/14	14/15	13/14	14/15
ACC	Made	4	4	-	-
	Refused/withdrawn	-	-	-	-
	Issued	4	4	-	-
ACCC	Made	-	4	-	-
	Refused/withdrawn	-	-	-	-
	Issued	-	4	-	-
AFP	Made	39	94	-	-
	Refused/withdrawn	-	-	-	-
	Issued	39	94	-	-
ASIC	Made	3	-	-	-
	Refused/withdrawn	-	-	-	-
	Issued	3	-	-	-
CCC (QLD)	Made	1	-	-	-
	Refused/withdrawn	-	-	-	-
	Issued	1	-	-	-
CCC (WA)	Made	1	-	-	-
	Refused/withdrawn	-	-	-	-
	Issued	1	-	-	-
CUSTOMS	Made	12	10	-	-
	Refused/withdrawn	-	-	-	-
	Issued	12	10	-	-
ICAC (NSW)	Made	3	-	-	-
	Refused/withdrawn	-	-	-	-
	Issued	3	-	-	-
NSW CC	Made	8	3	-	-
	Refused/withdrawn	-	-	-	-
	Issued	8	3	-	-
NSW Police	Made	233	290	1	-
	Refused/withdrawn	-	-	-	-
	Issued	233	290	1	-
NT Police	Made	5	16	-	-
	Refused/withdrawn	-	-	-	-
	Issued	5	16	-	-
PIC	Made	4	7	-	-
	Refused/withdrawn	-	-	-	-
	Issued	4	7	-	-

Agency	Relevant statistics	Applications for stored communications warrants		Telephone applications for stored communications warrants	
		13/14	14/15	13/14	14/15
QLD Police	Made	107	123	-	-
	Refused/withdrawn	1	-	-	-
	Issued	106	123	-	-
SA Police	Made	21	38	-	-
	Refused/withdrawn	-	-	-	-
	Issued	21	38	-	-
TAS Police	Made	52	30	-	-
	Refused/withdrawn	-	1	-	-
	Issued	52	29	-	-
VIC Police	Made	47	40	-	-
	Refused/withdrawn	-	-	-	-
	Issued	47	40	-	-
WA Police	Made	32	38	-	-
	Refused/withdrawn	-	-	-	-
	Issued	32	38	-	-
Total	**Made**	**572**	**697**	**1**	**-**
	Refused/withdrawn	**1**	**1**	**-**	**-**
	Issued	**571**	**696**	**1**	**-**

Table 25: Stored communications subject to conditions or restrictions – sections 162(2)(d)

Agency	Application for warrants
	14/15
NSW Police	290
QLD Police	3
SA Police	38
TAS Police	1
VIC Police	1
Total	**333**

Effectiveness of stored communications warrants

In 2014–15 law enforcement agencies made 377 arrests, conducted 335 proceedings and obtained 198 convictions based on evidence obtained under stored communications warrants.

Table 26: Number of arrests, proceedings and convictions made on the basis of lawfully accessed information—s. 163(a)-(b)

Agency	Arrests		Proceedings		Convictions	
	13/14	14/15	13/14	14/15	13/14	14/15
ACC	15	5	8	-	-	-
AFP	23	46	19	34	1	15
CCC (QLD)	-	3	-	-	-	-
CCC (WA)	-	-	2	-	2	-
Customs	4	-	1	-	1	-
NSW Police	51	179	138	221	121	107
NT Police	2	8	-	-	-	-
PIC	-	8	-	-	-	-
QLD Police	23	69	-	68	-	68
SA Police	-	17	-	3	-	2
TAS Police	1	4	1	-	1	1
VIC Police	21	28	3	7	16	1
WA Police	13	10	4	2	2	4
Total	**153**	**377**	**176**	**335**	**144**	**198**

Care should be taken in interpreting Table 26 as an arrest recorded in one reporting period may not result in a prosecution (if any) until a later reporting period. Any resulting conviction may be recorded in that or an even later reporting period.

Preservation notices

Under Part 3-1A of Chapter 3 of the TIA Act, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications held that relate to the person or telecommunications service specified in the notice. The carrier is required to keep the stored communications while the notice is in force, which allows a period of time for enforcement agencies to obtain a warrant to access them. The purpose of the preservation notice is to prevent the communications from being destroyed before an agency can obtain a warrant to access the information.

The TIA Act provides for two types of preservation notices:

- *domestic preservation notices*—which cover stored communications that might relate either to a contravention of certain Australian laws or to security
- *foreign preservation notices*—which cover stored communications that might relate to a contravention of certain foreign laws. Only the AFP can give a foreign preservation notice to a carrier. The AFP can only issue a notice if a foreign country has requested the preservation of stored communications that relate to the contravention of certain foreign laws.

Domestic preservation notices must be revoked if the stored communications relating to the person or telecommunications service specified in the notice are no longer under investigation.

Foreign preservation notices must be revoked if 180 days has elapsed since the carrier was given the notice and the foreign country has not made a request to the Attorney-General for access to those communications in that time period, or if the Attorney-General refuses the request to access the communications.

In 2014–15, 1,716 domestic preservation notices and 592 domestic preservation revocation notices were issued (see Table 27).

Table 27: Domestic preservation notices—s. 161A(1)

Agency	Domestic preservation notice issued	Domestic preservation notice revocations issued
ACC	15	-
ACCC	4	-
ACLEI	9	9
AFP	287	60
CCC (QLD)	43	13
CUSTOMS	7	-
ICAC (NSW)	2	-
NSW CC	8	4
NSW Police	351	43
NT Police	189	140
PIC	25	3
QLD Police	390	194
SA Police	82	33
TAS Police	106	41
VIC Police	74	22
WA Police	124	30
Total	**1,716**	**592**

Under section 161A(2) of the TIA Act the AFP is required to report on foreign preservation notices. In 2014–15, the AFP reported that three foreign preservation notices and no foreign preservation notice revocation notices were issued.

Mutual assistance

Section 162(1)(c) requires the report to outline the number of stored communications warrants obtained to assist in mutual assistance applications. No stored communications warrants were obtained in these circumstances.

Section 163A of the TIA Act provides that the annual report must provide information regarding the number of occasions in which lawfully accessed information or stored communications warrant information was provided to a foreign country under the *Mutual Assistance in Criminal Matters Act 1987* (the Mutual Assistance Act). In 2014-15 there were no occasions on which this information was provided to a foreign country under the Mutual Assistance Act.

Commonwealth Ombudsman—inspection of stored communications records expiring between 1 July 2013 and 30 June 2014

During the reporting period the Commonwealth Ombudsman inspected the preservation notices and stored communications access records of 20 enforcement agencies. The inspections are retrospective and on the basis of a full year, and for this reason, the Ombudsman inspected enforcement agencies' preservation notices and stored communication warrants that expired between 1 July 2013 to 30 June 2014.

During this inspection period the Ombudsman noted that agencies have generally displayed a positive attitude towards compliance and meeting their requirements under Chapter 3 of the TIA Act. It was noted that agencies were generally responsive to the inspection findings and receptive to any suggestions for improvement, continuing to update relevant policies and procedures to help staff to comply with the TIA Act.

The Ombudsman's inspection criteria are:

1. Were destructions properly conducted and reported on (ss 150 and 151(e))?
2. Were records properly kept (ss 150A and 151)?
3. Were preservation notices properly given (ss 107H(2), 107H(3) and 107M, 107N, and 107S)?
4. Were preservation notices properly revoked (ss 107L and 107M, 107R and 107S)?
5. Were warrants properly applied for (ss 113, 5E, 6B, 116(1)(d), 116(1)(da), 6DB, 118, and 119(5))?
6. Were warrants properly revoked (where applicable) (ss 122 and 123)?
7. Was the authority of warrants lawfully exercised and were accessed stored communications received by authorised officers in the first instance (ss 127(1) and (2), and 135(2))?

8. Were conditions and restrictions on warrants adhered to (s 117)?
9. Does the agency have procedures in place to ensure that it is only dealing with lawfully accessed stored communications (ss 108, 117 and 119) and were any unlawfully accessed stored communications properly dealt with (s133)?

The Ombudsman also met with agencies to discuss policies and procedures and highlighted any gaps in agency processes that may pose potential compliance risks.

Overall

Most agencies were assessed as compliant and where issues of non-compliance were identified, the agency in question undertook to implement appropriate remedial action or seek further legal advice.

Record keeping compliance

The Ombudsman concluded that all agencies who gave preservation notices were compliant with record-keeping requirements under section 150 and 150A of the TIA Act except one. The agency accepted this finding and was able to identify the reasons why this occurred and advised of additional remedial action to prevent reoccurrences.

Additionally, in the previous reporting period, the Ombudsman made a recommendation to another agency to improve its record-keeping procedures to ensure compliance with section 150 of the TIA Act. The agency did not appear to have a reliable system in place for keeping track of how many warrants with which it had been issued to enable it to accurately report on warrant numbers. During the current reporting period, the agency advised it had not taken any measures to improve its processes and procedures relating to record-keeping compliance. The Ombudsman advised it will continue to closely monitor this agency's compliance during its next inspection.

Preservation notices

The Ombudsman identified a number of instances of non-compliance where preservation notices were not given and revoked in accordance with the TIA Act. In particular, the Ombudsman made a number of suggestions to agencies that they improve their processes which were generally accepted. In some instances, agencies are seeking further clarification from the Attorney-General's Department regarding the operation of the legislation.

Properly handling unlawfully accessed stored communications

The Ombudsman advised that it was satisfied that agencies have appropriate screening procedures in place, in line with recommendations from previous reporting years. However, the Ombudsman identified several instances where unlawfully accessed stored communications were not appropriately handled. In response to the findings, the relevant agencies subsequently quarantined that unlawfully accessed information.

Destructions

The Ombudsman identified that most agencies were compliant with the provisions relating to the destruction of stored communications. Any agencies identified as non-compliant have advised the Ombudsman of remedial action.

Applying for warrants

Several agencies applied for warrants in relation to a victim of a serious contravention who was able, but chose not to, consent to their stored communications being accessed by law enforcement against the intention of paragraph 116(1)(da) of the TIA Act. The Attorney-General's Department has provided advice regarding the operation of the legislation in relation to victims.

Figure 6: Commonwealth Ombudsman Stored Communications Access Inspection Criteria

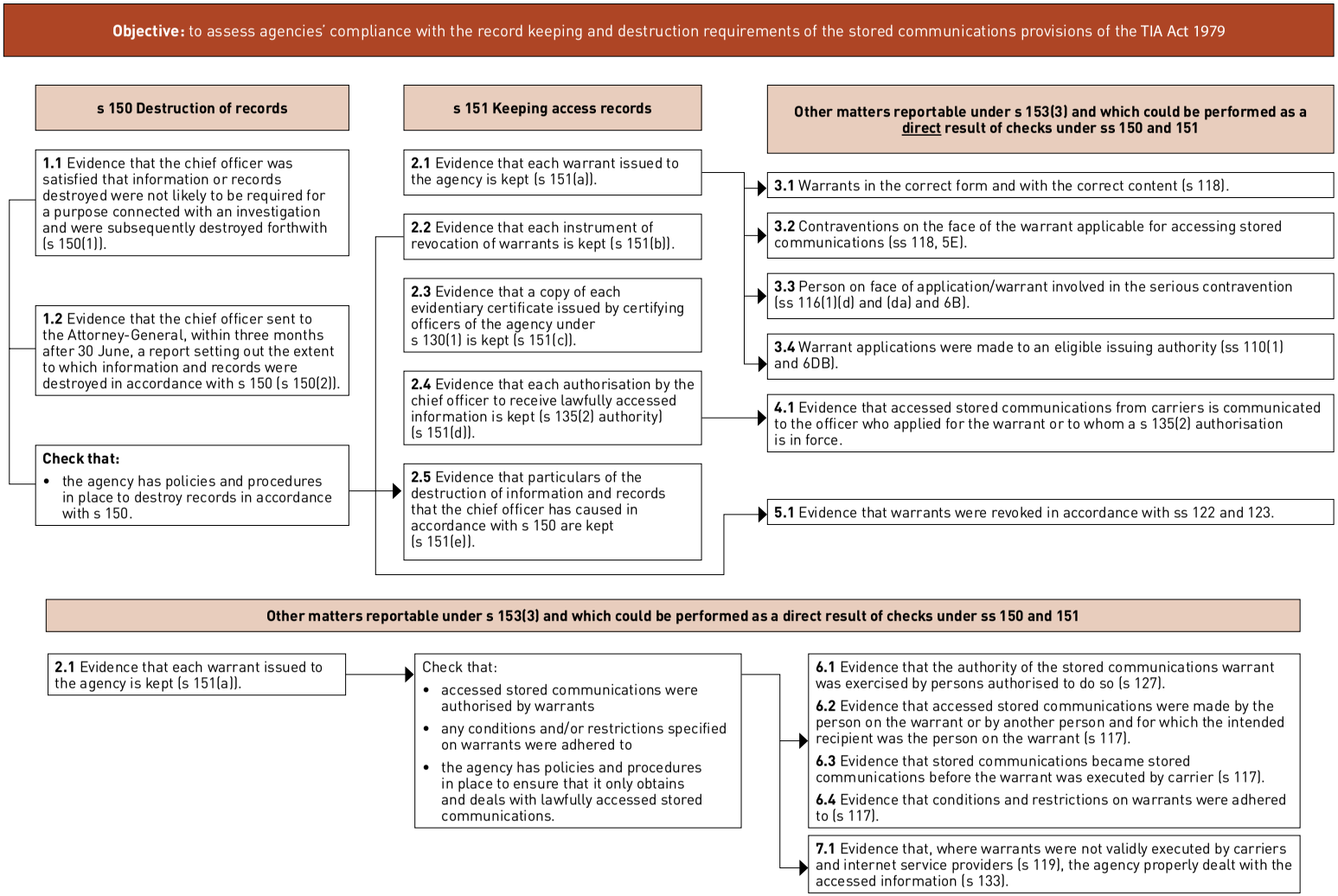
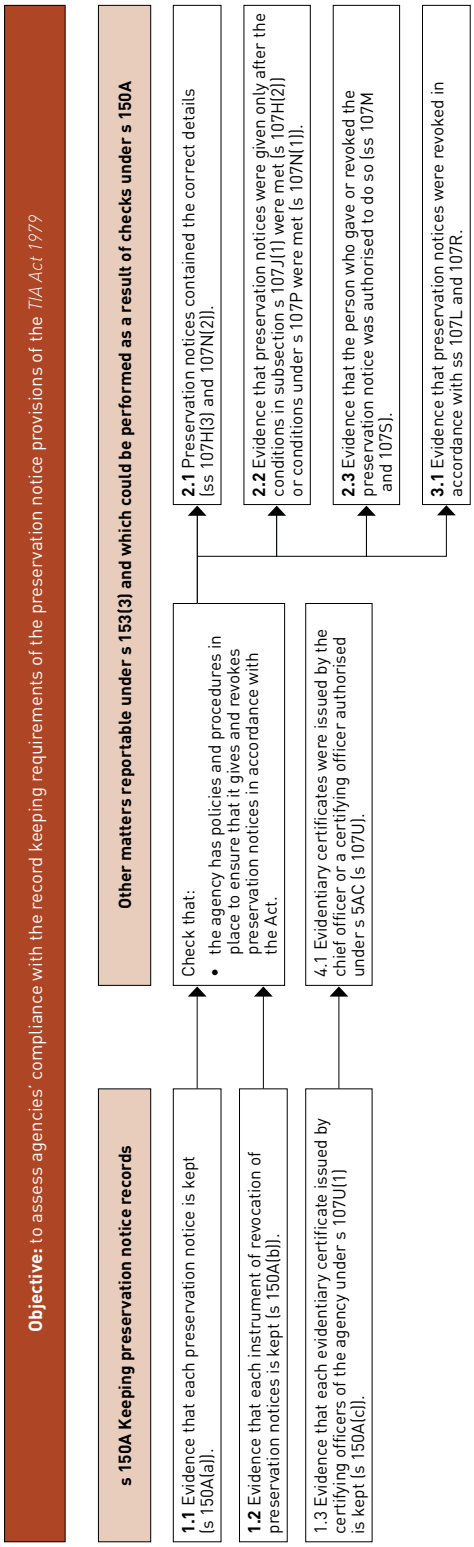


Figure 7: Commonwealth Ombudsman Preservation Notice Inspection Criteria



CHAPTER 3

TELECOMMUNICATIONS DATA

Access to telecommunications data is regulated by Chapter 4 of the TIA Act which permits enforcement agencies to authorise telecommunications carriers to disclose telecommunications data where that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue.

Definition

An 'enforcement agency' is broadly defined to include all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue.

In 2014–15, 83 enforcement agencies made historical data authorisations.

Access to telecommunications data is a critical tool for investigating criminal offences and other activities that threaten community safety and security.

Definition

'Telecommunications data' is information about a communication—such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent.

Data is often the first source of lead information for further investigations, helping to eliminate potential suspects and to support applications for more privacy intrusive investigative tools including search warrants and interception warrants.

Under the TIA Act, all enforcement agencies can access historical data and criminal law enforcement agencies can also access prospective data. Disclosure of telecommunications data must be approved by an authorised senior officer of the relevant enforcement agency.

Definition

'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.

'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 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 and is effective for 45 days or less.

Future reporting obligations

From 13 October 2015, enforcement agencies will be required to keep statistics on the types of offences for which data authorisations are made and the types of data being sought, i.e subscriber data or traffic data to assist in investigations. These reporting figures will be included in the next and future annual reports.

Existing data—enforcement of a criminal law

Tables 28, 29, 30 and 31 provide information on agency use of historical data authorisations to enforce the criminal law. In 2014–15, enforcement agencies made 354,841 data authorisations to enforce the criminal law.

Table 28: Number of authorisations made by a Law Enforcement Agency for access to existing information or documents in the enforcement of a criminal law—s. 186(1)(a)

Agency	Authorisations	
	13/14	14/15
ACC	5,447	7,429
ACLEI	2,244	5,908
AFP	21,358	27,462
CCC (QLD)	10,896	12,451
CCC (WA)	1,804	1,333
IBAC	321	424
ICAC (NSW)	933	532
ICAC (SA)	16	734
NSW CC	3,294	3,023
NSW Police	111,889	114,111
NT Police	10,182	3,391
PIC	1,475	1,296
QLD Police	35,663	40,710

Agency	Authorisations	
	13/14	14/15
SA Police	8,504	11,668
TAS Police	9,921	8,152
VIC Police	63,325	66,663
WA Police	27,315	36,310
Total	**314,587**	**341,597**

Table 29: Number of authorisations made by a Commonwealth Enforcement Agency for access to existing information or documents in the enforcement of a criminal law—s. 186(1)(a)

Agency	Authorisations	
	13/14	14/15
ACCC	10	133
ASIC	1,771	1,691
ATO	277	206
Australian Financial Security Authority	128	76
Australian Fisheries Management Authority	3	-
Civil Aviation Safety Authority	-	11
Clean Energy Regulator	-	2
Customs	6,196	9,749
Dept. of Agriculture	84	58
Dept. of Defence (IGD, ADFIS)	25	21
Dept. of Health	38	58
Dept. of Immigration And Border Protection	107	102
Dept. of Social Services	1	-
Dept. of The Environment	13	21
Total	**8,653**	**12,128**

Table 30: 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—s. 186(1)(a)

Agency	Authorisations	
	13/14	14/15
Consumer and Business Services (SA)	-	111
Corrective Services NSW	52	52
Dept. of Commerce (WA)	78	97
Dept. of Economic Development, Jobs, Transport and Resources (VIC)	-	226
Dept. of Environment Regulation (WA)	-	18
Dept. of Environment, Land, Water and Planning (VIC) (formerly the Dept. of Fisheries (VIC))	347	27
Dept. of Justice (Corrections Victoria)	389	276
Environment Protection Authority (NSW)	5	51
Legal Services Board (VIC)	-	3
Office of Environment & Heritage (NSW)	47	46
Roads and Maritime Services NSW	-	5
RSPCA Queensland	-	14
RSPCA TAS	-	2
RSPCA Victoria	64	133
The Hills Shire Council	1	-
Transport Accident Commission (VIC)	8	8
Workcover NSW	4	6
Worksafe Victoria	25	41
Total	**1,020**	**1,116**

Table 31: 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	
	13/14	14/15
No. of authorisations made by a Law Enforcement Agency	314,587	341,597
No. of authorisations made by a Commonwealth Agency	8,653	12,128
No. of authorisations made by a State or Territory Agency	1,020	1,116
Total	**324,260**	**354,841**

Existing data—enforcement of a law imposing a pecuniary penalty or protecting public revenue

Tables 32, 33, 34 and 35 provide information on agency use of historical data authorisations in the enforcement of a law that imposes a pecuniary penalty or protects the public revenue.

Table 32: 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—s. 186(1)(b)

Agency	Authorisations	
	13/14	14/15
AFP	36	43
CCC (QLD)	11	3
NSW Police	5,324	3,570
NT Police	4	-
QLD Police	239	400
SA Police	2	2
TAS Police	764	536
Total	**6,380**	**4,554**

Table 33: 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—s. 186(1)(b)

Agency	Authorisations	
	13/14	14/15
ACCC	31	132
ASIC	110	160
ATO	66	43
Australia Post	810	625
Australian Health Practitioner Regulation Agency	23	22
Clean Energy Regulator	1	-
Customs	156	261
Department of Industry and Science (National Measurement Institute)	1	1
Dept. of Defence (IGD, ADFIS)	94	71
Dept. of Foreign Affairs and Trade	227	145

Agency	Authorisations	
	13/14	14/15
Dept. of Human Services	339	269
Dept. of Prime Minister & Cabinet (Formerly the Dept. of Families, Housing, Community Services and Indigenous Affairs)	-	1
Dept. of Social Services	1	6
Fair Work Building & Construction	7	8
Total	**1,866**	**1,744**

Table 34: 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—s. 186(1)(b)

Agency	Authorisations	
	13/14	14/15
ACT Revenue Office	3	3
Bankstown City Council	7	13
City of Darebin	1	-
Consumer Affairs Victoria	120	132
Consumer and Business Services (SA)	153	21
Dept of Environment and Heritage Protection (QLD)	32	28
Dept. of Agriculture and Fisheries (QLD)	25	41
Dept. of Commerce (WA)	87	115
Dept. of Economic Development, Jobs, Transport and Resources (VIC)	-	1
Dept. of Fisheries (WA)	113	98
Dept. of Justice (Sheriffs Office of Victoria)	16	3
Dept. of Mines and Petroleum (WA)	2	1
Dept. of Parks And Wildlife (WA)	6	42
Dept. of Primary Industries (NSW)	226	148
Harness Racing New South Wales	7	15
Harness Racing Victoria	3	2
Health Care Complaints Commission (NSW)	20	63
Ipswich City Council	21	3
Juvenile Justice NSW	-	2
Knox City Council	5	15

Agency	Authorisations	
	13/14	14/15
Legal Services Board (VIC)	9	-
Office of Fair Trading (NSW)	758	675
Office of Fair Trading (QLD)	252	361
Office of Liquor and Gaming Regulation (QLD)	3	2
Office of State Revenue (NSW)	127	34
Office of State Revenue (QLD)	1	1
Office of The Racing Integrity Commissioner (VIC)	10	48
Primary Industries & Regions (SA)	-	238
Racing and Wagering Western Australia	18	7
Racing NSW	16	33
Racing Queensland	4	5
Revenue SA	17	10
RSPCA Queensland	19	-
State Revenue Office Victoria	53	32
Taxi Services Commission (VIC)	-	5
Worksafe Victoria	17	-
Wyndham City Council	1	-
Total	**2,152**	**2,197**

Table 35: Total number of authorisations made for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or protecting public revenue—s. 186(1)(b)

Agency	Authorisations	
	13/14	14/15
No. of authorisations made by a Law Enforcement Agency	6,380	4,554
No. of authorisations made by a Commonwealth Agency	1,866	1,744
No. of authorisations made by a State or Territory Agency	2,152	2,197
Total	**10,398**	**8,495**

Prospective data—authorisations

Tables 36 and 37 set out information about the use of prospective data authorisations during the reporting year. 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 an authorisation is in force is continued in Table 36.

Table 36: Prospective data authorisations—s. 186(1)(c)

Agency	Number of authorisations made	Days specified in force	Actual days in force	Authorisations discounted
ACC	1,552	46,250	29,033	51
ACLEI	20	546	278	4
AFP	1,624	62,144	39,291	136
CCC (QLD)	339	9,915	7,855	8
CCC (WA)	59	2,554	1,040	14
Customs	157	216	206	1
IBAC	165	7,125	5,848	13
ICAC (NSW)	18	514	359	1
ICAC (SA)	4	165	138	-
NSW CC	809	31,748	24,439	107
NSW Police	630	22,059	11,846	61
NT Police	448	19,485	13,235	90
PIC	111	4,637	3,325	15
QLD Police	5,240	226,403	182,222	596
SA Police	372	14,465	9,236	23
TAS Police	161	7,245	4,998	10
VIC Police	4,797	98,226	43,859	53
WA Police	923	41,535	29,500	96
Total	**17,429**	**595,232**	**406,708**	**1,279**

The table also outlines the number of days the authorisations were to be in force and how many days they were actually in force as well as providing the number of authorisations still in force at the end of the reporting period.

Table 37 provides information about the average number of days the authorisations were specified to be in force and the average actual number of days they remained in force.

Table 37: Average specified and actual time in force of prospective data authorisations

Agency	Average period specified		Average period actual	
	13/14	14/15	13/14	14/15
ACC	28	30	19	19
ACLEI	8	27	21	17
AFP	32	38	25	26
CCC (QLD)	18	29	18	23
CCC (WA)	34	43	25	23
Customs	1	1	1	1
IBAC	45	43	37	38
ICAC (NSW)	45	29	35	21
ICAC (SA)	-	41	-	35
NSW CC	36	39	29	35
NSW Police	38	35	25	21
NT Police	45	43	45	37
PIC	40	42	36	35
OPI	44	-	44	-
QLD Police	42	43	37	39
SA Police	42	39	32	26
TAS Police	45	45	30	33
VIC Police	15	20	9	9
WA Police	45	45	36	36
Average	**33**	**35**	**28**	**29**

Data authorisations to locate missing persons

Under section 178A of the TIA Act, the AFP and state police forces can authorise the disclosure of telecommunications data to help find a missing person.

Table 38: The number of authorisations made for access to existing information or documents for the location of missing persons—s. 178A

Agency	Authorisations	
	13/14	14/15
AFP	55	112
NSW Police	1,097	1,377
NT Police	36	8
SA Police	33	50
TAS Police	155	201
VIC Police	-	5
QLD Police	652	639
Total	**2,028**	**2,392**

Data authorisations for foreign law enforcement

The TIA Act also requires the AFP to report on data authorisations made in relation to foreign law enforcement. In 2014–15, the AFP made 36 data authorisations for access to telecommunications data for the enforcement of the criminal law of a foreign country.

Following these requests, the AFP made 11 disclosures to foreign law enforcement agencies. Information was disclosed to the following countries: the Former Yugoslav Republic of Macedonia, France, New Zealand, the United Kingdom, Czech Republic, Switzerland, Vietnam, the United States of America, Thailand and Mexico.

CHAPTER 4

FURTHER INFORMATION

For further information about the *Telecommunications (Interception and Access) Act 1979* please contact the Attorney-General's Department:

Electronic Surveillance Policy 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 <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 <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 s.34 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 Corruption 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
Police Integrity Commission (New South Wales)	14 July 1998
Queensland Police Service	8 July 2009
Independent Commissioner Against Corruption (South Australia)	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

Acronym	Agency/Organisation
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)
CCC (QLD)	Crime and Corruption Commission (Queensland)
Customs	Australian Customs and Border Protection Service
DIBP	Department of Immigration and Border Protection
Defence (IGD, ADFIS)	Inspector-General Defence, Australian Defence Force Investigative Service
IBAC (Vic)	Independent Broad-based Anti-corruption Commission (Victoria)
NSW CC	New South Wales Crime Commission
ICAC (NSW)	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 (SA)	Independent Commissioner Against Corruption (South Australia)

Acronym	Agency/Organisation
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